(La version française suit)

Disclaimer:

The attached or following information, regardless of format, is provided solely for the purpose of research or private study; any other use may require the authorization of the copyright owner. Digital reproductions of print material are provided for convenience; in the case of any inconsistency between the digital version and the original print version, the original print version shall prevail.

Avertissement :

L'information qui suit ou qui se trouve en pièce jointe, quel qu'en soit le format, n'est fournie qu'à des fins de recherche ou d'études privées : tout usage à d'autres fins pourrait requérir l'autorisation du détenteur du droit d'auteur. Les versions numérisées des documents imprimés sont fournies par souci de commodité : en cas d'écart entre la version numérisée et la version imprimée, c'est cette dernière qui fait foi.

ORDER/ADDRESS OF THE HOUSE OF COMMONS
ORDRE/ADRESSE DE LA CHAMBRE DES COMMUNES

NO.-N°	BY / DE	DATE
Q-942	Mr. Dubé (Beloeil—Chambly)	March 22, 2017/Le 22 mars 2017

RETURN BY THE LEADER OF THE GOVERNMENT IN THE HOUSE OF COMMONS
DÉPÔT DU LEADER DU GOUVERNEMENT À LA CHAMBRE DES COMMUNES

Mr. Lamoureux

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENT SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

MAY 08 2017

(TABLED FORTHWITH / DÉPOSÉ AUSSITÔT)

House of Commons
Chambre des communes
Canada

INQUIRY OF MINISTRY
DEMANDE DE RENSEIGNEMENT AU GOUVERNEMENT

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

QUESTION NO./Nº DE LA QUESTION	BY / DE	DATE
Q-942[2]	Mr. Dubé (Beloeil-Chambly)	March 22, 2017

Reply by the Minister of Public Safety and Emergency Preparedness
Réponse du Ministre de la Sécurité publique et de la Protection civile

The Honourable Ralph Goodale, P.C., M.P.

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

QUESTION

With respect to the acquisition and retention of data, including associated data, metadata, bulk data, or any other kind of data by the Canadian Security Intelligence Service (CSIS): (*a*) how many internal data repositories does CSIS have access to; (*b*) what are the different kinds of internal data repository to which CSIS has access; (*c*) are there any data repositories that have been accessed by CSIS, whether internal or external, that are housed within servers that do not belong to CSIS; (*d*) what is the difference, according to CSIS, between the terms "associated data" and "metadata"; (*e*) what is the exhaustive list of organizations with which CSIS shares information, including bulk data, metadata, associated data and any other data to which CSIS has access; (*f*) what is the exhaustive list of organizations, including telecommunications companies, financial institutions, government departments, and other organizations, with which CSIS communicates for purposes other than the sharing of information; - **See full text of the question attached.**

REPLY / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [X]
TRANSLATION / TRADUCTION [ ]

Canadian Security Intelligence Service (CSIS)

(a)-(c) CSIS's mandate is to investigate and to inform the government of threats to the security of Canada, which are defined in section 2 of the *CSIS Act*. In order to fulfill this mandate, CSIS is authorized in section 12, to collect, to the extent strictly necessary, and analyze and retain information on activities suspected of constituting a threat to the security of Canada. CSIS' collection and retention activities are further subject to robust internal policies and procedures.

Due to the classified nature of its work, CSIS is limited in the amount of detail it can publically disclose as it relates to the different types of information it collects, analyzes and retains. It must be noted though that the Security Intelligence Review Committee (SIRC) has the authority to review all material held by CSIS, with the exception of documents classified as Cabinet Confidence. Further, the Office of the Privacy Commissioner (OPC) has been briefed on the CSIS' collection, retention, and analysis of associated data prior to and following the Federal Court's decision. CSIS continues to engage and cooperate with the OPC on this matter.

.../2

(d) Associated data and metadata are synonymous. They both refer to the context, not the content of a communication. CSIS has used the term associated data to refer to metadata associated to a communication intercepted pursuant to a warrant.

(e)(f) For clarification, CSIS uses the term 'datasets' when referencing data SIRC has referred to as 'bulk data.' It is also worth noting that, in response to SIRC's report regarding the Operational Data Analytics Center's (ODAC) non-warranted collection of datasets, CSIS implemented a robust policy framework, which ensures that the "strictly necessary" threshold and privacy considerations are assessed in each case.

Any cooperation with foreign and domestic government partners must be conducted in accordance with the provisions in the *CSIS Act*, which includes the requirement to seek authorization from the Minister of Public Safety and Emergency Preparedness and, in the case of foreign arrangements, consultation with the Minister of Foreign Affairs. As part of this cooperation, CSIS may share information with these partners, however, it is important to note that CSIS does not share raw associated data with foreign or domestic partners; rather, assessment products which are only determined to be related to a threat.

CSIS' relationships with its foreign partners are classified and not publicly identified. To do so could hamper its ability to liaise with such agencies in order to obtain security intelligence information relevant to the national security of Canada and Canadian interests. This said, CSIS can state that it has more than 300 foreign relationships with some 150 countries.

CSIS regularly cooperates with domestic government partners and has arrangements with 16 federal government departments, including the Canada Border Services Agency, the Canada Revenue Agency, the Canadian Armed Forces, the Canadian Food Inspection Agency, the Canadian Nuclear Safety Commission, the Communications Security Establishment, the Department of Finance, the Department of Health, the Department of National Defence, the Department of Public Safety and Emergency Preparedness, the Department of Transport, the Financial Transactions and Reports Analysis Centre of Canada, the Department of Foreign Affairs, Trade and Development, The Department of Immigration, Refugees, and Citizenship, the Public Health Agency of Canada, and the Royal Canadian Mounted Police. In addition, CSIS has arrangements with all provinces, as well as the Yukon and Northwest Territories.

As it relates to cooperation with non-governmental organizations, including the private sector, any cooperation must adhere to the requirements of the *CSIS Act*. When CSIS is in possession of a Federal Court warrant, it may rely in part on the cooperation of the private sector to bring effect to the warranted collection. Nonetheless, details regarding cooperation with the private sector related to operational activity remains classified.

(g)(h) Ministers of Public Safety have, through various means, including section 33 and section 6(4) reports, been informed of CSIS' data analysis program since its creation. It must be noted that, in 2006, the Minister of Public Safety and Emergency Preparedness was briefed, via memo, on the creation of this program (ODAC). CSIS also provided a verbal, in-house briefing on ODAC to the Minister of Public Safety in 2010.

.../3

On September 19, 2016, the Minister of Public Safety and Emergency Preparedness was briefed via memo on the SIRC 2015-2016 Annual Report and key outcomes of SIRC's review, which included a review of bulk datasets as referred to by SIRC.

(i)(j)(k)

Given its mandate and specific operational requirements, CSIS does not publically disclose details related to operational activity. To do so would compromise the integrity of CSIS investigations and jeopardize its ability to fulfill the mandate ascribed by Parliament.

It must however be noted that CSIS has shared a list of its operational datasets currently used by ODAC to support data analytics with the OPC as well as SIRC to inform their respective classified reviews. Additionally, all data collection and retention practices are subject to robust internal policies and procedures informed by Ministerial Direction, relevant Canadian legislation, and decisions of the Courts.

(l) Given its mandate and specific operational requirements, CSIS does not publically disclose details related to operational activity, including numerical breakdowns of its warranted collection. However, it is important to note that in pursuit of its mandate, CSIS employs a variety of warranted and non-warranted methods of collecting information in accordance with the law.

(m)-(p)

As previously mentioned, when in possession of a Federal Court warrant, CSIS may cooperate with other public or private sector entities in order to bring effect to the warranted collection. Each interaction is governed by the *CSIS Act*, related Ministerial Direction and is subject to strict policies and guidelines. Pursuant to Section 21 of the *CSIS Act*, it may apply for a warrant when intrusive methods are required to investigate a threat to the security of Canada. These applications may only be submitted after receiving approval from the Minister of Public Safety and Emergency Preparedness. However, given its mandate and specific operational requirements, CSIS does not publically disclose details related to operational activity.

(q) Details regarding investigations undertaken in accordance with the *CSIS Act* remain classified and cannot be disclosed in a public forum. This said, data analytic programs are essential to support modern intelligence investigations; indeed, virtually all Western intelligence services have developed advanced data analytic capabilities to identify patterns of movement, communications, behaviours, links, and significant trends that are otherwise unidentifiable. CSIS' use of data analytics is in accordance with the law and is subject to review by SIRC and the OPC.

(r)-(t) CSIS is unable to disclose specific details of its data analytics programs as this information is classified. However, since 2015, CSIS has provided SIRC a list of datasets ODAC uses to support data analytics. The Service has agreed to update this information on an annual basis, and CSIS will continue to do so in order to support transparency without compromising its role in investigating threats to the security of Canada.

(u) The SMART data collection methodology is a project management framework used to identify critical acquisition issues and develop a framework for obtaining datasets. SMART is a methodology that is commonly used within the business community. It must be noted that CSIS' activities, including its collection of data, are undertaken in a manner that is consistent with the *CSIS Act*, relevant Canadian legislation, as well as internal policies and procedures. CSIS has also implemented a policy framework which ensures that the 'strictly necessary' threshold and privacy considerations are assessed in each case.

(v) When required and with the approval of the Minister of Public Safety and Emergency Preparedness, CSIS may make an application to the Federal Court to obtain warrants against subjects of investigation. These warrants, which are granted by the Federal Court, authorize the use of specific investigative techniques in accordance with conditions identified by the Court, as appropriate, and may include the interception of communications. When CSIS intercepts communications, it obtains the content, as well as the associated data linked with that communication. Separately, CSIS may collect datasets under the authority of the *CSIS Act*. CSIS maintains robust internal policies and procedures developed in accordance with all legislative requirements as well as those outlined in relevant Ministerial Direction.

(w)(x) CSIS is constantly reviewing its internal policies and practices to ensure its activities are undertaken in accordance with legislative requirements, including the requirements of the *CSIS Act*. Specifically, following the October 4, 2016, Federal Court decision, CSIS halted internal use and analysis of associated data obtained via warranted collection of communications to assess the impact of the decision and determine a way forward that complies with the Court's ruling. As of March 2017, CSIS implemented new retention practices for associated data collected under warrant to comply with the Court's ruling.

This will enable ODAC to recommence its analysis of newly acquired associated data in accordance with the Court's decision. To be clear, where it is determined that the associated data is not of use to an investigation, it will be destroyed in accordance with the timeframes established by the Court. ODAC's historical metadata holdings remain fenced off and unavailable for use, until a final decision regarding their disposition is made.

With regards to the Federal Court's decision, it is important to note that all associated data was collected legally via warrant. The Federal Court's key concern related to CSIS' retention of non-threat-related associated data linked to third party communications. The Court determined that CSIS' retention of associated data linked to third party communications found to be unrelated to threats or of no use to an investigation, prosecution, national defence or international affairs, was not compliant with the *CSIS Act*.

Further, in response to SIRC's report regarding ODAC's non-warranted collection of datasets, CSIS implemented a robust policy framework, to ensure that the 'strictly necessary' threshold and privacy considerations are assessed.

(y) CSIS' internal policies and practices are classified, however, CSIS can confirm that it initiated a review of the business and technical systems used for the collection, retention or destruction of information acquired pursuant to a warrant to identify and address any gaps. As a result CSIS is updating relevant policies and procedures and establishing the requisite governance systems to ensure ongoing compliance.

Q-942[2] — March 22, 2017 — Mr. Dubé (Beloeil—Chambly) — With respect to the acquisition and retention of data, including associated data, metadata, bulk data, or any other kind of data by the Canadian Security Intelligence Service (CSIS): (*a*) how many internal data repositories does CSIS have access to; (*b*) what are the different kinds of internal data repository to which CSIS has access; (*c*) are there any data repositories that have been accessed by CSIS, whether internal or external, that are housed within servers that do not belong to CSIS; (*d*) what is the difference, according to CSIS, between the terms "associated data" and "metadata"; (*e*) what is the exhaustive list of organizations with which CSIS shares information, including bulk data, metadata, associated data and any other data to which CSIS has access; (*f*) what is the exhaustive list of organizations, including telecommunications companies, financial institutions, government departments, and other organizations, with which CSIS communicates for purposes other than the sharing of information; (*g*) when were Cabinet Ministers informed of CSIS's collection of bulk data, and with relation to their notification, (i) who were those Ministers, (ii) what were the forms of communication through which they were informed, (iii) what were the dates on which each Minister was informed, starting from January 1, 2006, until December 31, 2016, inclusively; (*h*) when were Cabinet Ministers informed of the methodologies employed by CSIS for the purpose of the collection of bulk data, (i) who were those Ministers, (ii) what were the forms of communication through which they were informed, (iii) what were the dates on which each Minister was informed, starting from November 4, 2015, until the present time; (*i*) with respect to the bulk data that CSIS has collected or otherwise has or has had access to, does it include (i) communications metadata, (ii) travel information, (iii) passport data, (iv) law enforcement wiretaps, (v) arrest records, (vi) financial transactions, (vii) information collected from social media, (viii) medical data, (ix) other kinds of bulk data that CSIS have access to; (*j*) what are the descriptions of all the different methods through which this bulk data is collected; (*k*) what is the exhaustive list of sources of bulk data that CSIS has access to, and how many times were bulk data collected starting from January 1, 2006, until December 31, 2016, inclusively; (*l*) how many judicial warrants were given to CSIS for the purpose of acquisition of bulk data starting from January 1, 2006, until December 31, 2016, inclusively, and when were these warrants received by CSIS; (*m*) how many (i) telecommunications companies, (ii) financial institutions, (iii) medical institutions, (iv) airports, (v) other companies, were compelled or requested to provide access to bulk data, associated data, metadata or any other kind of data to CSIS; (*n*) what are the kinds of leverage that CSIS employs in order to request or compel the acquisition of data from external data suppliers, (i) how many judicial warrants were obtained by CSIS for the collection of such data from private entities, (ii) has CSIS ever collected or had access to any such data without obtaining judicial warrants beforehand; (*o*) how many government departments or agencies were compelled or requested to (i) transfer bulk data, associated data, metadata or any other kind of data to CSIS, (ii) grant access to such data to CSIS, starting from January 1, 2006, until December 31, 2016, inclusively; (*p*) how many judicial warrants were obtained by CSIS for the collection of such data from government departments or entities, and has CSIS ever collected or had access to any such data without obtaining judicial warrants beforehand; (*q*) how many investigations has the use of bulk data helped in during the period starting from January 1, 2006, until December 31, 2016, inclusively, and how many individuals were the subjects of these investigations; (*r*) how many datasets or data repositories are housed within the Operational Data Analysis Centre, and how many of these data sets or data repositories include bulk data; (*s*) how many datasets or data repositories are housed in internal CSIS servers; (*t*) what are the approximate percentages of (i) bulk data, (ii) associated data, (iii) metadata, (iv) any other data that are housed within the servers mentioned in (*s*); (*u*) what is the description of the SMART data collection methodology employed by CSIS, and what kinds of data does this methodology collect; (*v*) what are all the steps involved in obtaining validation of authority to collect any kind of data; (*w*) has all information collected by CSIS since November 3, 2016, passed the "strictly necessary" test, as stipulated in Section 12(1) of the *CSIS Act*; (*x*) has all information retained by CSIS since November 3, 2016, passed the "strictly necessary" test, as stipulated in Section 12(1) of the *CSIS Act*; and (*y*) in light of the ruling by the Federal Court of Canada on the illegality of the retention of associated data by CSIS, delivered on November 3, 2016, what are the changes that CSIS has undertaken in order to ensure that the policies and practices of CSIS comply with the Court's ruling?

CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

INQUIRY OF MINISTRY
DEMANDE DE RENSEIGNEMENT AU GOUVERNEMENT

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

QUESTION NO./Nº DE LA QUESTION	BY / DE	DATE
Q- 942[2]	M. Dubé (Beloeil-Chambly)	22 mars 2017

Reply by the Minister of Public Safety and Emergency Preparedness
Réponse du Ministre de la Sécurité publique et de la Protection civile

L'honorable Ralph Goodale, C.P., député

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

QUESTION

En ce qui concerne l'acquisition et la conservation des données, incluant les données connexes, les métadonnées, les données en vrac ou tout autre type de données, par le Service canadien du renseignement de sécurité (SCRS) : *a*) combien y a-t-il de banques de données internes auxquelles le SCRS a accès; *b*) quels sont les différents types de banques de données internes auxquelles le SCRS a accès; *c*) y a-t-il des banques de données, internes ou externes, que le SCRS a consultées et qui sont hébergées sur des serveurs n'appartenant pas au SCRS; *d*) selon le SCRS, quelle différence y a-t-il entre les expressions « données connexes » et « métadonnées »; *e*) quelle est la liste exhaustive d'organismes avec lesquels le SCRS échange de l'information, y compris des données en vrac, des métadonnées, des données connexes et tout autre type de données auquel il a accès; *f*) quelle est la liste exhaustive d'organismes, incluant les entreprises de télécommunications, les institutions financières, les ministères et autres organismes avec lesquels le SCRS communique autrement que pour échanger de l'information; - **Voir ci-joint pour le texte complet de la question.**

REPLY / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [ ]
TRANSLATION / TRADUCTION [x]

Service canadien du renseignement de sécurité (SCRS)

a)-c) Le SCRS a le mandat de faire enquête sur les menaces envers la sécurité du Canada, dont la définition figure à l'article 2 de la *Loi sur le SCRS*, et d'en informer le gouvernement. Pour remplir son mandat, il est autorisé à l'article12, à recueillir, dans la mesure strictement nécessaire, à analyser et à conserver des informations sur les activités dont il existe des motifs de soupçonner qu'elles constituent des menaces envers la sécurité du Canada. Des politiques et des procédures internes rigoureuses régissent les activités de collecte et de conservation du SCRS.

En raison de la nature classifiée de ses activités, le SCRS ne peut pas divulguer publiquement beaucoup de détails sur les différents types d'informations qu'il recueille, analyse et conserve. Notons que le Comité de surveillance des activités de renseignement de sécurité (CSARS) a le pouvoir d'examiner tout document que le SCRS a en sa possession, exception faite des documents confidentiels du Cabinet. En outre, le Commissariat à la protection de la vie privée du Canada (CPVP) a été informé des activités de collecte, de conservation et d'analyse des données connexes avant que la Cour fédérale ait rendu sa décision et après celle-ci. Le SCRS poursuit sa collaboration avec le CPVP en la matière.

.../2

d) Les expressions « données connexes » et « métadonnées » sont synonymes et renvoient aux informations relatives au contexte de la communication, pas à son contenu. Au SCRS, l'expression « données connexes » désigne les métadonnées liées à une communication interceptée en vertu d'un mandat.

e)f) Précisons que le SCRS utilise le terme « ensembles de données » pour désigner ce que le CSARS appelle « données en vrac ». Soulignons en outre qu'à la suite du rapport du CSARS sur la collecte sans mandat d'ensembles de données par le Centre d'analyse des données opérationnelles (CADO), le SCRS a mis en place un cadre stratégique rigoureux qui lui permet de veiller à ce que le critère de la stricte nécessité et les considérations relatives au respect de la vie privée soient évalués dans chaque cas.

La coopération avec des partenaires gouvernementaux au Canada et à l'étranger est assujettie à la *Loi sur le SCRS*, qui prévoit que le SCRS doit demander l'autorisation du ministre de la Sécurité publique et de la Protection civile et, lorsqu'il s'agit d'une entente avec un organisme étranger, consulter le ministre des Affaires étrangères. Le SCRS peut communiquer des informations aux partenaires avec lesquels il collabore. Toutefois, il est important de noter qu'il ne communique aucune donnée connexe brute à des partenaires canadiens ou étrangers. Seuls les produits d'évaluations qui ont un lien avec une menace peuvent être communiqués.

Les relations que le SCRS entretient avec ses partenaires étrangers sont classifiées et ne sont pas rendues publiques. En effet, cela pourrait nuire à la capacité du SCRS de collaborer avec ces services afin d'obtenir des renseignements utiles ayant trait à la sécurité du Canada et des intérêts canadiens. Cela dit, le SCRS entretient des relations avec plus de 300 organismes étrangers dans quelque 150 pays.

Le SCRS coopère régulièrement avec des partenaires gouvernementaux au Canada. Il a conclu des ententes avec 16 ministères et organismes fédéraux (l'Agence des services frontaliers du Canada, l'Agence du revenu du Canada, les Forces armées canadiennes, l'Agence canadienne d'inspection des aliments, la Commission canadienne de sûreté nucléaire, le Centre de la sécurité des télécommunications, le ministère des Finances, le ministère de la Santé, le ministère de la Défense nationale, le ministère de la Sécurité publique et de la Protection civile, le ministère des Transports, le Centre d'analyse des opérations et déclarations financières du Canada, le ministère des Affaires étrangères, du Commerce et du Développement, le ministère de l'Immigration, Réfugiés et Citoyenneté, l'Agence de la santé publique du Canada et la Gendarmerie royale du Canada), avec toutes les provinces ainsi qu'avec le Yukon et les Territoires du Nord-Ouest.

La coopération avec des organismes non gouvernementaux, dont ceux du secteur privé, est assujettie aux dispositions de la *Loi sur le SCRS*. Le SCRS peut s'assurer, en partie, de la coopération d'un organisme du secteur privé pour effectuer la collecte en vertu d'un mandat que lui a décerné la Cour fédérale. Toutefois, les détails relatifs aux activités opérationnelles menées en collaboration avec le secteur privé demeurent classifiés.

.../3

g)h) Le SCRS a toujours informé le ministre de la Sécurité publique de son programme d'analyse des données depuis sa création, à l'aide notamment des rapports prévus à l'article 33 et au l'article 6(4) de la *Loi sur le SCRS*. Il convient de signaler qu'en 2006, un mémoire portant sur la création du CADO a été envoyé au ministre de la Sécurité publique. Le SCRS a également organisé à son intention une séance d'information interne et de vive voix sur le CADO en 2010.

Le 19 septembre 2016, le SCRS a envoyé au ministre de la Sécurité publique et de la Protection civile un mémoire sur le rapport annuel de 2015-2016 du CSARS et les principaux résultats de l'étude du Comité. Ce mémoire visait à informer le ministre de la question des « données en vrac », comme le CSARS les appelle.

i)-k) Étant donné son mandat et ses besoins opérationnels particuliers, le SCRS ne rend pas publics les détails de ses activités opérationnelles. Il évite ainsi de compromettre l'intégrité de ses enquêtes et sa capacité de remplir le mandat que lui a confié le Parlement.

Toutefois, il faut signaler que pour les aider dans leurs études classifiées respectives, le SCRS a communiqué au CPVP et au CSARS une liste des ensembles de données opérationnelles utilisés par le CADO dans le cadre de l'analytique des données. Par ailleurs, toutes les pratiques de collecte et de conservation des données sont régies par des politiques et des procédures internes rigoureuses qui s'appuient sur les instructions du ministre, les lois canadiennes pertinentes et les décisions des tribunaux.

l) Étant donné son mandat et ses besoins opérationnels particuliers, le SCRS ne rend pas publics les détails de ses activités opérationnelles, notamment la ventilation des informations recueillies en vertu de mandats. Il importe de signaler toutefois que dans l'exécution de son mandat, le SCRS a recours à diverses méthodes de collecte d'informations avec ou sans mandat, toutes conformes à la législation en vigueur.

m)-p) Comme il a déjà été mentionné, une fois en possession d'un mandat décerné par la Cour fédérale, le SCRS peut collaborer avec d'autres organismes des secteurs public et privé pour exercer les pouvoirs prévus dans le mandat. Chaque relation est régie par la *Loi sur le SCRS* et les instructions du ministre connexes et est assujettie à des politiques et à des lignes directrices rigoureuses. Conformément à l'article 21 de la *Loi sur le SCRS*, le SCRS peut demander un mandat lorsque des méthodes intrusives sont nécessaires pour faire enquête sur une menace pour la sécurité du Canada. Il doit obtenir l'approbation du ministre de la Sécurité publique et de la Protection civile avant de présenter une telle demande. Toutefois, étant donné son mandat et ses besoins opérationnels particuliers, le SCRS ne rend pas publics les détails de ses activités opérationnelles.

q) Les détails des enquêtes menées conformément à la *Loi sur le SCRS* demeurent classifiés et ne peuvent être rendus publics. Cela dit, les services de renseignement modernes ont absolument besoin de programmes d'analytique des données pour mener leurs enquêtes. En fait, pratiquement tous les services de renseignement occidentaux ont mis au point de tels programmes de pointe pour repérer des modes de déplacement, de communication ou de comportement habituels, des liens et des tendances importantes qu'il serait impossible de déceler autrement. Le Service utilise ces techniques conformément à la législation et peut faire, à ce sujet, l'objet d'une surveillance et de contrôles par le CSARS et le CPVP.

r)-t) Le SCRS ne peut pas divulguer les détails précis de ses programmes d'analytique des données parce que ces informations sont classifiées. Toutefois, depuis 2015, il fournit au CSARS une liste des ensembles de données dont se sert le CADO dans le cadre de l'analytique des données. Le SCRS s'est engagé à mettre ces informations à jour tous les ans, et le SCRS continuera de le faire avec le plus de transparence possible, mais sans compromettre ses enquêtes sur les menaces pour la sécurité du Canada.

u) La méthode de collecte de données intelligentes est un cadre de gestion de projet utilisé pour repérer les grands enjeux liés à l'acquisition et définir les paramètres d'obtention des ensembles de données. Elle est employée couramment dans le milieu des affaires. Il convient de rappeler que le SCRS mène toutes ses activités, y compris ses activités de collecte de données, conformément à la *Loi sur le SCRS*, aux lois fédérales pertinentes et à ses politiques et procédures internes. Plus particulièrement, cependant, le SCRS a mis en place un cadre stratégique afin de veiller à ce que le critère de la mesure « strictement nécessaire » et les considérations relatives au respect de la vie privée soient évalués dans chaque cas.

v) Au besoin et avec l'approbation du ministre de la Sécurité publique et de la Protection civile, le SCRS peut présenter une demande à la Cour fédérale afin d'obtenir des mandats visant la cible d'une enquête. Ces mandats, qui sont accordés par la Cour fédérale, l'autorisent à employer des techniques d'enquête précises, ce qui peut comprendre l'interception de communications, conformément aux conditions définies par la Cour, s'il y a lieu. Lorsque le SCRS intercepte des communications, il en obtient le contenu ainsi que les données connexes. Par ailleurs, le SCRS peut recueillir des ensembles de données en vertu de la *Loi sur le SCRS*. Le SCRS s'est doté de politiques et procédures internes rigoureuses, conformes à toutes les exigences législatives ainsi qu'aux instructions du ministre.

w)x) Le Service réexamine constamment ses politiques et ses pratiques pour s'assurer de mener ses activités en toute conformité avec la législation, en particulier la *Loi sur le SCRS*. Ainsi, à la suite de la décision de la Cour fédérale du 4 octobre 2016, le SCRS a mis fin à l'analyse et à l'utilisation interne des données connexes obtenues en vertu de mandats d'interception de communications afin d'évaluer les répercussions de la décision et de déterminer les mesures à prendre pour s'y conformer. En mars 2017, le Service a mis en œuvre de nouvelles pratiques de conservation des données connexes collectées aux termes de mandats pour se conformer à la décision de la Cour.

Cela va permettre au CADO de recommencer à analyser les données connexes nouvellement obtenues conformément à la décision de la Cour. Soyons clairs, lorsqu'il est déterminé que des données connexes ne peuvent pas servir dans le cadre d'une enquête, elles sont dorénavant détruites dans les délais fixés par la Cour. Les bases de métadonnées historiques du CADO demeureront toutefois interdites d'accès et ne pourront pas être utilisées jusqu'à ce qu'une décision définitive soit prise concernant leur élimination.

En ce qui a trait à la décision de la Cour fédérale, il est important de rappeler que toutes les données connexes avaient été recueillies légalement en vertu de mandats. La Cour fédérale était surtout préoccupée par la conservation de données connexes qui sont liées aux communications de tiers, mais qui n'ont pas trait à la menace. Elle a déterminé que le SCRS contrevenait à la *Loi sur le SCRS* en conservant des données connexes liées aux communications de tiers qui ne sont pas liées à des menaces et qui ne servent pas dans le cadre d'une enquête ou de poursuites ou qui ne concernent pas la conduite des affaires internationales ou la défense du Canada.

De plus, à la suite du rapport du CSARS sur la collecte sans mandat d'ensembles de données par le CADO, le SCRS a mis en place un solide cadre stratégique, afin de veiller à ce que le critère de la mesure « strictement nécessaire » et les considérations relatives au respect de la vie privée soient évalués.

y) Les politiques, les procédures et les pratiques du SCRS sont classifiées. Cela dit, le SCRS peut confirmer qu'il a entrepris un examen des systèmes administratifs et techniques qui servent à la collecte de données aux termes de mandats, à leur conservation et à leur destruction et qu'il corrigera toute lacune à cet égard. Ainsi, les systèmes de gouvernances nécessaires pour assurer la conformité des activités sont mis en place.

Q-942[2] — 22 mars 2017 — M. Dubé (Beloeil—Chambly) — En ce qui concerne l'acquisition et la conservation des données, incluant les données connexes, les métadonnées, les données en vrac ou tout autre type de données, par le Service canadien du renseignement de sécurité (SCRS) : *a*) combien y a-t-il de banques de données internes auxquelles le SCRS a accès; *b*) quels sont les différents types de banques de données internes auxquelles le SCRS a accès; *c*) y a-t-il des banques de données, internes ou externes, que le SCRS a consultées et qui sont hébergées sur des serveurs n'appartenant pas au SCRS; *d*) selon le SCRS, quelle différence y a-t-il entre les expressions « données connexes » et « métadonnées »; *e*) quelle est la liste exhaustive d'organismes avec lesquels le SCRS échange de l'information, y compris des données en vrac, des métadonnées, des données connexes et tout autre type de données auquel il a accès; *f*) quelle est la liste exhaustive d'organismes, incluant les entreprises de télécommunications, les institutions financières, les ministères et autres organismes avec lesquels le SCRS communique autrement que pour échanger de l'information; *g*) quand les ministres du Cabinet ont-ils été informés de la collecte de données en vrac par le SCRS, et liée à leur notification, (i) qui étaient ces ministres, (ii) par quels moyens de communication ont-ils été informés, (iii) quelles sont les dates auxquelles chacun des ministres a été informé, entre le 1er janvier 2006 et le 31 décembre 2016 inclusivement; *h*) quand les ministres du Cabinet ont-ils été informés des méthodes utilisées par le SCRS pour recueillir des données en vrac, (i) qui étaient ces ministres, (ii) par quels moyens de communication ont-ils été informés, (iii) quelles sont les dates auxquelles chacun des ministres a été informé, entre le 4 novembre 2015 et maintenant; *i*) en ce qui concerne les données en vrac que le SCRS a recueillies ou consultées, comprennent-elles (i) des métadonnées liées aux communications, (ii) de l'information sur les déplacements, (iii) des renseignements contenus dans des passeports, (iv) des bandes d'écoute enregistrées pour l'application de la loi, (v) des dossiers d'arrestation, (vi) des transactions financières, (vii) de l'information recueillie dans les médias sociaux, (viii) des renseignements médicaux, (ix) d'autres types de données en vrac auxquels le SCRS a accès; *j*) quelles sont les descriptions des différentes méthodes utilisées pour la collecte de ces données en vrac; *k*) quelle est la liste exhaustive des sources de données en vrac que peut consulter le SCRS et combien de fois a-t-on recueilli des données entre le 1er janvier 2006 et le 31 décembre 2016 inclusivement; *l*) combien de mandats judiciaires ont été donnés au SCRS pour qu'il puisse obtenir des données en vrac entre le 1er janvier 2006 et le 31 décembre 2016 inclusivement, et quand le SCRS a-t-il obtenu ces mandats; *m*) combien (i) d'entreprises de télécommunications, (ii) d'institutions financières, (iii) d'établissements médicaux, (iv) d'aéroports, (v) d'autres entreprises, ont été obligés ou priés de fournir au SCRS des données en vrac, des données connexes, des métadonnées ou d'autres types de données; *n*) quels sont les moyens qu'emploie le SCRS pour demander ou exiger des données auprès des fournisseurs externes, (i) combien de mandats judiciaires le SCRS a-t-il obtenus pour recueillir des données auprès d'entités privées, (ii) le SCRS a-t-il déjà recueilli ou consulté de telles données sans avoir obtenu au préalable un mandat judiciaire; *o*) combien de ministères ou organismes gouvernementaux ont été obligés ou priés (i) de transférer des données en vrac, des données connexes, des métadonnées ou tout autre type de données au SCRS, (ii) d'accorder au SCRS l'accès à ces données, entre le 1er janvier 2006 et le 31 décembre 2016 inclusivement; *p*) combien de mandats judiciaires le SCRS a-t-il obtenus pour recueillir de telles données auprès des ministères ou organismes gouvernementaux, et le SCRS a-t-il déjà recueilli ou consulté de telles données sans avoir obtenu au préalable un mandat judiciaire; *q*) combien d'enquêtes ont été facilitées par l'utilisation de données en vrac entre le 1er janvier 2006 et le 31 décembre 2016 inclusivement, et combien de personnes ont fait l'objet de ces enquêtes; *r*) combien d'ensembles de données ou de banques de données le Centre d'analyse de données opérationnelles héberge-t-il et parmi eux, combien comprennent des données en vrac; *s*) combien d'ensembles de données ou de banques de données les serveurs internes du SCRS hébergent-ils; *t*) quel sont les pourcentages approximatifs de (i) données en vrac, (ii) données connexes, (iii) métadonnées, (iv) tout autre type de données qui sont hébergées sur les serveurs mentionnés en *s*); *u*) quelle est la description de la méthode de collecte de données intelligentes employée par le SCRS et quels sont les types de données recueillies à l'aide de cette méthode; *v*) quelles sont les étapes en place pour obtenir la validation de l'autorité nécessaire à la collecte de ce type de données; *w*) est-ce que toutes les informations recueillies par le SCRS depuis le 3 novembre 2016 l'ont été dans la « mesure strictement nécessaire » que prévoit le paragraphe 12(1) de la Loi sur le SCRS; *x*) est-ce que toutes les informations conservées par le SCRS depuis le 3 novembre 2016 le sont dans la « mesure strictement nécessaire » que prévoit le paragraphe 12(1) de la Loi sur le SCRS; *y*) compte tenu de la décision rendue le 3 novembre dernier par la Cour fédérale du Canada au sujet de la conservation illégale de données connexes par le SCRS, quels sont les changements apportés par le SCRS pour s'assurer que ses politiques et ses pratiques respectent la décision de la Cour?