TOP SECRET
CONF-3-17
2017 FC 1048

Docket: [***]

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 [***] Threat-Related Activities

and

Docket: [***]

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: X (Re)

Federal Court, Crampton C.J.—Ottawa, May 25, 26 and June 23; September 27, 2017.

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

Security Intelligence — Applications concerning requests by Canadian Security Intelligence Service (CSIS) for warrants in relation to its investigation of activities suspected of constituting threats to security of Canada — CSIS requesting ability to obtain basic identifying information (BII) from communications services providers — CSIS seeking to add two additional authorizations to warrants previously issued by Court — At issue was whether Court can authorize CSIS to obtain BII in respect of: (1) communications accounts corresponding to telephone numbers or electronic identifiers that may in the future

TRÈS SECRET
CONF-3-17
2017 CF 1048

Dossier : [***]

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

et

Affaire intéressant les activités liées à la menace [***]

et

Dossier : [***]

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

et

Dans l'affaire visant le terrorisme islamiste

Répertorié : X (Re)

Cour fédérale, le juge en chef Crampton—Ottawa, 25 et 26 mai, et 23 juin; 27 septembre 2017.

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

Renseignement de sécurité — Demandes concernant les demandes de mandats présentées par le Service canadien du renseignement de sécurité (SCRS) dans le cadre d'enquêtes sur des activités au sujet desquelles il pourrait exister des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada — Le SCRS a demandé l'autorisation d'obtenir des données d'identification de base (DIB) auprès des fournisseurs de services de communication — Le SCRS souhaitait ajouter deux autres autorisations aux mandats décernés par la Cour — Il s'agissait de déterminer si la

come to its attention in the course of its investigations; (2) communications accounts identified pursuant to its review of specifically defined information obtained in relation to certain individuals; (3) a communications account that corresponds to a telephone number or an electronic identifier where a "chief" within CSIS determines that the account was identified during its investigation, and that the BII would assist CSIS in its investigation. — Except in exceptional circumstances (not demonstrated herein), CSIS cannot be prospectively authorized to obtain BII in relation to communications accounts whose nexus with CSIS investigations not yet described, established — Persons responsible for authorizing use of intrusive powers required to consider impact of such intrusion on subject of search — Assessment having to be made of context of each particular situation, impact on individual — Balancing analysis having to be conducted between interests of state, specific individual whose privacy interests at issue — Appropriate balance with respect to first type of authorization sought (i.e. broad authorization) not met herein — CSIS not providing Court with any understanding of specific nexus between information sought, CSIS investigation — Court not having sufficient sense of nexus between identified threat-related activities, individual whose privacy rights would be encroached to be considered "reasonable" within meaning of Charter, s. 8 — Second group of requested amendments granted, although some conditions necessary to address certain issues — As to third issue raised herein, proposed authorizations impermissibly delegating to a "chief" within CSIS a function having to be performed by designated Federal Court judge — Only designated judge can make determination of whether grounds that must be established before specific individual's privacy interests can be intruded upon met — Application in [***] dismissed; application in [***] dismissed in part.

These were applications concerning requests by the Canadian Security Intelligence Service (CSIS) for warrants in relation to its investigation of two separate groups of activities that may on reasonable grounds be suspected of constituting threats to the security of Canada.

The applications pertained to CSIS's ability to obtain basic identifying information (BII) from communications services providers (CSPs). BII, consisting of the name and address of a subscriber, would be obtained in respect of communications

Cour peut autoriser le SCRS à obtenir des DIB liées à 1) des comptes de communication correspondant à des numéros de téléphone ou à des identificateurs électroniques qui pourront éventuellement attirer son attention lors de ses enquêtes; 2) des comptes de communications qu'il a découverts en examinant des informations clairement définies ayant trait à certaines personnes; et 3) un compte de communications correspondant à un numéro de téléphone ou à un identificateur électronique lorsqu'un « chef » au sein du SCRS détermine que ce compte a été découvert lors d'une enquête et que les DIB faciliteraient cette enquête — Sauf en des circonstances exceptionnelles (dont l'existence n'a pas été démontrée en l'espèce), le SCRS ne peut être autorisé, de manière prospective, à obtenir les DIB liées à des comptes de communication s'il n'a pas encore décrit et établi de lien précis entre les DIB et les enquêtes en question — Les personnes chargées d'autoriser le recours à des pouvoirs envahissants doivent tenir compte des répercussions de l'intrusion sur l'objet de la fouille — Il est nécessaire d'évaluer le contexte de chaque situation et son incidence sur la personne — Il y a lieu d'atteindre un équilibre entre les intérêts de l'État et ceux de la personne dont le droit au respect de sa vie privée est en jeu — Le juste équilibre n'a pas été atteint en ce qui concerne les modifications du premier type (à savoir la vaste autorisation) — Le SCRS n'a fourni à la Cour aucune explication lui permettant de comprendre le lien précis entre l'information recherchée et ses enquêtes — Cela n'a pas permis à la Cour d'assez bien constater le lien entre les activités liées à la menace et la personne dont les droits en matière de vie privée seraient enfreints pour qu'elle considère le libellé du mandat « non abusif » au sens de l'art. 8 de la Charte — La deuxième catégorie d'amendements demandés a été accordée, mais il s'est avéré nécessaire d'imposer des conditions pour répondre à certaines préoccupations — En ce qui concerne la troisième question soulevée dans les demandes, les autorisations proposées auraient pour effet de déléguer de façon inacceptable au titulaire d'un poste de « chef » au SCRS une fonction qui relève exclusivement d'un juge désigné de la Cour fédérale — Seul un juge désigné peut déterminer si les motifs qui doivent être établis avant qu'il soit possible d'enfreindre le droit d'une personne au respect de sa vie privée l'ont bel et bien été — Demande dans le dossier [***] rejetée; demande dans le dossier [***] rejetée en partie.

Il s'agissait de demandes concernant les demandes de mandats présentées par le Service canadien du renseignement de sécurité (SCRS) dans le cadre d'enquêtes sur deux ensembles distincts d'activités au sujet desquelles il pourrait exister des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada.

Les demandes se rapportaient à la capacité du SCRS d'obtenir des données d'identification de base (DIB) auprès des fournisseurs de services de communication (FSC). Les DIB, qui comprennent le nom et l'adresse de l'abonné, seraient

accounts of individuals whose telephone number or other electronic identifiers may come to CSIS's attention in the course of its investigations. In the absence of judicial pre-authorization, CSIS cannot obtain BII without contravening a person's right to be secure against unreasonable search or seizure, pursuant to section 8 of the *Canadian Charter of Rights and Freedoms*. The Court advised CSIS in *X (Re)*, 2016 FC 1105, [2017] 2 F.C.R. 396 (*X (Re)*) that broad authorizations of the type being sought in the present proceedings would no longer be granted until they were the subject of further exchanges between the Court and CSIS. Given the position taken by the Court in *X (Re)* with respect to broad authorizations to obtain access to subscriber data, CSIS's application in [***] was separated into two phases. The first phase focused on warrant powers that CSIS sought in respect of individuals who are subjects of its investigation into the threat to the security of Canada. The Court issued the warrants that were sought at that time. The second phase concerned two additional authorizations that CSIS sought to add to three of the warrants that the Court issued in the initial phase. The first of those authorizations was very broad and would enable CSIS to obtain BII in respect of any communications account corresponding to any telephone number or electronic identifier that CSIS may identify during its investigation into Islamist terrorism, where a chief within CSIS determines that BII will assist CSIS to advance its investigation. The second type of authorization was narrower, and would enable CSIS to obtain BII in respect of communications accounts identified pursuant to its review of specifically defined information obtained in relation to named individuals.

At issue was whether the Court can authorize CSIS to obtain BII in respect of: (1) communications accounts corresponding to telephone numbers or electronic identifiers that may in the future come to its attention in the course of its investigations; (2) communications accounts identified pursuant to its review of specifically defined information obtained in relation to certain individuals; and (3) a communications account that corresponds to a telephone number or an electronic identifier where a "chief" within CSIS determines that the account was identified during its investigation, and that the BII would assist CSIS in its investigation.

Held, the application in [***] should be dismissed; the application in [***] should be dismissed in part.

The broad authorization that CSIS sought in the first type of proposed amendments to three of the warrants that were issued in the first phase could not be provided. Privacy interests are held by individuals and corporations. The words "the

liées à des comptes de communications de personnes dont le numéro de téléphone ou d'autres identificateurs électroniques pourraient éventuellement attirer l'attention du SCRS lors de ses enquêtes. En l'absence d'une autorisation judiciaire préalable, le SCRS ne peut pas obtenir les DIB sans enfreindre le droit d'une personne d'être protégée contre les fouilles, les perquisitions ou les saisies abusives garanti par l'article 8 de la *Charte canadienne des droits et libertés*. Dans la décision *X (Re)*, 2016 CF 1105, [2017] 2 R.C.F. 396 (*X (Re)*), la Cour a avisé le SCRS qu'elle n'accorderait plus d'autorisations du type vaste demandé en l'espèce avant qu'elles ne fassent l'objet d'autres échanges entre la Cour et le SCRS. Compte tenu de la décision de la Cour dans *X (Re)* en ce qui a trait aux vastes autorisations d'obtenir des données sur l'abonné, la demande du SCRS dans le dossier [***] a été divisée en deux étapes. La première portait sur les mandats que demandait le SCRS contre des personnes faisant l'objet de son enquête sur la menace qui pesait sur la sécurité du Canada. La Cour a décerné les mandats demandés. La deuxième étape de l'instance portait sur deux autres autorisations que le SCRS voulait ajouter à trois des mandats décernés par la Cour lors de l'étape initiale. La première de ces autorisations était très générale et permettrait au SCRS d'obtenir des DIB concernant tout compte de communication correspondant à tout numéro de téléphone ou identificateur électronique que le SCRS pourrait découvrir dans le cadre de son enquête sur le terrorisme islamiste, lorsqu'un chef au SCRS détermine que ces DIB permettraient au SCRS de faire progresser son enquête. L'autorisation du second type avait une portée plus circonscrite et elle autoriserait le SCRS à obtenir des DIB liées à des comptes de communications qu'il a découvert en examinant des informations clairement définies ayant trait à des personnes identifiées par leur nom.

Il s'agissait de déterminer si la Cour peut autoriser le SCRS à obtenir des DIB liées à 1) des comptes de communication correspondant à des numéros de téléphone ou à des identificateurs électroniques qui pourront éventuellement attirer son attention lors de ses enquêtes; 2) des comptes de communications qu'il a découverts en examinant des informations clairement définies ayant trait à certaines personnes; et 3) un compte de communications correspondant à un numéro de téléphone ou à un identificateur électronique lorsqu'un « chef » au sein du SCRS détermine que ce compte a été découvert lors d'une enquête et que les DIB faciliteraient cette enquête.

Jugement : la demande dans le dossier [***] doit être rejetée; la demande dans le dossier [***] doit être rejetée en partie.

La vaste autorisation demandée par le SCRS dans la première catégorie de modifications qu'il souhaite faire apporter à trois des mandats décernés à la première étape de l'instance ne pouvait être accordée. Le droit au respect de la vie privée est

identity of the person, if known" in paragraph 21(2)(d) of the *Canadian Security Intelligence Service Act* (Act) reflects the practical reality that CSIS may not know, at the time it applies for a warrant, the identity of an ascertainable person whose communication is proposed to be intercepted, or who has possession of the information, record, document or other thing proposed to be obtained under the warrant, as contemplated by that provision. Except in exceptional circumstances that were not demonstrated to exist in this case, CSIS cannot be prospectively authorized to obtain BII in relation to communications accounts that may in the future come to its attention in the course of its investigations, where CSIS has not yet described and established their specific nexus with those investigations. This is because persons who are responsible for authorizing the use of intrusive powers are required to consider the impact of such intrusion on the specific "subject of the search". In other words, an assessment must be made of the context of each "particular situation", and its impact on "the individual". A balancing analysis must be conducted between the interests of the state and the interests of the specific individual whose privacy interests are at issue. Where a "class of persons" whose privacy interests may be encroached upon can be described in a manner that enables the Court to clearly understand the nexus between those persons and the threat-related activities that are the focus of a CSIS investigation, the balancing analysis can comfortably be conducted in respect of those persons. This is contemplated by the references to "class of persons" in paragraphs 21(2)(e) and 21(4)(c) of the Act. The need to consider the interests of the specific individual or class of individuals whose privacy interests are engaged is reinforced by three additional requirements: (1) the requirement to assess the individual's subjective expectation of privacy, (2) the requirement that CSIS's powers to investigate activities that pose threats to the security of Canada must be "strictly controlled", and (3) the requirement to consider "the totality of the circumstances". The last requirement implies that the interests of the specific person(s) whose privacy interests are at stake must be taken into account. It is difficult to imagine how the totality of the circumstances would not involve an assessment of the privacy interests of the very individual whose interests would be engaged if CSIS were to obtain BII from a CSP. It is not necessary for warrants that authorize CSIS to obtain BII to associate the communications accounts in question with named individuals. CSIS may know sufficient information about the individual to provide the Court with reasonable grounds to believe that obtaining the BII of a particular communications accounts is required to advance its investigation. It will remain open to CSIS, when it does not have the telephone number or other identifier at the time of a warrant application for authorization to obtain BII, to describe the telephone number or identifier in a way that enables the Court to satisfy itself of the matters referred to in paragraphs 21(2)(a) and (b) of the Act. With respect to the reasonable grounds to believe referred to

l'apanage des personnes et des personnes morales. Le segment «l'identité de la personne, si elle est connue» à l'alinéa 21(2)d) de la *Loi sur le Service canadien du renseignement de sécurité* (Loi) reflète le fait qu'en pratique, lorsqu'il présente une demande de mandat, le SCRS peut ne pas connaître l'identité de la personne vérifiable dont il propose d'intercepter les communications ou qui détient des informations, des documents ou des objets qu'il entend obtenir, comme le précise cette disposition. Sauf en des circonstances exceptionnelles dont l'existence n'a pas été démontrée en l'espèce, le SCRS ne peut être autorisé, de manière prospective, à obtenir les DIB liées à des comptes de communication qui pourraient attirer son attention dans le cadre d'enquêtes, s'il n'a pas encore décrit et établi de lien précis entre les DIB et les enquêtes en question. En effet, les personnes chargées d'autoriser le recours à des pouvoirs envahissants doivent tenir compte des répercussions de l'intrusion sur l'«objet de la fouille». Autrement dit, il est nécessaire d'évaluer le contexte de chaque situation et son incidence sur « la personne ». Il y a lieu d'atteindre un équilibre entre les intérêts de l'État et ceux de la personne même dont le droit au respect de sa vie privée est en jeu. Cet exercice de pondération peut se faire aisément lorsqu'il s'agit d'une « catégorie de personnes », dont le droit au respect de la vie privée peut être enfreint, et dont il est possible de décrire de manière à ce que la Cour comprenne très bien le lien qui peut être établi entre elles et les activités liées à la menace qui font l'objet d'une enquête du SCRS. C'est ce qui est visé par l'expression «catégorie de personnes» aux alinéas 21(2)e) et 21(4)c) de la Loi. Trois autres exigences renforcent la nécessité de tenir compte des intérêts des personnes ou des catégories de personnes dont le droit au respect de la vie privée est en jeu : 1) il est nécessaire d'évaluer l'attente subjective de la personne en matière de vie privée; 2) il est nécessaire d'assujettir à des «contrôles sévères» les pouvoirs dont jouit le SCRS pour enquêter sur des activités qui constituent des menaces envers la sécurité du Canada; 3) il est nécessaire de prendre en considération «l'ensemble des circonstances». Cela signifie qu'il faut tenir compte des intérêts de la personne ou des personnes en particulier dont le droit au respect de la vie privée est en jeu. Il est difficile d'imaginer comment l'ensemble des circonstances n'inclurait pas une évaluation du droit au respect de la vie privée de la personne ou des personnes elles-mêmes dont les intérêts seraient touchés si le SCRS obtenait des DIB auprès d'un FSC. Il n'est pas nécessaire que les mandats autorisant le SCRS à obtenir des DIB établissent un lien entre les comptes en question et des personnes nommées. Le SCRS peut disposer d'assez d'informations sur elles pour fournir à la Cour des motifs raisonnables de croire qu'il lui faut obtenir les DIB liées à un compte pour faire progresser son enquête. Lorsqu'il ne dispose pas du numéro de téléphone ou d'un autre identificateur au moment de demander un mandat l'autorisant à obtenir des DIB, le SCRS a toujours la possibilité de le décrire d'une manière qui permet à la Cour d'être convaincue de la présence

in paragraph 21(2)(a), it may suffice to provide the Court with an understanding of the nexus between CSIS's investigation and the specific individual whose privacy interests would be intruded upon. For example, it may suffice to describe a telephone number in terms of a future communication by a subject of investigation. This would meet the requirements of both section 21 of the Act and section 8 of the Charter, and would strike an appropriate balance between the public interest in affording CSIS with a reasonable degree of flexibility to fulfill its statutory mandate, and the privacy interests of yet-to-be identified individuals whose BII would be obtained under a warrant.

It was apparent that the appropriate balance was not met with the first type of amendments, i.e. the broad authorization, that were proposed to three of the warrants. CSIS did not provide the Court with any understanding whatsoever of the specific nexus between (i) the as-yet-to be discovered telephone numbers and electronic identifiers in respect of which BII would be sought, and (ii) CSIS's investigations. The loosely defined "nexus" was simply too broad and nebulous. The Court could not be satisfied that such BII information was required to enable CSIS to investigate the threat to the security of Canada posed by Islamist terrorism, as contemplated by paragraph 21(2)(a) of the Act. The language of the proposed warrant did not enable the Court to know with which of the identified groups a communications account would be associated. This did not permit the Court to have a sufficient sense of the nexus between the identified threat-related activities of Islamist terrorism and the individual whose privacy rights would be encroached upon to be considered "reasonable" within the meaning of section 8 of the Charter.

The second group of requested amendments to three of the warrants to enable CSIS to obtain BII in respect of communications accounts of third parties that may be identified pursuant to its review of the information of the identified individuals was granted. There was concern, however, of the potentially large number of third parties whose BII may be obtained by CSIS. Some conditions would be necessary to address these issues.

As to the third issue raised in the applications, the proposed authorizations would impermissibly delegate to a person holding the position of "chief" within CSIS a function that must be performed by a designated judge of the Court. Persons holding the position of "chief" within CSIS would, in essence, make the determination of whether the grounds that must be established before a specific individual's privacy interests can be intruded upon, have been met. Only a designated judge can make such determinations. An authorization for CSIS to engage in what amounts to a search that is more than minimally invasive must be given by an entirely neutral and impartial

des éléments prévus aux alinéas 21(2)a) et b) de la Loi. En ce qui a trait aux motifs raisonnables de croire dont il est question à l'alinéa 21(2)a), il pourrait être suffisant d'expliquer à la Cour le lien qui unit l'enquête du SCRS et la ou les personnes dont le droit au respect de la vie privée sera enfreint. À titre d'exemple, il peut suffire de mentionner qu'un numéro de téléphone pourrait être utilisé par une cible. Cela satisferait aux exigences de l'article 21 de la Loi et de l'article 8 de la Charte, et ferait état d'un juste équilibre entre l'intérêt public, car le SCRS s'y verrait accorder un degré de souplesse raisonnable dans l'exécution de son mandat, et le droit au respect de la vie privée des personnes toujours non-identifiées dont le Service obtiendrait les DIB en vertu d'un mandat.

Il était apparent que le juste équilibre n'avait pas été atteint en ce qui concerne les modifications du premier type — à savoir la vaste autorisation — proposées à trois des mandats décernés dans le dossier. Le SCRS n'a fourni à la Cour aucune explication lui permettant de comprendre le lien précis entre i) les numéros de téléphones et identificateurs électroniques qu'il pourrait découvrir, pour lesquels il demanderait d'obtenir les DIB, et ii) ses enquêtes. Le « lien », vaguement défini, avait tout simplement une portée excessive et manquait de clarté. La Cour n'a pu être convaincue que le SCRS avait besoin de ces DIB pour enquêter sur la menace que le terrorisme islamiste fait peser sur la sécurité du Canada, conformément à l'alinéa 21(2) a) de la Loi. Le libellé du mandat proposé n'a pas permis à la Cour de savoir auxquels de ces groupes un compte de communications serait associé. Cela n'a pas permis à la Cour d'assez bien constater le lien entre les activités liées à la menace que constitue le terrorisme islamiste et la personne dont les droits en matière de vie privée seraient enfreints pour qu'elle le considère « non abusif » au sens de l'article 8 de la Charte.

La deuxième catégorie d'amendements demandés à trois des mandats décernés de façon à permettre au SCRS d'obtenir les DIB ayant trait à tout compte de tiers pouvant être identifié à la suite de son examen de l'information des personnes identifiées a été accordée. Le nombre potentiellement élevé de tierces parties dont les DIB pourraient être obtenues par le SCRS suscitait cependant des préoccupations. Il s'avérerait nécessaire d'imposer des conditions pour répondre à ces préoccupations.

En ce qui concerne la troisième question soulevée dans les demandes, les autorisations proposées auraient pour effet de déléguer de façon inacceptable au titulaire d'un poste de « chef » au SCRS une fonction qui relève exclusivement d'un juge désigné de la Cour. Essentiellement, le titulaire d'un poste de « chef » au SCRS déterminerait si les motifs qui doivent être établis avant qu'il soit possible d'enfreindre le droit d'une personne au respect de sa vie privée l'ont bel et bien été. Seul un juge désigné peut ainsi trancher ces questions. Pour mener une activité assimilable à une fouille ou à une perquisition plus que minimalement envahissante, le SCRS doit en recevoir

arbiter who is capable of acting judicially in balancing the interests of the state against those of the individual. An individual holding the position of chief within CSIS is not capable of acting judicially in this regard. All of the foregoing was rendered even more troublesome by (i) the very broad definition of Islamist terrorism that CSIS has adopted, (ii) the fact that CSIS would indefinitely retain all of the BII that it seeks to obtain under the requested authorizations, and (iii) that there would be no limit on CSIS's ability to share that information with foreign intelligence agencies.

l'autorisation par un arbitre tout à fait neutre et impartial qui est en mesure d'exercer des fonctions judiciaires en établissant un équilibre entre les intérêts de l'État et ceux de la personne. Le titulaire d'un poste de chef au SCRS n'est pas en mesure d'exercer des fonctions judiciaires à cet égard. Ce qui précède était encore plus problématique en raison i) de la définition très vaste de terrorisme islamiste que le SCRS a adoptée, ii) du fait que le SCRS pourrait conserver indéfiniment toutes les DIB obtenues au titre des autorisations demandées et iii) du fait que le SCRS pourrait, sans aucune limite, communiquer ces informations à des services de renseignement étrangers.

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, 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. 2 « menaces envers la sécurité du Canada », 12, 21.

CASES CITED

APPLIED:

R. v. Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212; *Hunter et al. v. Southam Inc.*, [1984] 2 S.C.R. 145, (1984), 55 A.R. 291.

CONSIDERED:

X (Re), 2016 FC 1105, [2017] 2 F.C.R. 396; *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38, [2008] 2 S.C.R. 326; *R. v. Chehil*, 2013 SCC 49, [2013] 3 S.C.R. 220; *R. v. Thompson*, [1990] 2 S.C.R. 1111, (1990), 73 D.L.R. (4th) 596.

REFERRED TO:

R. v. Gomboc, 2010 SCC 55, [2010] 3 S.C.R. 211; *Goodwin v. British Columbia (Superintendent of Motor Vehicles)*, 2015 SCC 46, [2015] 3 S.C.R. 250; *Baron v. Canada*, [1993] 1 S.C.R. 416, (1993), 99 D.L.R. (4th) 350; *R. v. Rodgers*, 2006 SCC 15, [2006] 1 S.C.R. 554; *Atwal v. Canada*, [1988] 1 F.C. 107, (1987), 28 Admin. L.R. 92 (C.A.); *R. v. Poirier*, 2016 ONCA 582 (CanLII), [2016] O.J. No. 3873 (QL); *R. v. Noseworthy* (1997), 33 O.R. (3d) 641, 116 C.C.C. (3d) 376 (C.A.); *R. v. TELUS Communications Co.*, 2013 SCC 16, [2013] 2 S.C.R. 3; *Canadian Security Intelligence Act (Re)*, [1998] 1 F.C. 420, (1997), 10 C.R. (5th) 273 (T.D.); *Grabowski v. The Queen*, [1985] 2 S.C.R. 434, (1985), 22 D.L.R. (4th) 725; *R. v. Généreux*, [1992] 1 S.C.R. 259, (1992), 88 D.L.R. (4th) 110.

JURISPRUDENCE CITÉE

DÉCISIONS APPLIQUÉES :

R. c. Spencer, 2014 CSC 43, [2014] 2 R.C.S. 212; *Hunter et autres c. Southam Inc.*, [1984] 2 R.C.S. 145.

DÉCISIONS EXAMINÉES :

X (Re), 2016 CF 1105, [2017] 2 R.C.F. 396; *Charkaoui c. Canada (Citoyenneté et Immigration)*, 2008 CSC 38, [2008] 2 R.C.S. 326; *R. c. Chehil*, 2013 CSC 49, [2013] 3 R.C.S. 220; *R. c. Thompson*, [1990] 2 R.C.S. 1111.

DÉCISIONS CITÉES :

R. c. Gomboc, 2010 CSC 55, [2010] 3 R.C.S. 211; *Goodwin c. Colombie-Britannique (Superintendent of Motor Vehicles)*, 2015 CSC 46, [2015] 3 R.C.S. 250; *Baron c. Canada*, [1993] 1 R.C.S. 416; *R. c. Rodgers*, 2006 CSC 15, [2006] 1 R.C.S. 554; *Atwal c. Canada*, [1988] 1 C.F. 107 (C.A.); *R. v. Poirier*, 2016 ONCA 582 (CanLII), [2016] O.J. nº 3873 (QL); *R. v. Noseworthy* (1997), 33 O.R. (3d) 641, 116 C.C.C. (3d) 376 (C.A.); *R. c. Société TELUS Communications*, 2013 CSC 16, [2013] 2 R.C.S. 3; *Loi sur le Service canadien du renseignement de sécurité (Re)*, [1998] 1 C.F. 420 (1re inst.); *Grabowski c. La Reine*, [1985] 2 R.C.S. 434; *R. c. Généreux*, [1992] 1 R.C.S. 259.

AUTHORS CITED

Canada. Senate. Report of the Special Senate Committee on the Canadian Security Intelligence Service. *Delicate Balance: A Security Intelligence Service in a Democratic Society*. Ottawa: Minister of Supply and Services Canada, November 3, 1983.

APPLICATIONS concerning requests by the Canadian Security Intelligence Service for warrants in relation to its investigation of two separate groups of activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. Application in [***] dismissed; application in [***] dismissed in part.

APPEARANCES

Karla Unger, *Gordon Kirk* and *Nathalie Benoit* for Department of Justice, National Security Litigation and Advisory Group.
Gordon Cameron and *Owen Rees* as *amici curiae*.

SOLICITORS OF RECORD

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

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

Crampton C.J.:

Table of Contents

DOCTRINE CITÉE

Canada. Sénat. Rapport du Comité sénatorial spécial du Service canadien du renseignement de sécurité. *Équilibre délicat : Un Service du renseignement de sécurité dans une société démocratique.* Ottawa : Ministre des Approvisionnements et Services Canada, 3 novembre 1983.

DEMANDES concernant les demandes de mandats présentées par le Service canadien du renseignement de sécurité dans le cadre d'enquêtes sur deux ensembles distincts d'activités au sujet desquelles il pourrait exister des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada. Demande dans le dossier [***] rejetée; demande dans le dossier [***] rejetée en partie.

ONT COMPARU :

Karla Unger, *Gordon Kirk* et *Nathalie Benoit* pour le ministère de la Justice, Groupe litiges et conseils en sécurité nationale.
Gordon Cameron et *Owen Rees* à titre d'*amici curiae*.

AVOCATS INSCRITS AU DOSSIER

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

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

Le juge en chef Crampton :

Table des Matières

I. Introduction

[1] These applications concern requests by the Canadian Security Intelligence Service (CSIS) for warrants in relation to its investigation of two separate groups of activities that I am satisfied may on reasonable grounds be suspected of constituting threats to the security of Canada. CSIS has defined the first group in terms of "Islamist terrorism". Those activities are the focus of the application in Court file [***] The second group consists of certain activities engaged in by [***]

I. Introduction

[1] Les demandes de mandats dont il est question en l'espèce ont été présentées par le Service canadien du renseignement de sécurité (SCRS ou Service) dans le cadre d'enquêtes sur deux ensembles distincts d'activités au sujet desquels je suis convaincu qu'il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada. Le SCRS a attribué au premier ensemble le générique « terrorisme islamiste ». Ces activités font l'objet de la demande au

Those activities are described in materials filed by CSIS in Court file [***]

[2] The applications raise three issues pertaining to CSIS's request to be able to obtain basic identifying information (BII) from communications services providers (CSPs). That information would be obtained in respect of communications accounts of individuals whose telephone number, [***] or other electronic identifiers may in the future come to CSIS's attention in the course of its investigations of the activities described above. BII consists of the name and address of a subscriber to a communications account, [*** [The information relating to IP addresses in certain circumstances] ***]

[3] The Attorney General concedes that in the absence of judicial pre-authorization, CSIS cannot obtain BII in respect of a person's communications account without contravening that person's right to be secure against unreasonable search or seizure, pursuant to section 8 of the *Canadian Charter of Rights and Freedoms*, being Part I of the *Constitution Act, 1982*, Schedule B, *Canada Act 1982*, 1982, c, 11 (U.K.) [R.S.C., 1985, Appendix II, No. 44] (the Charter).

[4] Accordingly, the focus of these applications has been upon a broad BII authorization that CSIS is seeking in each of [***] and [***], a narrower BII authorization that it is seeking in [***] alone, and a delegation issue that exists with respect to the first of those two authorizations. More specifically, the three issues raised by these applications are as follows:

i. Can the Court authorize CSIS to obtain BII in respect of communications accounts corresponding to telephone numbers or electronic identifiers that *may in the future* come to its attention in the course of its investigations, where CSIS has not described and established their specific nexus to those investigations? (This is a common issue in both applications.)

dossier de la Cour [***] Le deuxième ensemble comprend certaines activités menées par [***] Ces activités sont décrites dans les documents déposés par le SCRS au dossier de la Cour [***]

[2] Ces demandes soulèvent trois questions relatives à l'autorisation demandée par le SCRS d'obtenir, auprès des fournisseurs de services de communication (FSC), des données d'identification de base (DIB) liées à des comptes de communications de personnes dont le numéro de téléphone, [***] ou d'autres identificateurs électroniques peuvent éventuellement attiré l'attention du SCRS lors de ses enquêtes sur les activités décrites plus haut. Les DIB comprennent le nom et l'adresse de l'abonné à un compte de communications, [***[Ainsi que l'information concernant les adresses IP dans certaines circonstances]***]

[3] La procureure générale admet qu'en l'absence d'une autorisation judiciaire préalable, le SCRS ne peut pas obtenir les DIB liées au compte de communication d'une personne sans enfreindre son droit d'être protégée contre les fouilles, les perquisitions ou les saisies abusives garanti par l'article 8 de la *Charte canadienne des droits et libertés*, qui constitue la partie I de la *Loi constitutionnelle de 1982*, annexe B, *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.) [L.R.C. (1985), appendice II, nº 44] (Charte).

[4] En bref, le point central de ces demandes consiste en une autorité générique pour les DIB que le SCRS voudrait obtenir pour chacun des dossiers [***] et [***] puis une demande plus ciblée pour une autorisation au dossier [***] seulement et finalement une question de délégation pour la première de ces deux autorités. Plus précisément, voici les trois questions soulevées en l'espèce.

i. La Cour peut-elle autoriser le SCRS à obtenir des DIB liées à des comptes de communication correspondant à des numéros de téléphone ou à des identificateurs électroniques qui pourront éventuellement attirer son attention lors de ses enquêtes, lorsque le SCRS n'a ni décrit ni établi leur lien précis avec ces enquêtes? (Cette question est commune aux deux dossiers).

ii. Can the Court authorize CSIS to obtain BII in respect of communications accounts identified pursuant to its review of specifically defined information obtained in relation to [***] named individuals and [***] additional individuals who have been identified by [***] (This issue arises only in [***]

iii. Can the Court authorize an employee of CSIS to obtain BII in respect of a communications account that corresponds to a telephone number or an electronic identifier, where a "chief" within CSIS determines that the account was identified during its investigation, and that the BII would assist CSIS in its investigation? (This is a common issue in both applications.)

[5] In my view, the Court cannot provide the first of the requested authorizations described above. It does not meet the basic requirements for authorizing intrusive activity by the state.

[6] Before the Court may authorize CSIS to obtain BII or to exercise other intrusive search powers, the Court must have an understanding of the nexus between CSIS's investigation and the specific persons or class of persons whose privacy rights would be engaged. Only then can the Court assess whether the specific privacy interests of those persons must give way to the interests of the state in obtaining the information in question. In addition, CSIS must satisfy the requirements for obtaining a warrant set forth in subsections 21(2) and (3) of the *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23 (the Act), in respect of such person or class of persons.

[7] The Court has not been provided with that required understanding of the nexus described above in respect of the broad BII authorization that CSIS is seeking in both [***] and [***] Indeed, the Court has not been provided with any sense whatsoever as to how the individual or class of individuals whose privacy interests would be intruded upon would be linked to its investigations.

ii. La Cour peut-elle autoriser le SCRS à obtenir des DIB liées à des comptes de communications qu'il a découverts en examinant des informations clairement définies ayant trait à [***] personnes identifiées par leur nom et à [***] autres personnes ciblées en fonction [***] (Cette question n'est pertinente qu'au dossier [***])

iii. La Cour peut-elle autoriser un employé du SCRS à obtenir les DIB liées à un compte de communications correspondant à un numéro de téléphone ou à un identificateur électronique lorsqu'un « chef » au sein du SCRS détermine que ce compte a été découvert lors d'une enquête et que les DIB permettraient de faire progresser cette enquête? (Cette question est commune aux deux dossiers.)

[5] À mon avis, la Cour ne peut pas accorder la première des autorisations susmentionnées, car elle ne satisfait pas aux exigences de base nécessaires pour autoriser l'État à mener une activité envahissante.

[6] Avant de pouvoir autoriser le SCRS à obtenir des DIB ou à exercer d'autres pouvoirs lui permettant de mener des fouilles ou des perquisitions envahissantes, la Cour doit comprendre le lien entre l'enquête du SCRS et les personnes ou les catégories de personnes dont les droits en matière de vie privée pourraient être enfreints. Ce n'est qu'à ce moment que la Cour peut établir si le droit de ces personnes au respect de leur vie privée doit céder la place aux intérêts de l'État quant à l'obtention des informations. De plus, pour obtenir un mandat, le SCRS doit satisfaire aux exigences figurant aux paragraphes 21(2) et (3) de la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. (1985), ch. C-23 (Loi sur le SCRS) pour chacune des personnes ou des catégories de personnes.

[7] La Cour n'a pas obtenu l'information nécessaire pour lui permettre de bien comprendre ce lien en ce qui a trait aux vastes autorisations que le Service recherche dans les dossiers [***] et [***] Qui plus est, la Cour n'a aucune idée du lien que pourrait avoir la personne ou la catégorie de personnes dont les droits en matière de vie privée pourraient être enfreints par ces enquêtes.

[8] With respect to the second, narrower, BII authorization that CSIS has requested in [***] alone, I am satisfied that the required nexus has been described and established by CSIS. This is because that authorization is confined to telephone numbers or electronic identifiers that CSIS may identify in the course of reviewing information that specifically relates to [***] identified individuals who are subjects of investigation. [***] of those individuals have been identified by name, while the remaining [***] have been identified by reference to [***]

[9] The information that relates to those individuals includes BII [***] information will reveal the [***] identifiers [***]

[10] I am satisfied that there are reasonable grounds to believe that anyone with whom those [***] individuals has been in contact may be able to provide information that will assist CSIS to advance its investigation into the threat-related activities [***] that it has identified. For this reason, I am satisfied that there are reasonable grounds to believe that CSIS requires the BII relating to the communications accounts that correspond to the telephone numbers and electronic identifiers of those third parties, to advance its investigation. Without being able to obtain that BII, [***]

[11] Although the Court has not been provided with the names of [***] of those individuals, the Court has been provided with sufficient information regarding [***] to be able to conduct the assessment required by section 8 of the Charter. That assessment is whether the specific privacy interests of those individuals must give way to the interests of the state in obtaining the BII that CSIS requires to advance its investigation into the identified threat-related activities [***]

[12] At the time it issues a warrant authorizing the exercise of powers that would intrude upon the privacy interests of one or more individuals or classes of persons, the Court does not need to know the specific names of those individuals or persons within the class. However, the Court needs to have a sufficient understanding of the nexus between CSIS's investigation and the specific persons or class of persons whose privacy interests would be intruded upon. The Court has been provided with that

[8] En ce qui concerne la deuxième autorisation, plus ciblée, relative aux DIB demandée par le SCRS au dossier [***] je suis convaincu que le SCRS a décrit et établi ce lien. En effet, ces autorisations concernent seulement des numéros de téléphone ou des identificateurs électroniques que le SCRS peut découvrir en examinant des informations concernant précisément [***] personnes identifiées qui font l'objet d'une enquête. [***] d'entre elles sont connues par leur nom, les [***] autres le sont [***]

[9] Les informations relatives à ces personnes comprennent les DIB [***] Elles révéleront entre autres [***]

[10] Je suis convaincu qu'il existe des motifs raisonnables de croire que tout individu avec qui ces [***] personnes ont été en contact peut fournir des informations qui aideraient le SCRS à faire avancer son enquête sur les activités liées à la menace [***] Pour cette raison, je suis convaincu qu'il existe des motifs raisonnables de croire que le SCRS a besoin des DIB liées aux comptes de communications correspondant aux numéros de téléphone et aux identificateurs électroniques de ces tiers pour progresser dans son enquête. S'il n'est pas en mesure d'obtenir ces DIB, [***]

[11] Bien qu'elle ne connaisse pas le nom de [***] de ces personnes, la Cour a reçu suffisamment d'informations sur [***] pour effectuer l'évaluation requise à l'article 8 de la Charte, qui vise à établir si le droit de ces personnes au respect de leur vie privée doit céder la place aux intérêts de l'État quant à l'obtention des DIB dont le SCRS a besoin pour faire progresser son enquête sur les activités liées à la menace [***]

[12] Pour décerner un mandat autorisant l'exercice de pouvoirs qui enfreindraient le droit d'une ou de plusieurs personnes ou catégories de personnes au respect de leur vie privée, la Cour n'a pas besoin de connaître le nom précis de ces personnes ou des personnes au sein de la catégorie. Par contre, la Cour doit avoir une compréhension suffisante du lien entre l'enquête du SCRS et les personnes ou catégories de personnes dont le droit au respect de leur vie privée pourrait être enfreint. La Cour

understanding in respect of the [***] individuals [***] have been described to the Court, as well as in respect of the third parties who CSIS may discover have been in contact with those individuals, or with the [***] other individuals who have been identified by name.

[13] Where the Court is not able to conduct, in advance, the assessment required by section 8 of the Charter in respect of the specific individuals or class of individuals whose privacy interests would be engaged by CSIS's access to their BII, CSIS will need to return to the Court each time it identifies additional telephone numbers or electronic identifiers in respect of which it wishes to obtain BII from a CSP. At that time, CSIS will have to establish a sufficient nexus between the telephone number or other identifier in question and its investigations to satisfy the Court that there are reasonable grounds to believe that CSIS requires the BII of the corresponding communications account to advance those investigations.

[14] The third issue raised in these proceedings is whether the Court can authorize any employee of CSIS to obtain BII in respect of a communications account, where an individual holding the position of chief within CSIS makes certain determinations. In my view, the Court cannot do so, because this would amount to the delegation of functions that must be exercised by the Court itself. Although the Court may delegate to CSIS certain types of decisions with respect to the execution of its warrants, it cannot delegate the determination of which specific communications accounts will be the subject of requests to CSPs for BII. To the extent that this determination requires an assessment of whether the privacy interests of the persons in question must give way to the interests of CSIS in obtaining the BII in question, this is a function that must be performed by the Court.

[15] I recognize that the conclusions I have reached in respect of the first and third issues discussed above may well impose a potentially significant additional burden on CSIS. I also recognize that this may give rise to additional costs and delays associated with obtaining BII authorizations in relation to telephone numbers or electronic identifiers that may come to CSIS's attention dur-

comprend ce lien pour les [***] personnes dont [***] ont été décrits ainsi que pour les tiers qui peuvent avoir été en contact avec ces personnes ou avec les [***] personnes connues par leur nom.

[13] Si la Cour n'est pas en mesure d'effectuer à l'avance l'évaluation relative à l'article 8 de la Charte pour les personnes ou catégories de personnes dont le droit au respect de la vie privée pourrait être enfreint si le SCRS a accès à leurs DIB, le SCRS devra s'adresser de nouveau à elle chaque fois qu'il trouve d'autres numéros de téléphone ou identificateurs électroniques à propos desquels il désire obtenir les DIB auprès d'un FSC. Le SCRS devra alors établir un lien suffisant entre le numéro de téléphone ou l'identificateur électronique et son enquête afin de convaincre la Cour qu'il existe des motifs raisonnables de croire que les DIB de ces comptes de communication sont nécessaires pour faire progresser son enquête.

[14] La troisième question soulevée en l'espèce concerne la possibilité que la Cour autorise tout employé du SCRS à obtenir les DIB liées un compte de communication si une personne occupant un poste de chef au SCRS prend certaines décisions. Selon moi, une telle autorisation ne peut être accordée, car cela signifierait que sont déléguées des fonctions qui doivent être exercées par la Cour elle-même. Bien que la Cour puisse déléguer au SCRS le pouvoir de prendre certaines décisions relatives à l'exécution des mandats, elle ne peut pas lui permettre ainsi de déterminer quels comptes de communication en particulier feront l'objet d'une demande d'obtention de DIB auprès d'un FSC. Dans la mesure où elle exige d'évaluer si le droit des personnes visées au respect de leur vie privée, qui pourrait être enfreint, doit laisser place aux intérêts du SCRS quant à l'obtention des DIB, cette décision doit être prise par la Cour.

[15] Je reconnais que les conclusions auxquelles je suis arrivé en ce qui a trait à la première et troisième des questions soulevées en l'espèce peuvent facilement ajouter un fardeau important pour le SCRS. Je reconnais également qu'elles peuvent entraîner l'accroissement des coûts et des délais relatifs aux demandes d'autorisations d'obtenir des DIB liées aux numéros de téléphone

ing the course of its investigations into Islamist terrorism and the threat-related activities [***] Given the adverse implications that the potential delays, in particular, may have for CSIS's ability to investigate threat-related activities, the Court will remain open to considering alternate approaches that are Charter compliant.

[16] These reasons for judgment are being issued contemporaneously with my reasons for judgment in [***] which concerns CSIS's use of cellular-site simulator (CSS) technology to capture the identifying characteristics of an individual's mobile device(s) without a warrant [***]

II. Background

[17] This Court has been authorizing CSIS to obtain subscriber and similar information from CSPs in respect of accounts corresponding to telephone numbers and electronic identifiers for many years. In most cases, such authorizations have been provided in respect of the [***] identifiers of known individuals who are subjects of investigation, or of third parties with whom such individuals may communicate. However, in some cases the Court has also authorized CSIS to obtain such information in respect of communications accounts of known, but still unidentified, individuals. For example, such authorizations have been provided in respect of individuals [***] The same is true with respect to the [***] identifiers of third parties with whom such known, but as yet unidentified, individuals have communicated, or may in the future communicate. Given that the [***] identifiers in question are not yet known at the time of the warrant application, they cannot be specified in the warrant.

[18] The types of authorizations described above have always been provided in warrants that have focused primarily upon named subjects of investigation, also known as "targets", and their involvement in particular threat-related activities. In some of those warrants, the Court also granted authorizations to obtain BII in relation to the communication accounts associated with [***] identifiers that CSIS identified during its investigation of the threat to the security of Canada in question,

et aux identificateurs électroniques qui pourraient attirer l'attention du SCRS lors de ses enquêtes sur le terrorisme islamiste et les activités liées à la menace [***] Puisque de possibles retards peuvent nuire à la capacité du SCRS d'enquêter sur des activités liées à la menace, la Cour demeure disposée à étudier d'autres approches qui seraient conforme aux exigences prévues à la Charte.

[16] Les présents motifs sont publiés en même temps que ceux qui ont trait à ma décision dans le dossier [***] qui porte sur l'utilisation, par le SCRS, de la technologie relative aux émulateurs de station de base (ESB) pour recueillir sans mandat les caractéristiques distinctives des appareils mobiles d'une personne. [***]

II. Contexte

[17] Depuis de nombreuses années, la Cour autorise le SCRS à obtenir, auprès des FSC, des informations sur l'abonné et des informations de même nature ayant trait à des comptes correspondant à [***] des identificateurs [***] Dans la plupart des cas, de telles autorisations ont été accordées pour les [***] de personnes connues qui font l'objet d'une enquête ou de tiers avec qui ces personnes pourraient communiquer. Toutefois, dans certains cas, la Cour a également autorisé le SCRS à obtenir de telles informations sur les comptes de communication de personnes connues, mais dont l'identité n'a pas encore été confirmée. Par exemple, de telles autorisations ont été accordées relativement à des personnes [***] Il en va de même pour [***] identificateurs [***] de tiers avec lesquels ces personnes, dont l'identité n'a pas été établie, ont communiqué ou communiqueront. Puisque les [***] identificateurs [***] ne sont pas encore connus au moment de demander un mandat, ils ne peuvent pas y être précisés.

[18] Les autorisations décrites plus haut sont toujours accordées dans des mandats qui portent principalement sur des cibles identifiées par leur nom en raison de leur participation à des activités précises liées à la menace. Dans certains de ces mandats, la Cour a également autorisé la collecte des DIB liées à des comptes de communications associés [***] aux identificateurs [***] que le SCRS a trouvés pendant son enquête sur la menace envers la sécurité du Canada, même lorsqu'il n'y avait

even where there was no direct link between such [***] identifiers and the target(s) identified in the warrants. There was simply the indirect link that existed by virtue of the fact that the [***] identifier would be identified in the future course of CSIS's investigation of the same threat to the security of Canada with which the named targets were also connected.

[19] However, beginning in 2013, some of my colleagues and I started to express concerns about granting the latter type of authorizations. After CSIS failed to avail itself of opportunities to address our concerns, we began to narrow the scope of the powers that we authorized. However, given that we did so in the context of individual applications for warrants, which sometimes had to be dealt with on an urgent basis, this gave rise to some inconsistencies in the language of the authorizations in question.

[20] As a result of the foregoing, Justice Noël advised CSIS in *X (Re)*, 2016 FC 1105, [2017] 2 F.C.R. 396 (*X (Re)*), at paragraph 230, that broad authorizations of the type being sought in the present proceedings, as well as authorizations to obtain [***] would no longer be granted by the Court until they were the subject of further exchanges between the Court and CSIS. Soon afterwards, in [***] I requested that CSIS endeavour to establish the legal basis for this Court to authorize such powers, in a separate proceeding. I explained that if CSIS could establish that legal basis, the powers in question could be authorized in a single application that would be made each year. Among other things, I considered that such an approach would avoid having to deal with CSIS's requests for such broad authorizations in the context of multiple different applications made over the course of a year, that are otherwise focused on named subjects of investigation. I made the foregoing request after declining to issue such an authorization.

[21] The application in [***] is CSIS's response to my request and to Justice Noël's decision. CSIS requested that I hear that application.

[22] Given the position taken by Justice Noël in *X (Re)* with respect to broad authorizations to obtain access to

pas de lien direct entre eux et la ou les cibles du mandat. Il n'y avait qu'un lien indirect qui s'expliquait par le simple fait que [***] l'identificateur [***] se retrouverait dans le cadre d'une enquête éventuelle portant sur la même menace à la sécurité du Canada pour laquelle les cibles nommées étaient également associées.

[19] Toutefois, depuis 2013, certains de mes collègues et moi avions commencé à soulever des préoccupations quant aux autorisations de ce dernier type. Puisque le SCRS ne s'est pas prévalu des possibilités qui lui ont été offertes de donner suite à nos préoccupations, nous avons commencé à réduire la portée des pouvoirs que nous accordons. Toutefois, puisque nous l'avons fait dans le contexte des demandes individuelles de mandats, qui devaient parfois être décernés de façon urgente, cela a entraîné un certain manque d'uniformité dans le libellé de ces autorisations.

[20] En raison de ce qui précède, dans la décision *X (Re)*, 2016 CF 1105, [2017] 2 R.C.F. 396 (*X (Re)*), au paragraphe 230, le juge Noël a avisé le SCRS que la Cour n'accorderait plus d'autorisations du type vaste demandé en l'espèce ni d'autorisations d'obtenir [***] avant qu'elles ne fassent l'objet d'autres échanges entre la Cour et le SCRS. Peu après, dans le dossier [***] j'ai demandé au SCRS de tenter d'établir le fondement juridique qui permettrait à la Cour de conférer de tels pouvoirs lors d'une instance distincte. J'ai expliqué que, si le SCRS pouvait établir ce fondement juridique, les pouvoirs en questions pourraient être accordés dans le cadre d'une seule demande présentée une fois par année. Entre autres, je crois qu'une telle approche permettrait d'éviter de traiter de telles demandes d'autorisations vastes que présenterait le SCRS pendant l'année dans le cadre de multiples demandes de mandat qui portent nommément sur des cibles. J'ai suggéré cette approche après avoir refusé d'accorder une telle autorisation.

[21] La demande présentée dans le dossier [***] est la réponse du Service à ma demande et à la décision du juge Noël. Le SCRS a demandé que j'en sois saisi.

[22] Compte tenu de la décision du juge Noël dans *X (Re)* en ce qui a trait aux vastes autorisations d'obtenir

subscriber data, CSIS's application in [***] was separated into two phases. The first phase focused on warrant powers that CSIS sought in respect of individuals who are subjects of its investigation into the threat to the security of Canada posed by [***] That phase of the proceeding took place in February of this year, and was based on affidavit evidence provided by Mr. [***] After being satisfied that [***] is engaged in activities that may on reasonable grounds be suspected of constituting threats to the security of Canada, Justice Noël issued the warrants that were sought at that time.

[23] At Justice Noël's suggestion, the second phase of [***] took place before me, and concerned two additional authorizations that CSIS is seeking to add to three of the warrants that Justice Noël issued in the initial phase of that proceeding. The first of those authorizations is essentially the same as the sole, and very broad, authorization being sought in [***] (the BII Warrant). The second is much more focused, and would enable CSIS to obtain the BII corresponding to the communications accounts of third parties whose telephone number or electronic identifier has been linked to one or more of [***] named individuals, or to [***] unnamed individuals [***] At CSIS's suggestion, the evidentiary hearings and oral submissions in this second phase of [***] as well as in [***] were held separately, but concurrently, on [***] and [***] of this year.

[24] To preserve the *status quo* with respect to the BII-type power that is being sought in [***] in relation to the threat to the security of Canada posed by Islamist terrorism, I granted an interim order on [***] which provided CSIS with that authorization for 60 days, to permit me to complete this decision.[1]

[25] In view of the nature of the legal issues raised in this application, the Court retained Mr. Gordon Cameron and Mr. Owen Rees to act as *amici curiae*.

[1] The last warrant that contained the BII authorization in respect of CSIS's investigation into [***]

des données sur l'abonné, la demande du SCRS dans le dossier [***] a été divisée en deux étapes. La première portait sur les mandats que demandait le SCRS contre des personnes faisant l'objet de son enquête sur la menace que [***] fait peser sur la sécurité du Canada. Cette étape de l'instance a eu lieu en février de cette année et reposait sur l'affidavit de M. [***] Après avoir été convaincu que [***] mène des activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada, le juge Noël a décerné les mandats demandés.

[23] À la suggestion du juge Noël, j'ai été saisi de la deuxième étape de l'instance dans le dossier [***] Elle portait sur deux autres autorisations que le SCRS voulait ajouter à trois des mandats décernés par le juge Noël lors de l'étape initiale. La première autorisation est essentiellement la même autorisation ayant une portée considérable qui a été demandée dans le dossier [***] (mandat sur les DIB). La deuxième est beaucoup plus précise et permettrait au SCRS d'obtenir les DIB ayant trait aux comptes de communications de tiers dont les numéros de téléphone ou identificateurs électroniques ont été liés à l'une ou à plusieurs des [***] personnes identifiées par leur nom ou [***] personnes dont le nom n'est pas connu [***] À la suggestion du SCRS, la preuve et les observations orales ayant trait à la deuxième étape de l'instance dans le dossier [***] et au dossier [***] ont été entendues séparément, mais de façon simultanée, [***] de cette année.

[24] [***] pour préserver le statu quo en ce qui a trait au pouvoir relatif à l'obtention de DIB qui avait été demandé dans le dossier [***] à l'égard des menaces envers la sécurité du Canada que pose le terrorisme islamiste, j'ai rendu une ordonnance provisoire qui accordait au SCRS cette autorisation pour une période de 60 jours afin de me permettre de trancher[1].

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

[1] Le dernier mandat contenant le pouvoir d'obtenir des DIB [***]

[26] Given that BII authorizations similar to those being requested in these applications may be sought in future proceedings before other designated judges of this Court, I considered it appropriate to convene the designated judges of the Court to join me on the bench, so that they would have the benefit of the evidence provided by the affiants, including on cross-examination by the *amici*. I also considered it to be important that they have the benefit of responses provided by the affiants to questions that any of them, or I, might pose. This should assist each of the designated judges of the Court in any future applications that may involve a request for a BII or similar authorization, and could reduce the need for similar evidence in those applications.

[27] Notwithstanding the involvement of other designated judges of this Court in this proceeding, I assured CSIS and representatives of the Attorney General at the outset of the initial hearing on these applications that my judicial independence would not thereby be compromised in any way. I, and I alone, have decided the issues that have been raised in these applications.

[28] Like several of my designated colleagues before me in previous applications dating back several years, I am satisfied that there are reasonable grounds to believe that activities that CSIS has defined as "Islamist terrorism" constitute a threat to the security of Canada, and that the same is true with respect to the threat-related activities engaged in by [***] that CSIS has identified.

[29] Accordingly, the balance of these reasons for judgment will focus on the three issues that are identified at paragraph 4 above.

[30] In passing, and for completeness, I will add that CSIS informed the Court earlier this year that it did not intend to seek or address in either [***] or [***] the [***] that was referred to in *X (Re)*, above. The Court understands that CSIS may return to the Court to make separate submissions in respect of that power at a future date, and that CSIS will not in the meantime be seeking any authorizations to use that power in respect of [***] communications accounts that correspond to telephone

[26] Puisque des autorisations concernant les DIB semblables à celles dont il est question en l'espèce pourraient être demandées dans de prochaines instances et devant d'autres juges désignés de la Cour, j'ai estimé qu'il y avait lieu de demander à ces juges de se joindre à moi afin qu'ils entendent la preuve des déposants et qu'ils assistent au contre-interrogatoire des *amici*. À mon avis, il était également important qu'ils entendent les réponses des déposants à leurs questions ainsi qu'aux miennes. Cela devrait aider chacun d'eux à traiter les futures demandes d'autorisations d'obtenir des DIB ou d'autorisations de même nature, sans compter qu'il pourrait être moins nécessaire d'y présenter des éléments de preuve similaires.

[27] Dès le début de l'audience initiale concernant ces demandes, j'ai assuré le SCRS et les représentants de la procureure générale que la présence d'autres juges désignés en cours d'instance ne compromettait en rien mon indépendance judiciaire. Moi seul me suis prononcé sur les questions soulevées en l'espèce.

[28] Comme plusieurs de mes collègues désignés qui ont été saisis d'affaires remontant à plusieurs années, je suis convaincu qu'il existe des motifs raisonnables de croire que les activités auxquelles le SCRS a attribué le générique « terrorisme islamiste » constituent une menace envers la sécurité du Canada et qu'il en va de même pour les activités liées à la menace [***] constatées par le SCRS.

[29] Par conséquent, les autres motifs étayant la décision en l'espèce porteront sur les trois questions mentionnées au paragraphe 4 des présents motifs.

[30] Par souci d'exhaustivité, j'ajoute en passant que le SCRS a déjà avisé la Cour qu'il ne compte pas demander, dans les dossiers [***] et [***] [TRADUCTION] [***] dont il est question dans la décision *X (Re)* ni en discuter. La Cour comprend que le SCRS pourra s'adresser de nouveau à elle à une date ultérieure pour présenter une autre demande à cet effet, et que d'ici là, il ne demandera pas l'autorisation d'utiliser ce pouvoir à l'endroit de comptes de communications [***] qui correspondent à

numbers or electronic identifiers that have no direct nexus with identified subjects of investigation.

III. The BII Authorizations Requested by CSIS

[31] The warrant that CSIS has requested the Court to issue in [***] consists of a single authorization. It is as follows:

> I authorize the Director and any employee of the service acting under his authority to obtain BII relating to any account with a CSP where a Chief determines that
>
> a) the account was identified during the investigation of Islamist terrorism and
>
> b) the identity of the subscriber to the account will assist in the investigation of Islamist terrorism.

[32] "BII" is defined in the warrant to mean:

> i. The name of a subscriber to an account;
>
> ii. The subscriber's address;
>
> [***[The information relating to IP addresses in certain circumstances]***]

[33] In essence, this authorization would enable CSIS to obtain BII in respect of any communications account corresponding to any telephone number or electronic identifier that CSIS may identify during its investigation into Islamist terrorism, where a chief within CSIS determines that BII will assist CSIS to advance its investigation.

[34] The Attorney General analogizes this authorization to a power to obtain "telephone book" information, which traditionally has been required to identify individuals. The Attorney General, the affiant in [***] and the affiant in [***] each maintained that this was the sole purpose of the BII authorization being requested. In this regard, they emphasized that the BII authorization is not used to track online activity. The Attorney General

des numéros de téléphone ou à des identificateurs électroniques qui n'ont pas de lien direct avec des cibles.

III. Autorisations d'obtenir des DIB demandées par le SCRS

[31] Le mandat que le SCRS demande à la Cour de lui décerner dans le dossier [***] se compose d'une seule autorisation.

> [TRADUCTION]
>
> J'autorise le directeur et tout employé du Service agissant sous son autorité à obtenir auprès d'un FSC les DIB liées à tout compte lorsqu'un chef détermine que :
>
> a) le compte a été découvert dans le cadre de l'enquête sur le terrorisme islamiste;
>
> b) l'établissement de l'identité de l'abonné au compte fera progresser l'enquête sur le terrorisme islamiste.

[32] Aux termes du mandat, les DIB sont :

> i. le nom de l'abonné à un compte;
>
> ii. l'adresse de l'abonné;
>
> [***[L'information concernant des addresses IP dans certaines circonstances]***]

[33] Essentiellement, cette autorisation permettrait au SCRS d'obtenir des DIB concernant tout compte de communication correspondant à tout numéro de téléphone ou identificateur électronique que le SCRS peut découvrir dans le cadre de son enquête sur le terrorisme islamiste, lorsqu'un chef au Service détermine que ces DIB permettraient au SCRS de faire progresser son enquête.

[34] La procureure générale fait une analogie entre cette autorisation et l'obtention d'informations figurant dans un « bottin téléphonique », qui servent depuis longtemps à identifier des personnes. La procureure générale et les déposants dans les dossiers [***] et [***] affirment qu'il s'agit de la seule raison de la demande d'autorisation d'obtenir des DIB. À cet égard, ils ont insisté sur le fait que l'autorisation ne servira pas à suivre des activités

added that if CSIS wanted to exercise such a power or indeed any other intrusive powers in respect of a person, it would have to return to the Court to seek specific authorizations to do so.

[35] The BII Warrant that has been requested in [***] also provides that if, in executing the warrant, CSIS provides [***] CSIS shall also provide [***] Islamist terrorism. This requirement has been included as a safeguard to help ensure that BII is provided in respect of the correct account, [***]

[36] For the purposes of the BII Warrant, "Islamist terrorism" is defined to mean "activities in paragraph (c) of the definition of 'threats to the security of Canada' found in section 2 of the Act [***] including activities of the [***]

[37] Both Mr. [***] and Mr. [***] testified that an authorization to obtain BII is crucial to CSIS's ability to investigate the threats to the security of Canada posed by the activities [***] and Islamist terrorism. This is because this may be the only manner in which CSIS can identify a person who is behind a phone number [***[or an electronic identifier]***] In addition, the ability to identify individuals and assess the nature of their relationship to Islamist terrorism or to the threat-related activities [***] is a fundamental building block of an investigation. This is particularly so given that many people associated with the threats in question interact exclusively or primarily by electronic means, and may never meet in person. According to Mr. [***] "identification is [***] part of the job", and [***] He emphasized that, without being able to identify someone, CSIS would not be able to fulfill its mandate.

[38] According to Mr. [***] the 2014-2016 Intelligence Priorities for CSIS from the Minister of Public Safety [***]

[39] The BII authorizations that CSIS is seeking in the amendments that it has requested be made to three of the warrants were issued in the first phase of [***] are of

en ligne. La procureure générale a ajouté que le SCRS, s'il souhaite exercer un tel pouvoir ou tout autre pouvoir envahissant à l'égard d'une personne, devra revenir devant la Cour pour obtenir l'autorisation nécessaire.

[35] Le mandat sur les DIB demandé dans [***] prévoit également que, dans le cadre de l'exécution du mandat, si le SCRS fournit [***], il doit également fournir [***] terrorisme islamiste. Cette exigence a été ajoutée comme mesure de protection pour assurer que les DIB fournies correspondent au bon compte, [***]

[36] Aux fins du mandat concernant les DIB, s'entend par « terrorisme islamiste » [TRADUCTION] « les activités mentionnées à l'alinéa c) de la définition de « menaces envers la sécurité du Canada » figurant à l'article 2 de la Loi sur le SCRS [***] dont les activités menées par [***]

[37] M. [***] et M. [***] ont témoigné que le SCRS a absolument besoin de l'autorisation d'obtenir les DIB pour enquêter sur les menaces que les activités [***] et le terrorisme islamiste font peser sur la sécurité du Canada, car elles peuvent être la seule ressource dont le SCRS dispose pour établir l'identité de la personne à qui appartient un numéro de téléphone, [***[ou identificateurs électroniques]***] En outre, la capacité d'identifier une personne et d'évaluer la nature de sa relation avec le terrorisme islamiste ou aux activités liées à la menace [***] est la pierre angulaire d'une enquête. Cela est particulièrement vrai dans la mesure où de nombreuses personnes liées à de telles menaces interagissent exclusivement ou principalement par voie électronique et peuvent ne jamais se rencontrer. Selon M. [***] [TRADUCTION] « l'établissement de l'identité est [***] part du travail [***] Il insiste sur le fait que le SCRS, s'il n'est pas en mesure d'établir l'identité de quiconque, ne pourra s'acquitter de son mandat.

[38] Selon M. [***] le ministre de la Sécurité publique [***] en matière de renseignement du SCRS pour 2014 à 2016. [***]

[39] Les autorisations d'obtenir des DIB que demande le SCRS en faisant modifier trois des mandats décernés à la première étape de l'instance dans le dossier [***]

two types. The first type would provide essentially the same broad power that is being sought in [***] That is to say, it would provide essentially the same authorization as is being requested in the BII Warrant, albeit in respect of communications accounts that are identified during CSIS's investigation of the threat-related activities [***] that it has described.

[40] The second type of authorization that CSIS is seeking to add to three of the warrants that have been issued in [***] is much narrower. In brief, it would authorize CSIS to obtain BII in respect of communications accounts identified pursuant to its review of specifically defined information obtained in relation to [***] named individuals and [***] additional individuals who [***]

[41] It bears underscoring that no individuals are named in the BII Warrant being sought in [***] or in the first group of amendments that CSIS is seeking to add to three of the warrants that have been issued in [***] In the words of Mr. [***] "the warrant itself is not [***] it's against Islamist terrorism". Likewise, the amendments sought to three of the warrants issued in [***] are directed towards the threat-related activities [***].

IV. Issues

[42] As explained at paragraph 4 above, the applications in [***] and [***] raise the following three issues:

i. Can the Court authorize CSIS to obtain BII in respect of communications accounts corresponding to telephone numbers or electronic identifiers that may in the future come to its attention in the course of its investigations, where CSIS has not described and established their specific nexus to those investigations?

ii. Can the Court authorize CSIS to obtain BII in respect of communications accounts identified pursuant to its review of specifically defined information obtained in relation to [***] named

sont de deux types. Le premier type lui donnerait essentiellement le même pouvoir élargi qui est demandé dans le dossier [***] Autrement dit, en pratique, l'autorisation serait la même que celle qui est demandée dans le mandat sur les DIB, sauf qu'elle aurait trait aux comptes de communications découverts par le SCRS pendant son enquête sur les activités liées à la menace [***]

[40] L'autorisation du second type que le SCRS veut faire ajouter à trois des mandats décernés dans le dossier [***] a une portée beaucoup plus circonscrite. En bref, elle autoriserait le SCRS à obtenir des DIB liées à des comptes de communications qu'il a découvert en examinant des informations clairement définies ayant trait à [***] personnes identifiées par leur nom et à [***] personnes [***]

[41] Je souligne que le mandat sur les DIB demandé dans le dossier [***] ou à la première catégorie de modifications que le Service souhaite apporter à trois des mandats décernés dans le dossier [***] ne visent nommément personne. Pour reprendre les propos de M. [***] [TRADUCTION] «le mandat en soi ne [***] mais le terrorisme islamiste». De la même façon, les modifications que le SCRS souhaite apporter à trois des mandats décernés dans le dossier [***] visent les activités liées à la menace [***]

IV. Questions

[42] Tel que déjà souligné au paragraphe 4, les demandes dans les dossiers [***] et [***] soulèvent les trois questions suivantes.

i. La Cour peut-elle autoriser le SCRS à obtenir des DIB liées à des comptes de communication correspondant à des numéros de téléphone ou à des identificateurs électroniques qui pourront éventuellement attirer son attention lors de ses enquêtes, lorsque le SCRS n'a ni décrit ni établi leur lien précis avec ces enquêtes?

ii. La Cour peut-elle autoriser le SCRS à obtenir des DIB liées à des comptes de communications qu'il a découverts en examinant des informations clairement définies ayant trait à [***] personnes

individuals and [***] additional individuals who have been identified [***]

iii. Can the Court authorize an employee of CSIS to obtain BII in respect of a communications account that corresponds to a telephone number or an electronic identifier, where a "chief" within CSIS determines that the account was identified during its investigation, and that the BII would assist CSIS in its investigation?

[43] In both [***] and [***] the Attorney General raised an additional issue, namely, the threshold issue of whether a warrant is required to obtain BII from a CSP. However, in each proceeding, the Attorney General conceded that a warrant is required to obtain BII from a CSP, because it may engage privacy rights that are protected by section 8 of the Charter. This is because "[***] information can be revealed to [CSIS] when BII is obtained from CSPs". Indeed, this was demonstrated by a number of examples included in the Attorney General's written submissions.

[44] The *amici* agreed. They maintained that, in view of the fact that CSIS may well be able to use BII [***] to link previously anonymous [***] activity to a named individual, such activity by CSIS would normally require a warrant. I agree.

[45] Given the Attorney General's acknowledgement that a warrant is required to access BII from a CSP, it is unnecessary to address this issue in detail. I will simply note that the linking of previously anonymous [***] activity to an individual's identity "engages a high level of informational privacy" (*R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212 (*Spencer*), at paragraph 51). As such, obtaining the information to make such a link, [***] would constitute a "search" that is more invasive than the minimally intrusive warrantless searches that are authorized by section 12 of the Act.

[46] The same is true with respect to telephone numbers, which can assist CSIS to obtain valuable personal information about a person. This was corroborated

identifiées par leur nom et à [***] autres personnes ciblées [***]

iii. La Cour peut-elle autoriser un employé du SCRS à obtenir les DIB liées à un compte de communications correspondant à un numéro de téléphone ou à un identificateur électronique lorsqu'un « chef » au sein du SCRS détermine que ce compte a été découvert lors d'une enquête et que les DIB faciliteraient cette enquête?

[43] Dans les dossiers [***] et [***] la procureure générale a soulevé une autre question, soit la nécessité d'un mandat pour obtenir des DIB auprès d'un FSC. Toutefois, dans chaque instance, elle a admis qu'il fallait un mandat pour ce faire, car cela pouvait enfreindre les droits en matière de vie privée garantis par l'article 8 de la Charte. En effet, [TRADUCTION] « [***] d'informations peuvent être révélées au SCRS lorsqu'il obtient des DIB auprès d'un FSC ». Cela a été effectivement démontré par un certain nombre d'exemples qui figurent dans les observations écrites de la procureure générale.

[44] Les *amici* sont d'accord. Ils ont soutenu que le SCRS a besoin d'un mandat pour effectuer ce genre de démarches, puisqu'il peut fort bien utiliser des DIB, [***] pour établir un lien entre une personne dont l'identité a été établie et des activités menées jusque-là dans l'anonymat, [***] Je suis d'accord.

[45] Puisque la procureure générale a reconnu qu'il faut un mandat pour obtenir des DIB auprès d'un FSC, il n'est pas nécessaire de traiter cette question en profondeur. Je noterai simplement que l'établissement d'un lien entre une activité menée anonymement [***] et une personne dont l'identité est établie « fait intervenir, dans une grande mesure, l'aspect informationnel du droit à la vie privée » (*R. c. Spencer*, 2014 CSC 43, [2014] 2 R.C.S. 212 (*Spencer*), au paragraphe 51). Partant, [***] pour établir un tel lien constituerait une fouille plus envahissante que ce que l'article 12 de la Loi sur le SCRS permet d'effectuer sans mandat.

[46] Il en va de même pour les numéros de téléphone, qui peuvent aider le SCRS à obtenir des renseignements personnels importants concernant une personne. Cela a

by one of the examples provided by Mr. [***] in his affidavit.

[47] I will simply add that the Attorney General's position that a warrant is required to obtain BII is consistent with the position that she took in [***] where she stated on multiple occasions that a warrant would be required to obtain subscriber information pertaining to any identifiers [***]

V. Analysis

A. *Applicable legal principles*

[48] Section 8 of the Charter provides that "[e]veryone has the right to be secure against unreasonable search or seizure."

[49] It follows that section 8 of the Charter does not afford protection against all searches, only against *unreasonable* ones (*R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, at paragraph 20).

[50] In assessing whether a search is "unreasonable", courts must adopt "a purposive approach … that emphasizes the protection of privacy as a prerequisite to individual security, self-fulfilment and autonomy as well as to the maintenance of a thriving democratic society" (*Spencer*, above, at paragraph 15).

[51] Broadly speaking, a determination of whether a search is unreasonable requires a balancing assessment of "whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals" (*Hunter et al. v. Southam Inc.*, [1984] 2 S.C.R. 145 (*Hunter*), at pages 159–160).

[52] Given that the underlying purpose of section 8 is to protect individuals from unjustified state intrusions upon their privacy, prior authorization of those intrusions is presumptively required. Such authorization must be given by an entirely neutral and impartial arbiter who

été corroboré par un des exemples fournis par M. [***] dans son affidavit.

[47] J'ajoute simplement que la position de la procureure générale quant à la nécessité d'un mandat pour obtenir des DIB est conforme à la position qu'elle a adoptée dans le dossier [***] où elle a indiqué à plusieurs reprises qu'il faut un mandat pour obtenir des informations sur l'abonné ayant trait aux identificateurs [***]

V. Analyse

A. *Principes juridiques applicables*

[48] L'article 8 de la Charte prévoit que « [c]hacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives ».

[49] Partant, l'article 8 de la Charte ne protège pas contre toute fouille et perquisition, uniquement contre celles qui sont *abusives* (*R. c. Gomboc*, 2010 CSC 55, [2010] 3 R.C.S. 211, au paragraphe 20).

[50] Pour évaluer si une fouille est « abusive », la Cour doit adopter « une approche téléologique axée principalement sur la protection de la vie privée considérée comme une condition préalable à la sécurité individuelle, à l'épanouissement personnel et à l'autonomie ainsi qu'au maintien d'une société démocratique prospère » (*Spencer*, précité, au paragraphe 15).

[51] De manière générale, pour déterminer si une fouille est abusive, il faut évaluer si « le droit du public de ne pas être importuné par le gouvernement doit céder le pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins » (*Hunter et autres c. Southam Inc.*, [1984] 2 R.C.S. 145 (*Hunter*), aux pages 159 et 160).

[52] Puisque l'objet sous-jacent de l'article 8 est de protéger les personnes contre les intrusions injustifiées de l'État dans leur vie privée, il est présumé qu'une telle intrusion doit être autorisée au préalable par un arbitre tout à fait neutre et impartial qui est en mesure d'exercer

is capable of acting judicially in balancing the interests of the state against those of the individual (*Spencer*, above, at paragraph 68; *Goodwin v. British Columbia (Superintendent of Motor Vehicles)*, 2015 SCC 46, [2015] 3 S.C.R. 250 (*Goodwin*), at paragraph 56; *Hunter*, above, at pages 160–162).

[53] In addition, the neutral arbiter must be satisfied that the person seeking the authorization has reasonable grounds, established under oath, to believe that the relevant statutory or other conditions to be met before the search power may be exercised, have in fact been met (*Hunter*, above, at pages 166–168).

[54] In deciding whether to issue a warrant, the neutral arbiter must have sufficient flexibility to consider all of the circumstances that may be relevant to the exercise of discretion to issue the warrant, and to impose any conditions that may be considered necessary (*Baron v. Canada*, [1993] 1 S.C.R. 416 (*Baron*), at paragraphs 437, 439 and 440).

B. *Can the Court authorize CSIS to obtain BII in respect of communications accounts corresponding to telephone numbers or electronic identifiers that may in the future come to its attention in the course of its investigations, where CSIS has not described and established their specific nexus to those investigations?*

(1) General

[55] In her written and oral submissions, the Attorney General characterized this issue as being whether the Act authorizes a judge of this Court to issue warrants against "threat-related activities".

[56] In support of her position that the Act is sufficiently flexible to allow for the issuance of warrants in respect of *activities*, the Attorney General notes that section 12 of the Act empowers CSIS to investigate activities, and that the definition of "threats to the security of Canada" that is set forth in section 2 of the Act also refers to *activities*, without any reference to the *persons* who would be conducting those activities. The Attorney

des fonctions judiciaires en établissant un équilibre entre les intérêts de l'État et ceux de la personne (*Spencer*, précité, au paragraphe 68; *Goodwin c. Colombie-Britannique (Superintendent of Motor Vehicles)*, 2015 CSC 46, [2015] 3 R.C.S. 250 (*Goodwin*), au paragraphe 56; et *Hunter*, précité, aux pages 160 à 162).

[53] En outre, l'arbitre impartial doit être convaincu que la personne qui demande l'autorisation a des motifs raisonnables de croire, déclarés sous serment, que les conditions applicables qui ont trait à la loi, entre autres, et qui sont préalables à l'exercice du pouvoir de fouille ou de perquisition ont effectivement été réunies (*Hunter*, précité, aux pages 166 à 168).

[54] Pour prendre sa décision, l'arbitre impartial doit disposer de suffisamment de souplesse pour tenir compte de toutes les circonstances qui peuvent avoir trait à l'exercice du pouvoir discrétionnaire de décerner ou de refuser un mandat et pour imposer toutes les conditions jugées nécessaires (*Baron c. Canada*, [1993] 1 R.C.S. 416 (*Baron*), aux pages 437, 439 et 440).

B. *La Cour peut-elle autoriser le SCRS à obtenir des DIB liées à des comptes de communication correspondant à des numéros de téléphone ou à des identificateurs électroniques qui pourront éventuellement attirer son attention lors de ses enquêtes, lorsque le SCRS n'a ni décrit ni établi leur lien précis avec ces enquêtes?*

1) Généralités

[55] Selon la procureure générale, dans ses observations écrites et orales, il s'agit de déterminer si la Loi sur le SCRS autorise un juge de la Cour à décerner des mandats contre des activités liées à une menace.

[56] Pour appuyer sa position selon laquelle la Loi sur le SCRS est suffisamment souple pour permettre la délivrance de mandats contre des *activités*, la procureure générale souligne que l'article 12 de la Loi sur le SCRS permet au Service de mener des enquêtes et que la définition de «menaces envers la sécurité du Canada» figurant à l'article 2 de la Loi sur le SCRS s'applique également à des *activités* sans faire allusion aux *personnes* qui les

General further notes that paragraph 21(2)(d) requires a warrant application to be accompanied by an affidavit that addresses various issues, including "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" (emphasis added).

[57] The Attorney General submits that it may be inferred from all of the foregoing that warrants issued pursuant to section 21 of the Act can be obtained to investigate identified threat-related activities. She maintains that this is so even where the warrant does not name any individuals or describe the specific nexus between CSIS's investigation and the individuals whose privacy interests would be intruded upon.

[58] I disagree. With respect, that position confuses the activities that CSIS is authorized to investigate under section 12 of the Act, with the privacy interests that might be engaged by a warrant issued under section 21 in connection with an investigation. Privacy interests are not held by activities or threats, such as those posed by [***] or "Islamist terrorism", or in respect of an event that might be the focus of an investigation, such as the Vancouver Olympics or the G7 meeting that took place in Toronto.

[59] Privacy interests are held by individuals and corporations, whether they be subjects of investigation, persons whose connection to an investigation may remain to be ascertained, or persons who might, on reasonable grounds, be believed to have information that is likely to assist an investigation. In my view, the words "the identity of the person, if known" (emphasis added) in paragraph 21(2)(d) simply reflects the practical reality that CSIS may not know, at the time it applies for a warrant, the identity of an ascertainable person whose communication is proposed to be intercepted, or who has possession of the information, record, document or other thing proposed to be obtained under the warrant, as contemplated by that provision.

mènent. La procureure générale fait aussi remarquer que l'alinéa 21(2)d) de la Loi sur le SCRS exige qu'une demande de mandat s'accompagne d'un affidavit portant sur différents points, dont «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» (non souligné dans l'original).

[57] La procureure générale soutient qu'il est possible de conclure de tout ce qui précède que des mandats peuvent être décernés au titre de l'article 21 de la Loi sur le SCRS pour enquêter sur des activités liées à la menace, et ce, même lorsque le mandat ne vise nommément personne et ne décrit pas le lien entre l'enquête du SCRS et les personnes dont le droit au respect de la vie privée pourrait être enfreint.

[58] Je ne suis pas d'accord. Selon moi, cette interprétation confond les activités qui peuvent faire l'objet d'une enquête du SCRS en vertu de l'article 12 de la Loi sur le SCRS et le droit au respect de la vie privée qui peut être enfreint par un mandat décerné en vertu de l'article 21 de la Loi sur le SCRS dans le cadre d'une enquête. Les activités ou les menaces, comme celles que mènent ou constituent [***] ou le terrorisme islamiste, n'ont pas de droit à la vie privée, pas plus que les événements qui peuvent faire l'objet d'une enquête, comme les Jeux olympiques de Vancouver ou la réunion du G7 qui a eu lieu à Toronto.

[59] Le droit au respect de la vie privée est l'apanage des personnes et des personnes morales, qu'elles fassent l'objet d'une enquête, qu'elles aient un lien qui reste à confirmer avec une enquête ou qu'il existe des motifs raisonnables de croire qu'elles détiennent des informations pouvant être utiles à une enquête. À mon avis, le segment «l'identité de la personne, si elle est connue» (non souligné dans l'original) à l'alinéa 21(2)d) reflète simplement le fait qu'en pratique, lorsqu'il présente une demande de mandat, le SCRS peut ne pas connaître l'identité de la personne vérifiable dont il propose d'intercepter les communications ou qui détient des informations, des documents ou des objets qu'il entend obtenir, comme le précise cette disposition.

[60] Accordingly, the more relevant question that arises in these proceedings is whether CSIS can be prospectively authorized to obtain BII in relation to communications accounts that may in the future come to its attention in the course of its investigations, where CSIS has not yet described and established their specific nexus with those investigations. In my view, the answer is "no, except in exceptional circumstances that have not been demonstrated to exist in this case".

[61] This is because persons who are responsible for authorizing the use of intrusive powers are required to consider the impact of such intrusion on the specific "subject of the search" (*Hunter*, above, at page 157; *Spencer*, above, at paragraph 36 (emphasis added)). In other words, an assessment must be made of the context of each "particular situation", and its impact on "the individual." As the *amici* underscored, the balancing analysis to be conducted is between the interests of the state and the interests of the specific individual whose privacy interests are at issue (*Hunter*, above, at pages 159–160, 161–162 and 167; *Baron*, above, at pages 435–436 and 437; *R. v. Rodgers*, 2006 SCC 15, [2006] 1 S.C.R. 554, at paragraph 27 (emphasis added)).

[62] Where a "class of persons" whose privacy interests may be encroached upon can be described in a manner that enables the Court to clearly understand the nexus between those persons and the threat-related activities that are the focus of a CSIS investigation, the balancing analysis described above can comfortably be conducted in respect of those persons. In my view, this is contemplated by the references to "class of persons" in paragraphs 21(2)(e) and 21(4)(c) of the Act.

[63] The need to consider the interests of the specific individual or class of individuals whose privacy interests are engaged is reinforced by three additional requirements that have been established by jurisprudence under section 8 of the Charter. The first is the requirement to assess the individual's subjective expectation of privacy, when considering whether there is a reasonable expectation of privacy (*Spencer*, above, at paragraph 18). The second is the requirement that CSIS's powers to investigate activities that pose threats to the security of Canada must be "strictly controlled" (*Charkaoui v. Canada*,

[60] Partant, la question la plus pertinente en l'espèce est celle qui consiste à déterminer si le SCRS peut être autorisé, de manière prospective, à obtenir les DIB liées à des comptes de communication qui peuvent attirer son attention dans le cadre d'enquêtes, s'il n'a pas encore décrit et établi de lien précis entre les DIB et les enquêtes en question. Selon moi, la réponse est négative, sauf en des circonstances exceptionnelles dont l'existence n'a pas été démontrée en l'espèce.

[61] En effet, les personnes chargées d'autoriser le recours à des pouvoirs envahissants doivent tenir compte des répercussions de l'intrusion sur l'« objet de la fouille » (*Hunter*, précité, à la page 157 et *Spencer*, précité, au paragraphe 36) (non souligné dans l'original). Autrement dit, il est nécessaire d'évaluer le contexte de chaque situation et son incidence sur la personne. Comme l'ont souligné les *amici*, il y a lieu d'atteindre un équilibre entre les intérêts de l'État et ceux de la personne même dont le droit au respect de sa vie privée est en jeu (*Hunter*, précité, aux pages 159, 160, 161, 162 et 167; *Baron*, précité, aux pages 435, 436 et 437; et *R. c. Rodgers*, 2006 CSC 15, [2006] 1 R.C.S. 554, au paragraphe 27) (non souligné dans l'original).

[62] Cet exercice de pondération peut se faire aisément lorsqu'il s'agit d'une catégorie de personnes, dont le droit au respect de la vie privée peut être enfreint, et dont il est possible de décrire de manière à ce que la Cour comprennent très bien le lien qui peut être établi entre elles et les activités liées à la menace qui font l'objet d'une enquête du SCRS. À mon avis, c'est ce qui est visé par l'expression « catégorie de personnes » aux alinéas 21(2)e) et 21(4)c) de la Loi sur le SCRS.

[63] Trois autres exigences ayant trait à l'article 8 de la Charte établies en jurisprudence renforcent la nécessité de tenir compte des intérêts des personnes ou des catégories de personnes dont le droit au respect de la vie privée est en jeu. D'abord, il est nécessaire d'évaluer l'attente subjective de la personne en matière de vie privée au moment de déterminer s'il existe une attente raisonnable en la matière (*Spencer*, précité, au paragraphe 18). Ensuite, il est nécessaire d'assujettir à des « contrôles sévères » les pouvoirs dont jouit le SCRS pour enquêter sur des activités qui constituent des menaces envers la

2008 SCC 38, [2008] 2 S.C.R. 326, at paragraph 22, quoting the Report of the Special Senate Committee on the Canadian Security Intelligence Service*, Delicate Balance: A Security Intelligence Service in a Democratic Society*, November 3, 1983, at paragraph 25; see also *Baron*, above, at pages 436–437). The third is the requirement to consider "the totality of the circumstances" (*Spencer*, above, at paragraph 18). In my view, this implies that the interests of the specific person(s) whose privacy interests are at stake must be taken into account. It is difficult to imagine how the totality of the circumstances would not involve an assessment of the privacy interests of the very individual(s) whose interests would be engaged if CSIS were to obtain BII from a CSP.

sécurité du Canada (*Charkaoui c. Canada (Citoyenneté et Immigration)*, 2008 CSC 38, [2008] 2 R.C.S. 326, au paragraphe 22, qui cite le rapport du Comité sénatorial spécial du Service canadien du renseignement de sécurité intitulé *Équilibre délicat : Un Service du renseignement de sécurité dans une société démocratique*, le 3 novembre 1983, au paragraphe 25; voir aussi *Baron*, précité, aux pages 436 à 437). Enfin, il est nécessaire de prendre en considération « l'ensemble des circonstances » (*Spencer*, précité, au paragraphe 18). À mon avis, cela signifie qu'il faut tenir compte des intérêts de la personne ou des personnes en particulier dont le droit au respect de la vie privée est en jeu. Il est difficile d'imaginer comment l'ensemble des circonstances n'inclurait pas une évaluation du droit au respect de la vie privée de la personne ou des personnes elles-mêmes dont les intérêts seraient touchés si le SCRS obtenait des DIB auprès d'un FSC.

[64] Notwithstanding the foregoing, it is not necessary for warrants that authorize CSIS to obtain BII to associate the communications accounts in question with named individuals. It is often precisely because CSIS does not know the name associated with a telephone number, [***[or electronic identifier]***] etc. that it needs to be able to obtain BII in respect of the corresponding communications account from a CSP.

[64] Malgré ce qui précède, il n'est pas nécessaire que les mandats autorisant le SCRS à obtenir des DIB établissent un lien entre les comptes en question et des personnes nommées. Souvent, c'est précisément parce que le SCRS ne connaît pas le nom lié au numéro de téléphone, [***[ou identificateurs électroniques]***] entre autres, qu'il doit être en mesure d'obtenir des DIB relatives aux comptes correspondants auprès d'un FSC.

[65] Even though CSIS may not know an individual's name, it may know sufficient information about the individual [***] to provide the Court with reasonable grounds to believe that obtaining the BII of a particular communications accounts is required to advance its investigation, as contemplated by paragraph 21(2)(a) of the Act. This may be because the individual behind a telephone number or electronic identifier appears to be engaged in activities that pose a threat to the security of Canada, or because he or she appears to be in a position to provide information that will assist CSIS to advance its investigation into those activities. I accept Mr. [***] testimony that obtaining BII, and thereby learning who is behind [***] identifiers [***] can assist CSIS to advance an investigation.

[65] Même s'il ne connaît pas le nom d'une personne, le SCRS peut disposer d'assez d'informations sur elle [***] pour fournir à la Cour des motifs raisonnables de croire qu'il lui faut obtenir les DIB liées à un compte pour faire progresser son enquête, comme le prévoit l'alinéa 21(2)a) de la Loi sur le SCRS. Cela peut être parce que la personne liée au numéro de téléphone ou à l'identificateur électronique semble mener des activités qui constituent une menace envers la sécurité du Canada ou parce qu'elle semble être en mesure de donner au SCRS des informations qui faciliteront son enquête sur ces activités. J'accepte le témoignage de M. [***] selon qui il peut être utile au SCRS, pour faire progresser une enquête, d'obtenir des DIB et, donc, d'apprendre qui se cache derrière [***] identificateurs [***]

[66] In such situations, it will suffice if CSIS can provide sufficient evidence about a telephone number or one

[66] Dans de telles situations, il suffit au SCRS de fournir des éléments de preuve suffisants au sujet d'un

of the types of other identifiers mentioned above to establish reasonable grounds to believe that CSIS requires the BII of the account corresponding to that number or identifier, to advance its investigation. In my experience, those grounds can often be established by providing the Court with a brief description of the context in which CSIS obtained the telephone number or other identifier in respect of which BII is sought. It is that specific context that can provide the Court with the nexus between the unidentified individual whose privacy rights will be engaged by the BII power, and CSIS's investigation.

[67] Where CSIS is not in possession of the telephone number or other identifier at the time of a warrant application for authorization to obtain BII information, it will remain open to CSIS to describe the telephone number or identifier in a way that enables the Court to satisfy itself of the matters referred to in paragraphs 21(2)(a) and (b) of the Act. With respect to the reasonable grounds to believe referred to in paragraph 21(2)(a), it may suffice to provide the Court with an understanding of the nexus between CSIS's investigation and the specific individual(s) whose privacy interests would be intruded upon. For example, it may suffice to describe a telephone number in terms of a future communication by a subject of investigation. If there were reasonable grounds to believe that the subject of investigation may be engaged in activities that pose a threat to the security of Canada, there would be reasonable grounds to believe that the BII associated with the telephone numbers at each end of a future call placed or received by that individual is required to assist CSIS to advance its investigation of the threat-related activities of that person. Stated differently, this information would provide the Court with the reasonable basis contemplated by section 8 of the Charter on which to authorize CSIS to obtain the BII pertaining to the accounts of both the subject of investigation, and the yet-to-be identified third parties with whom he or she may communicate.

[68] For the same reason, it may suffice for CSIS to describe a BII authorization that it may wish to seek, by reference to a [***[landline or electronic account]***] account that CSIS may in the future discover has been used by a subject of investigation. The same would apply with respect to [***[landline or electronic account]***]

numéro de téléphone ou d'un des autres types d'identificateurs susmentionnés pour faire valoir qu'il a des motifs raisonnables de croire qu'il a besoin des DIB liées au compte correspondant pour faire progresser son enquête. Selon mon expérience, il suffit souvent au SCRS, pour établir de tels motifs, de donner à la Cour une brève description du contexte entourant l'obtention du numéro de téléphone ou de l'identificateur relatif aux DIB recherchées. C'est justement ce contexte précis qui permet d'établir un lien entre l'enquête du SCRS et la personne non-identifiée dont les droits en matière de vie privée seront mis en jeu par le pouvoir d'obtenir des DIB.

[67] Lorsqu'il ne dispose pas du numéro de téléphone ou d'un autre identificateur au moment de demander un mandat l'autorisant à obtenir des DIB, le SCRS a toujours la possibilité de le décrire d'une manière qui permet à la Cour d'être convaincue de la présence des éléments prévus aux alinéas 21(2)a) et b) de la Loi sur le SCRS. En ce qui a trait aux motifs raisonnables de croire dont il est question à l'alinéa 21(2)a), il peut être suffisant d'expliquer à la Cour le lien qui unit l'enquête du SCRS et la ou les personnes dont le droit au respect de la vie privée sera enfreint. À titre d'exemple, il peut suffire de mentionner qu'un numéro de téléphone pourrait être utilisé par une cible. S'il existe des motifs raisonnables de croire que la cible mène des activités qui constituent une menace envers la sécurité du Canada, il existe également des motifs raisonnables de croire que le SCRS a besoin des DIB liées aux numéros de téléphone impliqués dans les appels qu'elle pourrait faire ou recevoir afin de faire progresser son enquête sur les activités liées à la menace de cette personne. Autrement dit, ces informations donneraient à la Cour le fondement raisonnable ayant trait à l'article 8 de la Charte pour autoriser le SCRS à obtenir les DIB liées aux comptes de la cible et de tiers toujours non-identifiés avec lesquels elle pourrait communiquer.

[68] Pour les mêmes motifs, il peut suffire au SCRS de décrire l'autorisation d'obtenir des DIB qu'il souhaite se voir octroyer par référence à un [***[ligne terrestre ou identificateur électronique]***] dont il pourrait éventuellement constater a été utilisé par une cible. Cela s'applique aussi aux [***[ligne terrestre ou identificateur

accounts that CSIS may in the future discover are used by individuals [***] Of course, CSIS would have to establish at the time it seeks the BII authorization in question that there are reasonable grounds to believe that persons [***] may have been associated with the threat-related activities in question.

[69] In my view, the foregoing examples would meet the requirements of both section 21 of the Act and section 8 of the Charter. They strike an appropriate balance between the public interest in affording CSIS with a reasonable degree of flexibility to fulfill its statutory mandate, and the privacy interests of yet-to-be identified individuals whose BII would be obtained under a warrant. Among other things, those examples help to respond to the practical difficulty associated with threat-related activities in respect of future events (*Atwal v. Canada*, [1988] 1 F.C. 107 (C.A.), at page 127).

(2) The BII Warrant and the first type of proposed amendments to the warrants issued in [***]

[70] With the foregoing in mind, it should be readily apparent that the appropriate balance is not met with the BII Warrant that CSIS has sought in [***] or with the first type of amendments that have been proposed to three of the warrants that were issued in [***]

[71] This is because the requested authorizations would permit CSIS to obtain BII in respect of any communications accounts that CSIS may identify over the course of very broadly defined investigations into threats to the security of Canada posed by Islamist terrorism and certain activities of [***] where CSIS simply determines that BII will assist it in its investigation. Among other things, CSIS has not provided the Court with any understanding whatsoever of the specific nexus between (i) the as-yet-to be discovered telephone numbers and electronic identifiers in respect of which BII would be sought, and (ii) CSIS's investigations. The loosely defined "nexus" is simply too broad and nebulous (*R. v. Chehil*, 2013 SCC 49, [2013] 3 S.C.R. 220, at paragraphs 36 and 51). And it does not provide sufficient information for the Court to

électronique]***] dont il pourrait constater éventuellement qu'ils sont utilisés par les titulaires [***] Bien sûr, lorsqu'il demande cette autorisation relativement aux DIB, le SCRS doit démontrer qu'il existe des motifs raisonnables de croire que les personnes qui ont [***] impliquées dans les activités liées à la menace en question.

[69] Selon moi, les exemples précédents satisferaient aux exigences de l'article 21 de la Loi sur le SCRS et de l'article 8 de la Charte. Ils font état d'un juste équilibre entre l'intérêt public, car le SCRS s'y voit accorder un degré de souplesse raisonnable dans l'exécution de son mandat, et le droit au respect de la vie privée des personnes toujours non-identifiées dont le Service obtiendrait les DIB en vertu d'un mandat. Entre autres, ces exemples aident à réagir aux difficultés pratiques ayant trait aux activités liées à la menace dans le cadre d'événements futurs (*Atwal c. Canada*, [1988] 1 C.F. 107 (C.A.), à la page 127).

2) Mandat sur les DIB et modifications du premier type proposées aux mandats décernés dans le dossier [***]

[70] Compte tenu de ce qui précède, il devrait être apparent que le juste équilibre n'a pas été atteint en ce qui concerne le mandat sur les DIB demandé par le SCRS dans le dossier [***] ou les modifications du premier type proposées à trois des mandats décernés dans le dossier [***]

[71] En effet, les autorisations demandées permettraient au SCRS d'obtenir des DIB ayant trait à tout compte de communications qu'il pourrait découvrir dans le cadre d'enquêtes aux paramètres très généraux sur les menaces que le terrorisme islamiste et certaines activités de [***] font peser sur la sécurité du Canada, lorsque le SCRS estime simplement qu'elles lui seront utiles pour l'enquête. Entre autres, le SCRS n'a fourni à la Cour aucune explication lui permettant de comprendre le lien précis entre i) les numéros de téléphones et identificateurs électroniques qu'il pourrait découvrir, pour lesquels il demande d'obtenir les DIB, et ii) ses enquêtes. Le « lien », vaguement défini, a tout simplement une portée excessive et manque de clarté (*R. c. Chehil*, 2013 CSC 49, [2013] 3 R.C.S. 220, aux paragraphes 36 et 51). En outre, il n'est

be satisfied that such BII information is required to enable CSIS to investigate the threat to the security of Canada posed by Islamist terrorism, as contemplated by paragraph 21(2)(a) of the Act.

[72] As I have noted earlier, CSIS has described the threat to the security of Canada in [***] in terms of "activities in paragraph (c) of the definition of 'threats to the security of Canada' found in section 2 of the Act that are [***]

[73] The language of the proposed BII Warrant does not enable the Court to know with which of the [***] identified [***] groups a communications account would be associated. Indeed, it does not even enable the Court to know the [***] to which the telephone number or identifier would pertain. In my view, this does not permit the Court to have a sufficient sense of the nexus between the identified threat-related activities of Islamist terrorism and the individual whose privacy rights would be encroached upon to be considered "reasonable" within the meaning of section 8 of the Charter.

[74] This problem, which is fatal in and of itself, is exacerbated by the fact that one of the clauses in the BII Warrant that I initially assumed would limit, at least to some extent, the scope of the warrant, will not in fact have that effect. Specifically, I had assumed that the words "where a Chief determines that […] the identity of the subscriber to the account will assist in the investigation of Islamist terrorism", would place some important limit on the scope of the warrant. However, Mr. [***] testified that obtaining BII will always assist CSIS's investigation, even if it merely confirms that the individual who is identified through the BII is of no value to the investigation. Mr. [***] explained that even just eliminating a person from further consideration will invariably assist an investigation. The logical extension of that argument is that obtaining the BII corresponding to any and all accounts that are merely identified in the course of an investigation will always assist in that investigation**.**

[75] I will pause here to observe that one of the consequences of a determination that the BII of any account will assist in CSIS's investigation is that CSIS would retain collected information indefinitely. Another conse-

pas assez éloquent pour convaincre la Cour que le SCRS a besoin de ces DIB pour enquêter sur la menace que le terrorisme islamiste fait peser sur la sécurité du Canada, conformément à l'alinéa 21(2)a) de la Loi sur le SCRS.

[72] Comme je l'ai mentionné plus haut, aux fins du dossier [***] le SCRS a défini la « menace envers la sécurité du Canada » comme les activités comprises à l'alinéa c) de la définition de cette expression figurant à l'article 2 de la Loi sur le SCRS qui sont [***]

[73] Le libellé du mandat sur les DIB proposé ne permet pas à la Cour de savoir auxquels de ces [***] groupes [***] un compte de communications serait associé. En fait, il ne permet même pas à la Cour de savoir à quel [***] aurait trait le numéro de téléphone ou l'identificateur. À mon avis, le libellé ne permet pas à la Cour d'assez bien constater le lien entre les activités liées à la menace que constitue le terrorisme islamiste et la personne dont les droits en matière de vie privée seraient enfreints pour qu'elle le considère « non abusif » au sens de l'article 8 de la Charte.

[74] Il s'agit d'un problème rédhibitoire en soi que vient aggraver le fait que l'une des dispositions du mandat sur les DIB que je le croyais à l'origine en limiterait quelque peu sa portée, n'aura finalement pas cet effet. J'avais présumé que le segment [TRADUCTION] « lorsqu'un chef détermine que […] l'identité de l'abonné au compte sera utile pour l'enquête sur le terrorisme islamiste » limiterait de façon importante la portée du mandat. Toutefois, M. [***] a témoigné qu'obtenir des DIB aidera toujours le SCRS à faire progresser son enquête, même si cela ne fait que confirmer que la personne dont il établit l'identité grâce aux DIB n'a aucune utilité pour l'enquête. Selon M. [***] éliminer quelqu'un de la liste des personnes à prendre en considération est, en soi, nécessairement utile à l'enquête. Partant, il est logique de conclure que l'obtention de DIB correspondant à tout compte simplement découvert dans le cadre d'une enquête sera toujours utile à cette enquête.

[75] Je me dois de remarquer que le fait de déterminer que les DIB liées à un compte seront utiles à une enquête du SCRS entraîne des conséquences, notamment celle voulant que le Service conserve indéfiniment les infor-

quence is that such information may well be shared with a foreign intelligence agency.

[76] The same problems exist with the first of the two types of BII authorizations that CSIS requested be added to three of the warrants that were issued in the first phase of [***] I recognize that the threat-related activities in [***] are more narrowly defined than they are in [***] as they are confined to activities of [***] that fall within paragraphs (a) and (b) of the definition of "threats to the security of Canada" set forth in section 2 of the Act. Nevertheless, to the extent that the language of the first group of authorizations sought in the requested warrant amendments in [***] is virtually identical to the language of the BII Warrant being sought in [***] it suffers from the same fatal flaw of overbreadth. This is because the Court has no understanding whatsoever of the specific nexus between the as-yet-to be discovered telephone numbers or electronic identifiers, and CSIS's investigation.

[77] In passing, I will pause to recognize that in exceptional circumstances, CSIS may require BII or similar information in a shorter timeframe than may be needed to obtain a warrant or an amendment to an existing warrant. One such circumstance was the focus of an [***] Warrant that was sought and granted in [***] There, Justice Noël recognized that CSIS needed to be able to investigate threat-related [***] Accordingly, he authorized CSIS to obtain subscriber information [***] during its investigation of the threat to the security of Canada in question, where a regional director general or his designated had reasonable grounds to believe that such information might assist in that investigation. [***] However, CSIS was then subject to a condition that required it to bring a further application to the Court, without delay, to execute the warranted powers in respect of any [***] all as defined in the warrant.

[78] In my view, no exceptional situation of this nature, or any other nature, has been identified in these proceedings.

mations recueillies et, une autre conséquence serait que le SCRS les communique éventuellement à un service de renseignement étranger.

[76] Le premier des deux types d'autorisations relatives aux DIB dont le SCRS a demandé l'ajout à trois des mandats décernés dans le dossier [***] comporte les mêmes problèmes. Je reconnais que, dans ce dossier, les activités liées à la menace sont mieux circonscrites que dans le dossier [***] En effet, elles concernent uniquement les activités [***] qui correspondent aux alinéas a) et b) de la définition de « menaces envers la sécurité du Canada » figurant à l'article 2 de la Loi sur le SCRS. Néanmoins, puisqu'il est pratiquement identique au libellé du mandat sur les DIB demandé dans le dossier [***] le libellé de la première catégorie d'autorisations figurant dans les modifications demandées aux mandats décernés dans le dossier [***] comporte le même défaut rédhibitoire : une portée excessive. En effet, la Cour n'a aucune idée du lien précis entre l'enquête du SCRS et les numéros de téléphones ou identificateurs électroniques susceptibles d'être découverts.

[77] Je reconnais en passant que le SCRS, en des circonstances exceptionnelles, peut avoir besoin de DIB ou d'informations similaires dans un délai plus court que celui qui est nécessaire pour obtenir un mandat ou apporter des modifications à un mandat existant. Je mentionne à titre d'exemple le mandat sur [***] demandé et octroyé dans une telle circonstance dans le dossier [***] Dans ce dossier, le juge Noël avait reconnu que le SCRS devait pouvoir enquêter sur des [***] liées à la menace [***] Il avait donc autorisé le SCRS à obtenir des informations auprès d'un fournisseur de services en ligne sur [***] pendant son enquête sur la menace envers la sécurité du Canada, lorsqu'un directeur général régional ou la personne désignée avait des motifs raisonnables de croire que ces informations pouvaient lui être utiles dans le cadre de l'enquête.[***] Par contre, le SCRS était alors assujetti à une condition exigeant qu'il présente sans tarder une autre demande à la Cour pour exécuter le mandat contre toute [***] termes définis dans le mandat.

[78] À mon avis, aucune situation exceptionnelle de ce genre ou d'une autre nature n'a été constatée en l'espèce.

C. *Can the Court authorize CSIS to obtain BII in respect of communications accounts identified pursuant to its review of specifically defined information obtained in relation to [***] individuals and [***] additional individuals who have been identified [***]*

[79] This issue is raised solely in respect of the second type of BII authorization that CSIS has requested be added to three of the warrants in [***] This authorization would enable CSIS to obtain BII in respect of communications accounts identified pursuant to its review of specifically defined information obtained in relation to [***] named individuals and [***] additional individuals who have been identified [***]

[80] In my view, this authorization does not suffer from the defects described in the preceding section above. It is perhaps for that reason that it was not the subject of significant submissions by the Attorney General or the *amici* in these applications. Accordingly, I will only deal with this type of authorization briefly.

[81] In contrast to the first type of authorization sought in [***] and to the BII Warrant sought in [***] the Court has been provided with the information that it requires to grant the authorization. That is to say, it has been provided with sufficient information to have reasonable grounds to believe that the BII of the specific individuals whose privacy rights would be encroached upon is required to assist CSIS to advance its investigation into [***] threat-related activities.

[82] Specifically, paragraph 10(a) of the [***] would authorize the Director of CSIS and any employee of CSIS acting under his authority to obtain BII in respect of any third party account with a CSP that CSIS may identify during its review of:

i. [***[the identified individuals]***];

ii. [***]

iii. [***]

iv. [***]

C. *La Cour peut-elle autoriser le SCRS à obtenir des DIB liées à des comptes de communications qu'il a découverts en examinant des informations clairement définies ayant trait à [***] personnes identifiées par leur nom et à [***] autres personnes ciblées [***]*

[79] Cette question touche uniquement à l'autorisation du second type, relative aux DIB, dont le SCRS a demandé l'ajout à trois des mandats décernés dans le dossier [***] Elle permettrait au SCRS d'obtenir des DIB liées à des comptes de communications qu'il a découverts en examinant des informations clairement définies ayant trait à [***] personnes identifiées par leur nom et à [***] personnes ciblées [***]

[80] À mon avis, cette autorisation ne comporte pas les défauts dont il est question à la section précédente, ce qui explique peut-être pourquoi elle n'a pas fait l'objet d'observations substantielles par la procureure générale ou les *amici* en l'espèce. Je ne m'y attarderai donc que brièvement.

[81] En l'occurrence, contrairement à l'autorisation du premier type demandée dans le dossier [***] et au mandat sur les DIB demandé dans le dossier [***] la Cour a reçu les informations nécessaires pour accorder l'autorisation, c'est-à-dire qu'elle en a appris suffisamment pour avoir des motifs raisonnables de croire que le SCRS a besoin des DIB liées aux personnes dont les droits en matière de vie privée seraient enfreints pour faire progresser son enquête sur les activités liées à la menace de [***]

[82] En particulier, le paragraphe 10a) du [***] autoriserait le directeur du SCRS et tout employé du SCRS agissant sous son autorité à obtenir des DIB ayant trait à tout compte de tiers auprès d'un FSC que le Service peut découvrir dans le cadre de son examen :

i. [***[personnes identifiées]***]

ii. [***]

iii. [***]

iv. [***]

[83] CSIS seeks to include essentially the same authorization in paragraph 2(a) of the [***] and in paragraph 5(a) of the [***]

[84] The information described at paragraph 82 above all relates directly to [***] individuals who are subjects of investigation. There are reasonable grounds to believe that those individuals may be engaged in activities that constitute threats to the security of Canada. Based on those facts, I am satisfied that CSIS has established reasonable grounds to believe that BII in respect of telephone numbers or electronic identifiers that it may identify, after reviewing the information described at paragraph 82 above, is required to enable CSIS to advance its investigation into the threat-related activities [***]

[85] I will simply add in passing that I am satisfied that the other preconditions to obtaining a warrant, as set forth in paragraph 21(2)(b) of the Act, have been met.

[86] In summary, I will grant the second group of requested amendments to three of the warrants that were previously issued by Justice Noël in [***] to enable CSIS to obtain BII in respect of communications accounts of third parties that may be identified pursuant to its review of the information of the identified individuals that is described at paragraph 82 above.

[87] Nevertheless, I have a concern regarding the potentially large number of third parties whose BII may be obtained by CSIS, as a result of the execution of this BII authorization in respect of the [***] individuals who are targets [***] Those [***] respectively. Given the nature of [***] it is reasonably foreseeable that a potentially large number of members of the public who communicate with those individuals for entirely legitimate purposes will come within the scope of the BII authorization. And once subject to that authorization, their BII may be obtained by CSIS and retained indefinitely. Accordingly, it will be necessary to develop some conditions to address these issues.

[83] Le SCRS cherche à faire ajouter essentiellement la même autorisation au paragraphe 2a) du [***] et au paragraphe 5a) du [***]

[84] Les informations dont il est question au paragraphe 82 ci-haut ont toutes un lien direct avec [***] personnes [***] qui font l'objet d'une enquête. Il existe des motifs raisonnables de croire que ces personnes peuvent mener des activités qui constituent des menaces envers la sécurité du Canada. Me fondant sur ces faits, je suis convaincu que le SCRS a démontré qu'il existe des motifs raisonnables de croire qu'il a besoin des DIB liées à des numéros de téléphone ou à des identificateurs électroniques qu'il pourrait découvrir en examinant les informations dont il est question au paragraphe 82 afin de faire progresser son enquête sur les activités liées à la menace [***]

[85] J'ajoute simplement en passant que je suis convaincu que les autres conditions préalables à l'obtention d'un mandat prévues à l'alinéa 21(2)b) de la Loi sur le SCRS ont été remplies.

[86] En résumé, j'accorderai la deuxième catégorie d'amendements demandés à trois des mandats décernés par le juge Noël au dossier [***] de façon à permettre au SCRS d'obtenir les DIB ayant trait à tout compte de tiers pouvant être identifié à la suite de son examen de l'information des personnes identifiées qui sont décrites plus haut au paragraphe 82.

[87] Néanmoins, je demeure préoccupé par le nombre potentiellement élevé de tierce-parties dont les DIB auraient pu être obtenues par le SCRS, en raison de l'exécution de cette autorisation pour les DIB en lien avec les [***] personnes [***] qui sont des cibles [***] Étant donné [***] il est raisonnablement prévisible qu'un nombre potentiellement élevé de membres du public communiquent avec les [***] à des fins totalement légitimes et, ce faisant, tombent dans le champ d'application de l'autorisation octroyée pour l'obtention de DIB. Une fois assujettie à une telle autorisation, leur DIB pourrait être obtenu et conservé indéfiniment. Par conséquent, il s'avérera nécessaire d'imposer des conditions pour mieux répondre à ces préoccupations.

D. *Can the Court authorize an employee of CSIS to obtain BII of a communications account that corresponds to a telephone number or an electronic identifier, where a "chief" within CSIS determines that the account was identified during its investigation, and that the BII would assist CSIS in its investigation?*

[88] The Attorney General submits that a judge of this Court has the required discretion to allow a designated employee within CSIS to determine whether prescribed circumstances have been met for CSIS to request and obtain BII from a CSP. In this regard, the Attorney General maintains that discretion may rest with those responsible for the execution of a warrant, because such discretion will frequently be necessary. For example, she notes that general warrants issued under the *Criminal Code*, R.S.C., 1985, c. C-46, often allow police a degree of discretion that is reasonably necessary to carry out a search (*R. v. Poirier*, 2016 ONCA 582 (CanLII), at paragraphs 34 and 49), to search things that are not identified in the warrant (*R. v. Noseworthy* (1997), 33 O.R. (3d) 641 (C.A.)), or to search during a timeframe that is not specified in the warrant (*R. v. TELUS Communications Co.*, 2013 SCC 16, [2013] 2 S.C.R. 3, at paragraph 69).

[89] The Attorney General asserts that the discretion being sought is appropriate because of several safeguards that have been put in place to ensure that there is only a minimal impact on any privacy rights that may be engaged as a result of CSIS obtaining access to BII, and to ensure compliance with what the Court will be authorizing. Those safeguards are as follows:

i. Before making a request for BII from a CSP, CSIS will first try to confirm the identity of the subscriber in question by other means.

ii. Each request for BII from a CSP [***]

iii. Before a chief may approve a request for BII, he must be satisfied that the circumstances specified in the warrant exist, namely that (i) the telephone number or [***[electronic identifier]***] was identified in the course of the investigation in question,

D. *La Cour peut-elle autoriser un employé du SCRS à obtenir les DIB liées à un compte de communications correspondant à un numéro de téléphone ou à un identificateur électronique lorsqu'un « chef » au sein du SCRS détermine que ce compte a été découvert lors d'une enquête et que les DIB faciliteraient cette enquête?*

[88] La procureure générale soutient que les juges de la Cour ont le pouvoir discrétionnaire de permettre à un employé désigné du SCRS de déterminer si les circonstances justifient que le Service demande des DIB à un FSC et les obtienne. À cet égard, selon la procureure générale, ce pouvoir peut être exercé par les personnes responsables d'exécuter le mandat, car cela sera souvent nécessaire. À titre d'exemple, elle souligne que les mandats généraux décernés en vertu du *Code criminel*, L.R.C. (1985), ch. C-46, accordent souvent aux forces de police un pouvoir discrétionnaire raisonnablement nécessaire de procéder à une fouille ou à une perquisition (*R. v. Poirier*, 2016 ONCA 582 (CanLII), aux paragraphes 34 et 49), de le faire contre des objets qui ne figurent pas dans le mandat (*R. v. Noseworthy* (1997), 33 O.R. (3d) 641 (C.A.)) ou à un moment qui n'est pas précisé dans le mandat (*R. c. Société TELUS Communications*, 2013 CSC 16, [2013] 2 R.C.S. 3, au paragraphe 69).

[89] La procureure générale soutient que le pouvoir discrétionnaire demandé est adéquat, car certaines mesures ont été prises afin d'assurer que l'obtention de DIB par le SCRS empiète minimalement sur les droits en matière de vie privée et que ceci soit fait en conformité avec ce que la Cour autorisera. Ces mesures sont :

i. Avant de demande des DIB à un FSC, le SCRS essaie d'abord de confirmer l'identité de l'abonné par d'autres moyens.

ii. [***] de chaque demande d'obtention de DIB auprès d'un FSC, [***]

iii. Avant d'approuver la demande d'obtention de DIB, le chef doit être convaincu que les circonstances précisées dans le mandat existent bel et bien, c'est-à-dire i) que le numéro de téléphone ou [***[identificateur électronique]***] a été découvert au cours

and (ii) obtaining the identity of the subscriber will assist in that investigation.

iv. The BII authorization provides that, when CSIS [***]

v. [***]

vi. CSIS will be required to destroy any information provided by a CSP that does not fall within the strict definition of BII.

[90] The *amici* acknowledge that agents of the state such as CSIS may be accorded a certain degree of discretion with respect to the *manner* in which a warrant is executed, including the discretion to do what is reasonably necessary to execute the warranted powers, and some temporal flexibility. However, they maintain that the BII Warrant and the first type of proposed amendments to the warrants that were issued in [***] go far beyond the discretion that may be granted to CSIS with respect to the *execution* of the proposed warranted powers.

[91] I agree. In my view, those proposed authorizations would impermissibly delegate to a person holding the position of "chief" within CSIS a function that must be performed by a designated judge of this Court (*Canadian Security Intelligence Service Act (Re)*, [1998] 1 F.C. 420 (T.D.) , at paragraph 17). That function is the determination of which specific communications accounts will be the subject of requests to CSPs for BII. In the exercise of that function, persons holding the position of "chief" within CSIS would, in essence, make the determination of whether the grounds that must be established before a specific individual's privacy interests can be intruded upon, have been met.

[92] Only a designated judge can make such determinations in respect of the exercise of powers by CSIS that are more than minimally intrusive in nature. In conceding that a warrant is required to obtain the proposed authorizations, the Attorney General has also effectively conceded that those authorizations would be more than minimally intrusive in nature.

de l'enquête et ii) que l'identité de l'abonné sera utile au SCRS dans le cadre de l'enquête.

iv. Conformément à l'autorisation relative aux DIB, le SCRS [***]

v. [***]

vi. Le SCRS est tenu de détruire toute information que lui remet un FSC qui ne correspond pas strictement à la définition de DIB.

[90] Les *amici* reconnaissent que les agents de l'État comme le SCRS peuvent se voir accorder un certain pouvoir discrétionnaire quant à la *manière* d'exécuter un mandat, notamment celui de prendre les mesures raisonnables pour exercer les pouvoirs octroyés, et une certaine souplesse de nature temporelle. Toutefois, ils soutiennent que le mandat sur les DIB et les modifications du premier type proposées aux mandats décernés dans le dossier [***] outrepassent largement le pouvoir discrétionnaire accordé au SCRS quant à l'*exercice* des pouvoirs proposés.

[91] Je suis d'accord. À mon avis, les autorisations proposées auraient pour effet de déléguer de façon inacceptable au titulaire d'un poste de « chef » au SCRS une fonction qui relève exclusivement d'un juge désigné de la Cour (*Loi sur le Service canadien du renseignement de sécurité (Re)*, [1998] 1 C.F. 420 (1re inst.), au paragraphe 17). Cette fonction consiste à déterminer quels comptes de communications en particulier feront l'objet de demandes d'obtention de DIB auprès de FSC. Essentiellement, en exerçant cette fonction, le titulaire d'un poste de « chef » au SCRS déterminerait si les motifs qui doivent être établis avant qu'il soit possible d'enfreindre le droit d'une personne au respect de sa vie privée l'ont bel et bien été.

[92] Seul un juge désigné peut ainsi trancher les questions relatives à l'exercice, par le SCRS, de pouvoirs qui sont plus que minimalement envahissants. La procureure générale a reconnu qu'il faut un mandat pour obtenir les autorisations proposées. Partant, elle admet effectivement que ces autorisations concernent des activités dont les atteintes sont plus que minimales.

[93] An authorization for CSIS to engage in what amounts to a search that is more than minimally invasive in nature must be given by an entirely neutral and impartial arbiter who is capable of acting judicially in balancing the interests of the state against those of the individual whose privacy rights would be encroached upon (*Spencer*, above, at paragraph 68; *Goodwin*, above, at paragraph 56; *Hunter*, above, at pages 160–162; *R. v. Thompson*, [1990] 2 S.C.R. 1111, at page 1134; *Grabowski v. The Queen*, [1985] 2 S.C.R. 434, at pages 445–446).

[94] An individual holding the position of chief within CSIS is not capable of acting judicially in this regard, because such individuals cannot neutrally and impartially conduct that balancing exercise. As employees of CSIS, they are not neutral or independent in the sense required by the jurisprudence. In other words, the nature of their investigative functions "ill-accords with the neutrality and detachment necessary to assess whether the evidence reveals that the point has been reached where the interests of the individual must constitutionally give way to those of the state" (*Hunter*, above, at page 164; *R. v. Généreux*, [1992] 1 S.C.R. 259, at pages 311–312).

[95] This is borne out by the testimony provided by Mr. [***] regarding the likely incentives of an individual holding the position of chief within CSIS. For example, at one point during the hearing, Mr. [***] stated:

> I think the Chief's incentive is the same as everybody else's incentive. It's to determine whether or not there is a threat activity going on, to determine whether or not there is a threat to national security, and if so, to be in a position to investigate it and thereby be able to inform the government.

[96] In response to further questioning from the Court on this point, he stated:

> To me the calculus on this one is very easy. The risk of not pursuing means I have a potential threat that I know nothing about, and I'm not willing to live with that.

[97] Elsewhere, he observed:

[93] Pour mener une activité assimilable à une fouille ou à une perquisition plus que minimalement envahissante, le SCRS doit en recevoir l'autorisation par un arbitre tout à fait neutre et impartial qui est en mesure d'exercer des fonctions judiciaires en établissant un équilibre entre les intérêts de l'État et ceux de la personne dont les droits à la vie privée seront atteints (*Spencer*, précité, au paragraphe 68; *Goodwin*, précité, au paragraphe 56; *Hunter*, précité, aux pages 160 à 162; *R. c. Thompson*, [1990] 2 R.C.S. 1111, à la page 1134; et *Grabowski c. La Reine*, [1985] 2 R.C.S. 434, aux pages 445 et 446).

[94] Le titulaire d'un poste de chef au SCRS n'est pas en mesure d'exercer des fonctions judiciaires à cet égard, car il ne peut pas établir cet équilibre de façon neutre et impartiale. À titre d'employé du SCRS, il n'est ni neutre ni indépendant au sens exigé par la jurisprudence. Autrement dit, la nature de ses fonctions d'enquête « cadre mal avec la neutralité et l'impartialité nécessaires pour évaluer si la preuve révèle qu'on a atteint un point où les droits du particulier doivent constitutionnellement céder le pas à ceux de l'État » (*Hunter*, précité, à la page 164 et *R. c. Généreux*, [1992] 1 R.C.S. 259, aux pages 311 et 312).

[95] Cela est corroboré par le témoignage de M. [***] concernant les motivations probables du titulaire d'un poste de chef au SCRS. Par exemple, pendant l'audience, M. [***] a dit :

> [TRADUCTION] [J]e crois que les motivations d'un chef sont les mêmes que celles de toute autre personne. Il veut déterminer si une activité liée à une menace se déroule, s'il existe une menace envers la sécurité nationale et, dans l'affirmative, il souhaite être en mesure de faire enquête et, donc, d'en aviser le gouvernement.

[96] En réponse à d'autres questions de la Cour sur ce point, il a indiqué que :

> [TRADUCTION] [S]elon moi, la situation est très simple. Si je ne procède pas, je risque de me retrouver en présence d'une menace possible dont j'ignore tout, et je ne suis pas prêt à vivre avec une telle réalité.

[97] Il observe plus loin que :

> … I am not sure that the risk that the Chief would be assessing would be the risk of doing it but perhaps the risk of not doing it.
>
> If we had a situation where there is a piece of information that is missing from the puzzle and I believe as the Chief, if I am signing this, that to get that piece of information will advance my investigation and allow me to have a better overview of the situation, then the risk of not doing that is I can't do my job. I can't provide that value added advice to the Government of Canada. I can't tell them what the threat is.

[98] In my view, it is readily apparent from the foregoing passages of Mr. [***] testimony that a chief within CSIS would have a bias towards authorizing the obtaining of BII from a CSP any time that he thought that this would advance CSIS's investigation. And as discussed at paragraph 74 above, Mr. [***] also testified that obtaining BII would *always* advance CSIS's investigation, even where it simply assists CSIS to determine that the individual behind a telephone number or electronic identifier is not involved in threat-related activities, and therefore cannot provide information that will assist CSIS to advance its investigation.

[99] In summary, this Court cannot authorize an employee within CSIS to obtain BII corresponding to a telephone or an electronic identifier, where a "chief" within CSIS determines that the account was identified during its investigation, and that the BII would assist CSIS in its investigation. Determinations as to which specific communications accounts may be the subject of requests to CSPs for BII must be made by a designated judge of this Court. Allowing such determinations to be made by a chief within CSIS would constitute an impermissible delegation of the Court's responsibility to determine whether the grounds to be met before an individual's privacy interests can be intruded upon, have been met. Moreover, chiefs within CSIS would not have the required degree of neutrality and impartiality to perform this important function.

[100] In my view, all of the foregoing is rendered even more troublesome by (i) the very broad definition of

> [TRADUCTION] […] je ne suis pas persuadé que le chef évaluerait le risque de passer à l'action, mais plutôt le risque de ne rien faire.
>
> Si nous nous trouvions dans une situation où il manque une pièce du casse-tête, et si je croyais, à titre de chef, qu'accorder l'autorisation d'obtenir cette pièce permettrait à l'enquête de progresser et à moi-même d'avoir un meilleur aperçu de la situation, je risquerais, en ne prenant pas cette mesure, de ne pas faire mon travail, donc, de n'avoir aucun conseil à valeur ajoutée à offrir au gouvernement du Canada et de ne pas être en mesure de lui indiquer la nature de la menace.

[98] Selon moi, ces passages du témoignage de M. [***] indiquent de toute évidence qu'un chef au SCRS aurait tendance à autoriser l'obtention de DIB auprès d'un FSC lorsqu'il serait d'avis que cela permettrait de faire progresser une enquête du Service. Comme il en est question au paragraphe 74 ci-haut, M. [***] a également témoigné que l'obtention de DIB fait *toujours* progresser une enquête du SCRS, même si elle lui permet simplement de déterminer que la personne liée au numéro de téléphone ou à l'identificateur électronique n'est impliquée dans aucune activité liée à la menace et ne peut donc pas fournir des informations utiles au SCRS pour son enquête.

[99] En résumé, la Cour ne peut pas autoriser un employé du SCRS à obtenir des DIB liées à un numéro de téléphone ou à un identificateur électronique lorsqu'un « chef » au SCRS détermine que le compte de communications a été découvert dans le cadre d'une enquête et que ces DIB faciliteraient l'enquête du Service. Il est du ressort d'un juge désigné de la Cour de déterminer quels comptes de communication en particulier peuvent faire l'objet d'une demande de DIB auprès d'un FSC. Permettre à un chef au SCRS de prendre cette décision constituerait une délégation inacceptable de la responsabilité de la Cour, qui consiste à déterminer si les motifs qui doivent exister pour qu'il soit possible d'enfreindre le droit d'une personne au respect de sa vie privée ont bel et bien été établis. En outre, les chefs au SCRS ne disposent pas de la neutralité et de l'impartialité nécessaires pour assumer cette fonction importante.

[100] Selon moi, ce qui précède est encore plus problématique en raison i) de la définition très vaste de

Islamist terrorism that CSIS has adopted, (ii) the fact that CSIS would indefinitely retain all of the BII that it seeks to obtain under the requested authorizations, and (iii) the fact that there would be no limit whatsoever on CSIS's ability to share that information with foreign intelligence agencies.

[101] The defects identified above do not exist with respect to the second type of authorization that CSIS has sought in [***] This is because the Court is able to perform, *in advance*, the required balancing assessment in respect of the privacy rights of the ascertainable, but yet-to-be identified third parties behind those telephone numbers and electronic identifiers, and the interests of the state. As in *Thompson*, above, those yet-to-be identified third parties can be ascertained and circumscribed by reference to their communications with known subjects of investigation who have been identified in the warrant (*Thompson*, above, at pages 1134–1135).

[102] In brief, once the Court is satisfied that there are reasonable grounds to believe that the identified individuals are engaged in activities that may pose a threat to the security of Canada, it has a specific basis upon which to be satisfied on that basis alone that there are reasonable grounds to believe that third parties, with whom the Identified Individuals are communicating, may have information that will assist CSIS to advance its investigation, and that, therefore, CSIS requires the BII in question in order to advance its investigation.

VI. Conclusion

[103] For the reasons set forth in Parts V.B and D above, the Court cannot provide the broad authorization that CSIS has sought in the BII Warrant and in the first type of proposed amendments to three of the warrants that were issued in the first phase of [***]

[104] This is so for two principal reasons. First, CSIS has not established and described the specific and required nexus between (i) the future telephone numbers and electronic identifiers that it may identify, and in respect of which it would like to be authorized prospectively to

terrorisme islamiste que le SCRS a adopté, ii) du fait que le SCRS pourrait conserver indéfiniment toutes les DIB obtenues au titre des autorisations demandées et iii) du fait que le SCRS pourrait, sans aucune limite, communiquer ces informations à des services de renseignement étrangers.

[101] L'autorisation du second type demandée par le SCRS dans le dossier [***] ne comporte pas les problèmes susmentionnés, car la Cour peut effectuer, *au préalable*, l'évaluation requise pour établir l'équilibre entre les intérêts de l'État et les droits en matière de vie privée des tiers toujours non-identifiés, mais tout de même vérifiables, liés de façon vérifiable aux numéros de téléphone et aux identificateurs électroniques. Comme dans l'arrêt *Thompson*, précité, ces tiers toujours non-identifiés peuvent être repérés avec précision grâce à leurs communications avec des cibles connues que le mandat vise nommément (*Thompson*, précité, aux pages 1134 et 1135).

[102] En bref, lorsqu'elle est convaincue qu'il existe des motifs raisonnables de croire que les personnes identifiées participent à des activités qui peuvent constituer une menace envers la sécurité du Canada, la Cour dispose d'un motif précis et suffisant de croire que les tiers avec qui ces Personnes identifiées communiquent peuvent détenir des informations qui aideront le SCRS à faire progresser son enquête et que, partant, ce dernier a besoin de ces DIB pour faire progresser son enquête.

VI. Conclusion

[103] Pour les motifs énoncés aux parties V.B. et D ci-haut, la Cour ne peut pas accorder les vastes autorisations demandées par le SCRS dans le mandat sur les DIB et la première catégorie de modifications qu'il souhaite faire apporter à trois des mandats décernés à la première étape de l'instance dans le dossier [***]

[104] Cela s'explique par deux raisons principales. Premièrement, le SCRS n'a ni établi ni décrit le lien précis qui doit exister entre i) les numéros de téléphone et identificateurs électroniques qu'il pourrait trouver et pour lesquels il veut être autorisé de manière prospective

obtain BII, and (ii) its investigations into Islamist terrorism, or the threat-related activities [***] respectively. The loosely defined "nexus" that CSIS has described is simply too broad and nebulous. Moreover, CSIS has not provided sufficient information for the Court to be satisfied that BII is required to enable it to investigate the threats to the security of Canada posed by Islamist terrorism and [***] as contemplated by paragraph 21(2)(a) of the Act.

[105] Second, that proposed authorization would impermissibly delegate to a person holding the position of "chief" within CSIS a function that must be performed by a designated judge of this Court. That function is the determination of whether the grounds that must be established before a specific individual's privacy interests can be intruded upon, have been met. Quite apart from the fact that this is a function that must be performed by a designated judge of this Court, a chief within CSIS is not capable of making the required determination in a neutral and unbiased manner, as required by section 8 of the Charter.

[106] However, for the reasons set forth in Part V.C above, the Court is able to authorize the second group of amendments that CSIS has proposed be made to the warrants that were granted in [***] This is because CSIS has established reasonable grounds to believe that BII information in respect of telephone numbers or electronic identifiers that it may identify after reviewing the information described at paragraph 82 above, is required to enable CSIS to advance its investigation. That information all relates directly to [***] Identified Individuals who are subjects of investigation.

[107] Given the conclusion that I have reached with respect to the BII Warrant and the first group of amendments that CSIS has proposed in [***] it will be necessary for CSIS to seek an authorization from the Court each time it identifies additional telephone numbers or electronic identifiers in respect of which it wishes to obtain BII from a CSP. At that time, CSIS will have to establish a sufficient nexus between the telephone number or other identifier in question and its investigation to satisfy the Court that there are reasonable grounds to

à obtenir les DIB, et ii) ses enquêtes sur le terrorisme islamiste ou sur les activités liées à la menace [***] Le « lien » vaguement défini par le SCRS a tout simplement une portée excessive et manque de clarté. De plus, le Service n'a pas fourni suffisamment d'informations à la Cour pour la convaincre que les DIB sont nécessaires pour enquêter sur les menaces que le terrorisme islamiste et [***] font peser sur la sécurité du Canada, conformément à l'alinéa 21(2)a) de la Loi sur le SCRS.

[105] Deuxièmement, l'autorisation proposée entraînerait de façon inacceptable la délégation, au titulaire d'un poste de « chef » au SCRS, d'une fonction qui doit être exercée par un juge désigné de la Cour, c'est-à-dire déterminer si les motifs qui doivent être établis avant qu'il soit possible d'enfreindre le droit d'une personne au respect de sa vie privée l'ont bel et bien été. Outre le fait que cette fonction incombe exclusivement à un juge de la Cour, il demeure qu'un chef au SCRS n'est pas en mesure de prendre une telle décision de façon neutre et impartiale, comme l'exige l'article 8 de la Charte.

[106] Toutefois, pour les motifs énoncés à la partie V.C., la Cour peut autoriser la deuxième catégorie de modifications que le SCRS désire faire apporter aux mandats décernés dans le dossier [***] En effet, le Service a démontré qu'il existe des motifs raisonnables de croire que les DIB liées aux numéros de téléphone ou identificateurs électroniques qu'il peut trouver en examinant les informations mentionnées au paragraphe 82 ci-haut lui sont nécessaires pour faire progresser son enquête. Ces informations ont toutes un lien direct avec [***] Personnes identifiées qui font l'objet de l'enquête.

[107] Compte tenu de ma conclusion quant au mandat sur les DIB et la première catégorie de modifications proposée par le SCRS dans le dossier [***] ce dernier devra obtenir une autorisation de la Cour chaque fois qu'il trouvera d'autres numéros de téléphone ou identificateurs électroniques pour lesquels il veut obtenir des DIB auprès d'un FSC. Le SCRS devra alors établir un lien suffisant entre le numéro de téléphone ou l'identificateur électronique et son enquête pour convaincre la Cour qu'il existe des motifs raisonnables de croire qu'il

believe that CSIS requires the BII of the corresponding communications account to advance its investigation.

[108] This is subject to the *proviso* that CSIS need not return to the Court when it has already obtained an advance authorization to obtain the BII of communications accounts corresponding to the telephone numbers or electronic identifiers of ascertainable, but yet-to-be identified individuals, such as those described in paragraphs 65–69 and 101–102 above.

[109] I recognize that the conclusion I have reached will likely impose an additional burden on CSIS. I also recognize that this may give rise to additional costs and delays associated with obtaining BII authorizations in relation to telephone numbers or electronic identifiers that may come to CSIS's attention during the course of its investigations into Islamist terrorism and the threat-related activities [***] and which are not linked with a target that is the subject of a warrant. Given the adverse implications that the potential delays, in particular, may have for CSIS's ability to investigate threat-related activities, the Court will remain open to considering alternate approaches that are Charter compliant.

[110] In this regard, I note that CSIS already has an internal process in place that requires those who wish to seek warrant powers to explain why they require BII in respect of a telephone number or an electronic identifier that has been identified in the course of an investigation. Those explanations are provided in [***] forms, a number of examples of which were provided to the Court in the course of these applications. In my view, many of the examples of [***] forms provided to the Court contain sufficient information to provide the Court with reasonable grounds to believe that the BII in question was required to enable CSIS to investigate the threat-related activities of Islamist terrorism and [***]

[111] I find it difficult to understand why it would require substantial time and effort to provide the Court with essentially the same information that has already been prepared by CSIS internally. If such information were simply provided by way of a supplementary affidavit, together with a proposed amendment to an existing

a besoin des DIB liées aux comptes de communication connexes pour faire progresser son enquête.

[108] Je précise toutefois que le SCRS n'a pas besoin de s'adresser de nouveau à la Cour lorsqu'il a déjà été autorisé à obtenir les DIB liées à des comptes de communications correspondant aux numéros de téléphone ou aux identificateurs électroniques de tiers toujours non-identifiés, mais tout de même vérifiable, comme ceux qui sont mentionnés aux paragraphes 65 à 69 et 101 à 102 des présents motifs.

[109] Je reconnais que ma conclusion imposera probablement un fardeau supplémentaire au SCRS. Je reconnais également qu'elle peut entraîner l'accroissement des coûts et des délais relatifs aux demandes d'autorisations d'obtenir des DIB liées [***] identificateurs [***] qui pourraient attirer l'attention du SCRS lors de ses enquêtes sur le terrorisme islamiste et les activités liées à la menace [***] mais qui n'ont pas trait à la cible d'un mandat. Puisque de possibles retards peuvent nuire à la capacité du SCRS d'enquêter sur des activités liées à la menace, la Cour demeure disposée à étudier d'autres approches qui seraient conforme aux exigences prévues à la Charte.

[110] À ce propos, je souligne que le SCRS s'est doté d'une procédure interne qui exige des personnes qui souhaitent présenter une demande de mandat qu'elles donnent les raisons pour lesquelles elles ont besoin des DIB liées à un numéro de téléphone ou à un identificateur électronique découvert dans le cadre d'une enquête. Elles donnent ces explications dans le [***] dont des exemples ont été fournis à la Cour en l'espèce. À mon avis, bon nombre de [***] données en exemple à la Cour comportent suffisamment d'informations pour lui donner des motifs raisonnables que le SCRS avait besoin des DIB pour enquêter sur les activités liées à la menace [***] et des acteurs du terrorisme islamiste.

[111] Je trouve ça difficile de comprendre pourquoi il faudrait qu'il faille beaucoup de temps et d'efforts pour fournir à la Cour des informations qui ont essentiellement déjà été préparées au SCRS. S'il fournissait simplement ces informations dans un affidavit supplémentaire en compagnie d'une proposition de modification à mandat

warrant, the time and effort that would be required on CSIS's part may not be unduly onerous at all.

JUDGMENT in [***]

THIS COURT'S JUDGMENT is that this application is dismissed.

JUDGMENT in [***]

THIS COURT'S JUDGMENT is that this application is dismissed in part.

Specifically:

1. For the reasons provided in Parts V.B. and D. of the attached judgment and reasons, the following amendments that the Attorney General has sought to three of the warrants that were issued by Justice Noël during the first phase of this application will be not be granted:

    i. [***] new paragraph 10(b);

    ii. [***] new paragraph 5(b);

    iii. [***] new paragraph 2(b));

2. For the reasons provided in Part V.C. of the attached judgment and reasons, the other amendments that the Attorney General has sought to the aforementioned warrants will be granted.

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

existant, le SCRS pourrait ne pas trouver excessifs du tout le temps et les efforts nécessaires.

JUGEMENT DANS [***]

LE JUGEMENT DE CETTE COUR est que la demande est rejetée.

JUGEMENT DANS [***]

LE JUGEMENT DE CETTE COUR est que cette demande est rejetée en partie.

Plus précisément :

1. Pour les motifs prévus aux parties V.B. et D du jugement et motifs ci-joint, les amendements que la procureur générale avait demandé à trois des mandats qui avaient été décernés par le juge Noël à la première phase de cette demande ne seront pas accueillis :

    i. [***] nouveau paragraphe 10(b);

    ii. [***] nouveau paragraphe 5(b);

    iii. [***] nouveau paragraphe 2(b);

2. Pour les motifs prévus à la Partie V.C au jugement et motifs ci-joint, les autres amendements que la procureur générale a demandés aux mandats précités seront décernés.

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

APPENDIX I

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

Definitions

2 In this Act,

…

threats to the security of Canada means

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

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

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

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

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

…

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

ANNEXE I

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

Définitions

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

[…]

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

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

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

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

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

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

[…]

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

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.

…

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;

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.

[…]

Contrôle judiciaire

Demande de mandat

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

Contenu de la demande

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

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

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

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

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

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

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

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

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

Issuance of warrant

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

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

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

(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.

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

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

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

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

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

Délivrance du mandat

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

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

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

c) 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.

Matters to be specified in warrant

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

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

(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.

Contenu du mandat

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

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

b) 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.