CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

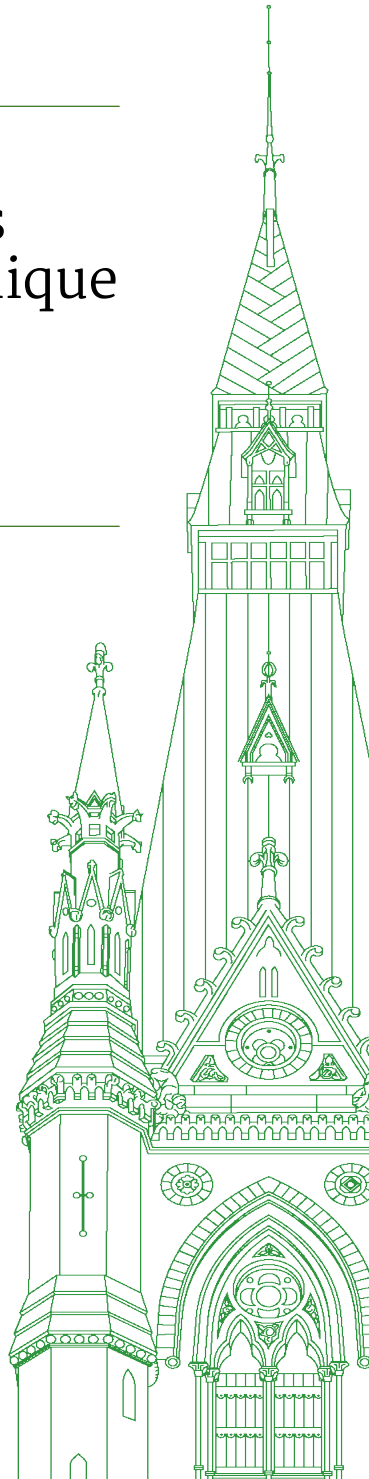
44e LÉGISLATURE, 1re SESSION

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

TÉMOIGNAGES

NUMÉRO 103

Le mardi 13 février 2024



Président : M. John Brassard

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le mardi 13 février 2024

● (1130)

[*Traduction*]

Le président (M. John Brassard (Barrie—Innisfil, PCC)): Je déclare la séance ouverte

Je suis désolé pour le retard. Il y avait des votes.

[*Français*]

Bienvenue à la 103e réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes.

Conformément à l'article 108(3)h) du Règlement et à la motion adoptée par le Comité le mercredi 6 décembre 2023, le Comité reprend aujourd'hui son étude sur l'utilisation par le gouvernement fédéral d'outils technologiques permettant d'extraire des données d'appareils mobiles et d'ordinateurs.

La réunion d'aujourd'hui se déroule sous forme hybride, conformément au Règlement de la Chambre. Les députés peuvent y participer en personne ou par l'entremise de l'application Zoom.

[*Traduction*]

J'aimerais rappeler à tous, en particulier à nos invités, qu'il ne faut pas approcher leur oreillette du microphone parce que cela provoque des réactions acoustiques et pourrait causer des blessures à nos interprètes. Je vous demanderais de faire attention.

J'aimerais maintenant souhaiter la bienvenue à nos témoins.

Nous accueillons aujourd'hui M. Pierre-Yves Guay, sous-commissaire de la Direction des cartels du Bureau de la concurrence du Canada, ainsi que M. Mario Mainville, dirigeant principal de l'application numérique. Nous avons aussi deux représentants de Services partagés Canada, soit M. Daniel Mills, sous-ministre adjoint, Direction générale de l'approvisionnement en TI pour l'entreprise et des services ministériels, et M. Scott Jones, président. Enfin, nous recevons M. Luc Casault, directeur général des services intégrés au Bureau de la sécurité des transports du Canada, ainsi que Mme Kathy Fox, présidente.

Bienvenue à tous.

Nous allons d'abord entendre les représentants du Bureau de la concurrence du Canada.

Vous disposez de cinq minutes pour nous présenter vos observations préliminaires. À vous la parole.

[*Français*]

M. Mario Mainville (dirigeant principal de l'application numérique, Bureau de la concurrence Canada): Merci, monsieur le président.

Bonjour, mesdames et messieurs les membres du Comité. Je vous remercie de nous avoir invités à comparaître devant vous aujourd'hui.

Je m'appelle Mario Mainville et je suis le dirigeant principal de l'application numérique au Bureau de la concurrence. Je suis accompagné aujourd'hui de mon collègue Pierre-Yves Guay, qui est sous-commissaire de la Direction des cartels.

Le Bureau de la concurrence est un organisme d'application de la loi qui protège la concurrence et en fait la promotion au bénéfice des consommateurs et des entreprises du Canada. Nous assurons le contrôle de l'application de la Loi sur la concurrence en menant des enquêtes et en prenant des mesures pour lutter contre les pratiques commerciales anticoncurrentielles qui nuisent aux consommateurs, à la concurrence et à notre économie.

Nous enquêtons sur les infractions criminelles comme la fixation des prix, le truquage des offres et la fraude par marketing de masse, ainsi que sur les affaires de nature civile comme les pratiques commerciales trompeuses et l'abus de position dominante par le biais de pratiques restrictives du commerce.

Nous examinons également les fusions pour nous assurer qu'elles ne nuisent pas sensiblement à la concurrence.

Enfin, nous faisons la promotion de politiques et de règlements gouvernementaux favorables à la concurrence.

C'est uniquement dans le cadre d'enquêtes que le Bureau de la concurrence utilise les outils technologiques dont il est question dans l'étude du Comité.

Les cibles de ces enquêtes peuvent être des entreprises dotées de moyens sophistiqués ou des individus menant leurs activités de manière délibérément secrète ou frauduleuse. La technologie, compte tenu de ses progrès rapides, peut permettre à des utilisateurs de communiquer entre eux pour mettre en œuvre un éventuel comportement anticoncurrentiel et peut contribuer à la perpétration d'un comportement anticoncurrentiel, tout en servant de dispositif pour héberger des renseignements liés à l'activité anticoncurrentielle. Dans de tels cas, le commissaire peut s'adresser aux cours pour obtenir un mandat de perquisition afin de recueillir tous les renseignements nécessaires.

● (1135)

[*Traduction*]

Il est important de comprendre que le Bureau ne peut pas décider de son propre chef de recueillir les données électroniques d'une partie sans son consentement. Le Bureau doit soumettre à la cour un document exposant les motifs qui justifient la délivrance d'un mandat de perquisition et la nécessité de fouiller des systèmes informatiques. La cour pourrait alors décider d'autoriser le commissaire à effectuer une perquisition dans les locaux identifiés, et à copier ou saisir certains documents ou autres choses aux fins d'examen. Notre utilisation de ces outils est donc limitée par les conditions énoncées dans le mandat de perquisition.

Le Bureau reconnaît l'importance de respecter le droit à la vie privée des personnes lors de l'exécution des mandats de perquisition. La délivrance d'un mandat de perquisition par une autorité judiciaire est une garantie qui permet de veiller à ce que les perquisitions soient menées avec l'autorisation légale appropriée. Les organismes d'application de la loi sont tenus de traiter et de gérer les renseignements personnels obtenus au cours des enquêtes de manière responsable et conformément à la loi et aux principes constitutionnels. Les considérations relatives à la protection de la vie privée sont pertinentes, et le Bureau a mis en place des politiques et des procédures pour garantir le respect des principes de protection de la vie privée et des exigences de la loi. Le Bureau travaille en étroite collaboration avec les services juridiques du ministère de la Justice pour s'assurer que ses pratiques sont conformes aux procédures du droit pénal et aux obligations en matière de protection de la vie privée. En outre, l'utilisation, la conservation et la divulgation ultérieures des renseignements recueillis dans le cadre de l'exécution d'un mandat de perquisition sont régies par les politiques du gouvernement du Canada en matière de conservation et d'élimination des données.

Sur ce, nous serons ravis de discuter avec vous aujourd'hui de l'utilisation de ces outils. Nous vous remercions et nous répondrons volontiers à vos questions.

Le président: Merci, monsieur Mainville.

Je cède maintenant la parole aux représentants de Services partagés Canada. Vous avez cinq minutes pour présenter vos observations préliminaires au Comité. Allez-y, je vous prie.

M. Scott Jones (président, Services partagés Canada): Monsieur le président, mesdames et messieurs les membres du Comité, je suis très heureux d'être ici pour faire une mise au point sur l'utilisation que fait Services partagés Canada des outils technologiques permettant d'extraire des renseignements à partir des appareils fournis par le gouvernement.

[*Français*]

Avant de commencer, je tiens à reconnaître que nous sommes réunis sur le territoire traditionnel non cédé du peuple anishinabe algonquin.

J'ai à mes côtés M. Daniel Mills, qui est sous-ministre adjoint principal responsable de l'approvisionnement en technologies de l'information pour l'entreprise et des services ministériels.

Comme vous le savez, Services partagés Canada, ou SPC, est responsable de fournir l'infrastructure de TI de base du gouvernement du Canada. SPC s'est engagé à améliorer son offre de services numériques. Le ministère joue également un rôle important en assurant la sécurité des renseignements du gouvernement du Canada, tout en respectant les exigences de la Loi sur la protection des renseignements personnels.

[*Traduction*]

Monsieur le président, bien qu'il ait été question de logiciels espions dans les médias, je tiens à vous assurer que les outils utilisés par SPC ne correspondent aucunement à cette description. Les ministères du gouvernement du Canada, y compris SPC, utilisent des outils d'investigation informatique dans le cadre d'enquêtes administratives. Ces outils sont essentiels pour nous permettre d'effectuer et de conclure des enquêtes que je suis autorisé à mener, en ma qualité d'administrateur général de SPC, en vertu de la Loi sur la gestion des finances publiques.

Ces enquêtes ont lieu uniquement lorsqu'il y a une allégation crédible d'acte répréhensible commis par un employé et pour assurer la sécurité des réseaux gouvernementaux dont dépendent les Canadiens. Les employés concernés sont toujours informés du déroulement de ces enquêtes et l'équité procédurale est respectée. Les enquêtes administratives peuvent porter, par exemple, sur des cas où l'on soupçonne la navigation sur des sites Web inappropriés à partir d'un appareil fourni par le gouvernement, sur l'installation d'un logiciel malveillant sur un appareil fourni par le gouvernement ou un réseau du gouvernement, ou sur l'utilisation inacceptable des réseaux et des dispositifs électroniques ministériels.

● (1140)

[*Français*]

Dans ces circonstances, j'ai le pouvoir de mener une enquête. De plus, nos experts techniques ont besoin de ces outils pour faire leur travail de manière efficace et équitable, tout en protégeant la vie privée des employés.

Nous prenons très au sérieux la protection de la vie privée des employés et nous utilisons très judicieusement les outils d'investigation informatique.

[*Traduction*]

Les enquêtes administratives relatives à la sécurité suivent des procédures opérationnelles normalisées très strictes et sont menées sous la direction du dirigeant principal de la sécurité de SPC. Le mandat et la portée des enquêtes sont clairement établis, tout comme les garanties d'indépendance et d'impartialité dans la collecte des données.

Nous utilisons les outils d'investigation informatique pour mener des enquêtes administratives dans des environnements étroitement contrôlés. Nous apportons d'abord les appareils fournis par le gouvernement — et seulement les appareils fournis par le gouvernement — dans un laboratoire isolé de niveau « secret », puis nous nous servons des outils d'investigation informatique pour effectuer des analyses. Seule l'information nécessaire à l'enquête est incluse. Nous utilisons également ces outils à des fins opérationnelles légitimes, par exemple pour accélérer l'extraction de renseignements afin de répondre plus rapidement aux demandes présentées conformément à la Loi sur l'accès à l'information et à la Loi sur la protection des renseignements personnels.

Je prends très au sérieux la responsabilité qu'a le ministère de protéger les renseignements personnels qui sont en sa possession. Nous avons des procédures opérationnelles normalisées bien définies afin de protéger la vie privée et d'insuffler la confiance à l'égard des opérations de SPC. C'est d'une importance primordiale.

Ces outils d'investigation informatique servent à analyser de grandes quantités de données et d'information en format numérique. J'aimerais ajouter que le gouvernement du Canada achète ces outils d'investigation informatique depuis de nombreuses années. Lors de la création de SPC, l'achat de ces outils a été centralisé au ministère pour tirer parti du pouvoir d'achat du gouvernement du Canada et pour regrouper les nombreux petits contrats qui étaient courants dans l'ensemble du gouvernement. En tant que fournisseur des services de TI du gouvernement du Canada, SPC a mis en place des contrats pour acquérir ces capacités, et les autres ministères et organismes fédéraux peuvent utiliser ces contrats aux fins d'approvisionnement pour appuyer leurs opérations.

[*Français*]

Nous sommes conscients que l'utilisation des outils d'investigation informatique peut soulever des questions du point de vue de l'éthique et de la vie privée. SPC prend donc très au sérieux la protection des renseignements, la vie privée des employés et la sécurité des Canadiens.

C'est avec grand plaisir que je répondrai à vos questions.

Merci beaucoup.

Le président: Merci, monsieur Jones.

Pour la prochaine déclaration, la parole est au Bureau de la sécurité des transports.

Vous avez cinq minutes pour vous adresser au Comité.

[*Traduction*]

Mme Kathy Fox: Monsieur le président, mesdames et messieurs les membres du Comité, bonjour.

J'aimerais remercier le Comité d'avoir invité le Bureau de la sécurité des transports du Canada, le BST, à témoigner aujourd'hui.

Tout d'abord, permettez-moi d'expliquer brièvement qui nous sommes et ce que nous faisons.

Le BST a été créé en 1990 en vertu de la Loi sur le Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports. Le BST est un organisme fédéral indépendant ayant pour mandat de promouvoir la sécurité des transports en menant des enquêtes sur des « événements de transport » survenus dans les modes de transport aérien, maritime, pipelinier et ferroviaire qui sont sous réglementation fédérale. Les « événements de transport » incluent tant les accidents que les situations qui, à défaut de mesure corrective, pourraient mener à des accidents.

[*Français*]

La mission du BST est énoncée à l'article 7 de la Loi sur le Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports. La principale mission du BST est de promouvoir la sécurité des transports canadiens en procédant à des enquêtes sur les causes des événements de transport et sur les facteurs contributifs et en constatant les manquements à la sécurité; en faisant des recommandations pour réduire ou éliminer ces manquements; ainsi qu'en publiant des rapports qui rendent compte de ses enquêtes et en présentant les conclusions qu'il en tire.

[*Traduction*]

Le BST a le pouvoir discrétionnaire d'enquêter sur tout événement de transport dans le but de s'acquitter de son mandat. La politique du BST est d'enquêter sur les événements qui pourraient nous permettre de tirer des leçons et ainsi de prendre des mesures de sécurité, ou qui sont une source importante de préoccupation publique en matière de sécurité des transports. Les enquêtes du BST, et les rapports qui en découlent, soulignent des enjeux que les organismes de réglementation fédéraux et l'industrie du transport doivent aborder afin de réduire les risques et les manquements à la sécurité dans le système de transport du Canada. Le BST est indépendant et dépose ses rapports au Parlement par l'entremise du président du Conseil privé du Roi pour le Canada.

[*Français*]

Conformément à son mandat à titre d'organisme d'enquête en matière de sécurité, le Bureau n'est pas habilité à attribuer ni à déterminer les responsabilités civiles ou pénales, et le paragraphe 7(4) de la Loi sur le Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports prévoit qu'aucune de ses conclusions ne lie les parties à une procédure judiciaire, disciplinaire ou autre. Le BST n'est pas un organisme réglementaire et il ne prend aucune décision administrative.

● (1145)

[*Traduction*]

Puisque nous sommes ici aujourd'hui pour discuter de l'utilisation de données, j'aimerais aborder brièvement notre processus de collecte et d'utilisation de données. La Loi sur le Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports prévoit un certain nombre de privilèges et de règles de preuve qui ont pour but de veiller à ce que le BST ait accès à l'information dont il a besoin pour mener ses enquêtes. Conformément à l'article 19 de la Loi, dans le contexte d'une enquête, les épaves et autres éléments pertinents à l'événement sont recueillis pour des motifs raisonnables. Ces éléments sont examinés et testés dans le cadre de l'enquête. Des outils spéciaux sont souvent nécessaires pour récupérer des données pertinentes, en particulier des informations techniques comme les données enregistrées et affichées dans le tableau de bord et les ordinateurs de bord; les positions des interrupteurs, des jauges et des vérins; les données GPS indiquant la longitude, la latitude et l'altitude; et les données d'accéléromètre qui fournissent la position ou l'orientation exacte ainsi que des informations portant sur la vitesse, l'accélération et la vibration.

Les données pertinentes peuvent englober les moments avant et pendant l'événement.

[*Français*]

Cette information est nécessaire pour déterminer la chronologie d'un événement de transport et permet au BST de remplir pleinement son mandat. À l'exception des enregistrements audio, par exemple les conversations du poste de pilotage, d'une locomotive ou du pont d'un navire, conformément à l'article 20 de la Loi sur le Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports, tous les éléments recueillis dans le cadre d'une enquête sont restitués à leur propriétaire.

[*Traduction*]

À titre d'organisme d'enquête, le BST traite une variété de renseignements sensibles. Le BST a pour priorité absolue et pour obligation légale de protéger les renseignements personnels recueillis dans le cadre de ses enquêtes. Par exemple, le BST doit toujours intervenir dans des procédures judiciaires pour protéger ses privilèges, comme les déclarations des témoins. Nous sommes résolus à mettre à jour notre évaluation des facteurs relatifs à la vie privée pour notre programme d'enquête afin de nous assurer qu'il englobe toutes les technologies actuelles utilisées pour remplir notre mandat.

Le BST est heureux d'avoir l'occasion de discuter avec le Comité des façons dont il a toujours protégé les renseignements conformément à la Loi sur le Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports et à la Loi sur la protection des renseignements personnels.

Merci.

Le président: Merci, madame Fox.

Comme vous le savez, nous avons commencé la séance en retard, mais nous tâcherons de ne pas dépasser l'heure prévue. Nous aurons le temps de faire deux séries de questions, et nous terminerons probablement avec une série de questions de deux minutes et demie. Certains d'entre vous ont mentionné avoir d'autres réunions après celle-ci; c'est pourquoi il est important de respecter le temps alloué.

Nous devrons discuter des travaux du comité. Comme je l'ai dit, je crois comprendre que certains députés souhaiteraient faire un voyage. Nous avons toutefois une date limite à respecter. Nous devons présenter une demande de déplacement au Comité de liaison avant le 16 février. Je dois donc laisser du temps à la fin de la séance pour que nous en discutions.

Nous allons entamer une série de questions de six minutes. Pour la gouverne de nos témoins, je suis de la vieille école. Vous n'avez pas besoin de vous adresser à la présidence. Vous pouvez répondre directement aux députés qui vous posent les questions. Je cède maintenant la parole au premier intervenant, M. Kurek, pour six minutes.

Allez-y, je vous prie.

M. Damien Kurek (Battle River—Crowfoot, PCC): Merci beaucoup, monsieur le président, et merci à nos témoins d'être ici aujourd'hui.

J'ai donné des conseils aux autres témoins qui ont comparu devant le Comité plus tôt en ce qui concerne la nécessité d'être proactifs relativement aux évaluations des facteurs relatifs à la vie privée et tout le reste. Je vous encourage tous, vos supérieurs et vos subordonnés, à prendre le téléphone. Le commissaire à la protection de la vie privée a dit très clairement qu'il serait heureux de collaborer avec vous de toutes les façons possibles.

Monsieur Jones, comme Services partagés Canada est un élément unique du fonctionnement de l'information et de la technologie dans l'ensemble du gouvernement, je suis curieux. Nous avons beaucoup parlé de l'utilisation de ces outils, mais je suis un peu curieux au sujet des outils eux-mêmes. Prenons l'exemple des courriels. Si un courriel est envoyé à partir d'un appareil gouvernemental et que ce courriel est supprimé, en reste-t-il toujours une trace quelque part?

M. Scott Jones: Oui. Lorsqu'un courriel est envoyé d'un appareil gouvernemental et d'un compte gouvernemental, ce courriel est enregistré sur le serveur.

M. Damien Kurek: Donc, si je comprends bien, même si l'utilisateur d'un appareil supprime ce courriel de son téléphone ou de son ordinateur, l'envoie dans la corbeille et vide même la corbeille, il reste toujours une trace de ce courriel quelque part?

M. Scott Jones: Oui. On pourrait voir sur le serveur qu'un courriel a été envoyé tel jour à telle heure, et on pourrait voir les métadonnées associées à ce courriel.

● (1150)

M. Damien Kurek: Je crois que c'est assez simple en ce qui concerne les courriels, mais y a-t-il des registres d'autres types de communications, comme des appels téléphoniques, des textos, l'accès à Internet et ce genre de choses? Est-ce que Services partagés conserve des métadonnées ou d'autres types de données?

M. Scott Jones: En ce qui concerne les téléphones mobiles, cela va directement sur le routeur de télécommunications. Les dossiers seraient donc directement conservés par le fournisseur de télécommunications. Il faudrait que je vérifie si nous avons accès aux appels qui ont été passés. En ce qui concerne les métadonnées associées à un appel, nous n'avons définitivement pas accès aux appels effectués. Ma réponse serait donc non, mais je devrai confirmer auprès de notre équipe si des arrangements ont été pris. Nous n'aurions pas accès aux textos ni aux appels. Ils ne seraient que sur les téléphones.

M. Damien Kurek: En ce qui concerne les données — nous reviendrons aux courriels comme exemple —, elles existent quelque part. Pour ce qui est de l'accès à cette information pour les demandes d'accès à l'information, les enquêtes administratives, dont vous avez parlé, cette information ne serait pas cachée, même si elle n'est plus accessible par un employé du gouvernement, par exemple? Ai-je bien compris?

M. Scott Jones: Si le courriel a été supprimé parce qu'il n'avait aucune valeur de dossier et qu'il n'a pas été versé dans le système officiel des dossiers — il a été supprimé du dossier « envoyé », etc. —, il y aurait toujours le dossier, et quiconque l'a reçu en aurait toujours une copie, mais la trace selon laquelle le courriel a été envoyé serait toujours dans les registres du système.

M. Damien Kurek: Monsieur Jones, dans une enquête qui a eu l'effet d'une bombe récemment, la vérificatrice générale a parlé de documents manquants pour des contrats non concurrentiels. Je paraphrase ici, mais on dit que la documentation manquait dans les discussions initiales, de sorte que la vérificatrice générale n'a pas eu accès à cette information, mais si des courriels étaient envoyés, ils existeraient toujours quelque part dans les serveurs du gouvernement. Cette hypothèse est-elle juste?

M. Scott Jones: Il devrait y avoir une trace du « courriel envoyé », du fait qu'un courriel a été envoyé. Il faudrait que nous vérifiions ce qui se trouve exactement dans ces métadonnées et dans ce dossier. Cela fait environ 20 ans que je ne me suis pas penché sur cette question.

M. Damien Kurek: D'accord, mais si nous devions creuser la question, simplement parce que la vérificatrice générale n'a pas eu accès à ces renseignements, si des renseignements ont été envoyés à partir d'un serveur du gouvernement, d'un courriel du gouvernement, ils existeraient quelque part. Vous en êtes certain. Est-ce que je...?

M. Scott Jones: Il faudrait que je vérifie exactement...

Si vous demandez si le courriel lui-même existe, une fois qu'il aura été envoyé, quiconque l'a reçu en aura une copie. Maintenant, qu'ils le suppriment ou non, la trace de l'événement, qu'un courriel a été envoyé, serait dans les dossiers.

Il faudrait que je confirme exactement ce qui est stocké dans ces métadonnées. Je ne le sais pas d'emblée.

M. Damien Kurek: Bien sûr. Je vous remercie, monsieur Jones, parce que c'est intéressant dans le contexte du fait que la vérificatrice générale n'a pas pu accéder à cette information. Elle a dit qu'il manquait de la documentation et ainsi de suite.

Cela nous mènerait inévitablement à la conclusion que des outils comme ceux dont nous discutons aujourd'hui sont peut-être nécessaires pour obtenir des réponses. Une opération de camouflage semble être la conclusion évidente à laquelle de nombreux Canadiens — moi y compris — sauteraient pour dire que les pratiques n'ont pas été suivies. Il me semble que les preuves devraient certainement se trouver quelque part.

En ce qui concerne l'utilisation de ces outils, vous a-t-on déjà demandé d'utiliser ces outils d'analyse judiciaire pour trouver des renseignements qui ont été perdus auprès d'organismes gouvernementaux, de ministères ou de mandataires indépendants du Parlement?

Le président: Veuillez répondre très brièvement.

M. Scott Jones: Il faudrait que je vérifie. Je ne peux penser à aucun exemple où nous les avons utilisées de cette façon.

M. Damien Kurek: Puis-je vous demander de revenir au Comité à ce sujet?

M. Scott Jones: Nous pouvons certainement le faire.

M. Damien Kurek: Merci beaucoup.

Le président: Merci, monsieur Kurek.

Monsieur Housefather, vous avez six minutes.

M. Anthony Housefather (Mont-Royal, Lib.): Merci beaucoup, monsieur le président.

Je vais revenir au sujet pour lequel je pense que nous devions nous réunir ici aujourd'hui, à savoir si ces outils prennent l'information et l'utilisent d'une manière que personne n'avait prévue.

Je vais commencer par Services partagés Canada.

Monsieur Jones et monsieur Mills, je suis heureux de vous revoir.

Si je me souviens bien, Services partagés Canada a été créé en 2011 à partir de différents ministères. Est-ce que Services partagés Canada possédait la technologie en question en 2011?

● (1155)

M. Scott Jones: La technologie dont nous parlons aurait été transférée dans le cadre de la fusion des 43 ministères, en même temps que le pouvoir d'amalgamer. Nous avons hérité des outils dont nous parlons.

M. Anthony Housefather: Ces outils existent depuis longtemps. Ils ne sont pas nouveaux. Vous ne les avez pas achetés depuis 2015. Ils étaient là avant 2015.

M. Scott Jones: Nous avons continuellement renouvelé les contrats, mais ces outils étaient en place lors de la création de SPC.

M. Anthony Housefather: Parfait.

Utilisez-vous ces outils pour espionner les Canadiens?

M. Scott Jones: Absolument pas.

M. Anthony Housefather: Pouvez-vous nous dire s'il existe un mécanisme par lequel vous utilisez ces outils lorsque l'appareil même dont vous extrayez les renseignements n'est pas en votre possession?

M. Scott Jones: Nous n'utilisons ces outils que dans un laboratoire physiquement distinct, où l'appareil est en notre possession. C'est aussi un appareil fourni par le gouvernement.

M. Anthony Housefather: D'accord. Ensuite, lorsque vous prenez l'appareil, y installez-vous des logiciels espions et malveillants afin de pouvoir l'espionner par la suite?

M. Scott Jones: Absolument pas. Jamais.

M. Anthony Housefather: Assurez-vous la sécurité de l'appareil seulement si vous avez un mandat ou si vous avez le consentement de la personne concernée?

M. Scott Jones: Lorsque nous menons une enquête administrative, nous le faisons en toute connaissance de cause... la personne sait qu'il y a une enquête administrative, mais il s'agit d'un appareil gouvernemental, alors nous le faisons en vertu de la Loi sur la gestion des finances publiques.

Ce ne sont toutefois pas les premiers outils que nous utilisons. Nous n'utilisons ces outils que lorsqu'ils sont nécessaires pour confirmer ou réfuter les allégations qui ont été faites.

M. Anthony Housefather: Le Canadien moyen à Winnipeg, à Montréal ou à Vancouver peut savoir avec certitude que Services partagés Canada n'espionne pas son téléphone en ce moment.

M. Scott Jones: Absolument. Ce serait tout à fait contraire à notre mandat et à notre code.

M. Anthony Housefather: Parfait.

Permettez-moi de poser la même question au Bureau de la sécurité des transports. Pouvez-vous m'assurer que vous n'espionnez pas les Canadiens avec les outils d'extraction dont nous parlons?

Mme Kathy Fox: Nous ne faisons certainement pas une telle chose. Nous utilisons cet outil dans le cadre de notre mandat pour mener nos enquêtes, et principalement avec le consentement du propriétaire.

M. Anthony Housefather: Ce serait avec le consentement ou sans doute avec un mandat quelconque.

Mme Kathy Fox: Nous pouvons émettre un mandat à la suite d'une demande faite à un juge de paix. Nous n'avons jamais eu à utiliser un mandat pour cela, parce que la plupart du temps, nous l'obtenons par consentement, sur place ou par l'intermédiaire des premiers intervenants.

M. Anthony Housefather: Ce serait la même chose dans votre cas, c'est-à-dire que le processus d'extraction vous obligerait à avoir l'appareil en votre possession. Est-ce exact?

Mme Kathy Fox: C'est exact. Nous avons l'appareil en notre possession. Il est téléchargé sur un ordinateur autonome. Ce n'est pas sur un réseau. Il se trouve dans notre laboratoire. Il est également protégé par un mot de passe, car l'accès est très limité.

M. Anthony Housefather: Vous ne téléchargez pas de logiciel dans l'appareil. Vous n'y installez pas de maliciels. Vous n'y installez pas de logiciels espions. Vous n'y installez rien qui vous permettra, une fois que la personne aura repris le contrôle de l'appareil, de savoir ce qu'elle fait ou de l'espionner de quelque façon que ce soit.

Mme Kathy Fox: Absolument pas. Nous ne gardons pas l'information que nous téléchargeons, sauf pour ce qui est absolument nécessaire à l'enquête, et nous retournons l'appareil intact à son propriétaire ou à son représentant.

M. Anthony Housefather: J'imagine que dans les deux cas, parce que je sais qu'il s'agit de Services partagés Canada, mais dans votre cas également, ceux qui ont accès à l'information sont un petit groupe restreint de personnes qui ont reçu une formation appropriée sur ce qu'elles sont censées faire en matière de protection des renseignements personnels.

Mme Kathy Fox: C'est exact.

M. Anthony Housefather: Merci.

Puis-je poser la même question au Bureau de la concurrence? Pouvez-vous répondre aux mêmes questions?

M. Mario Mainville: Nous n'utilisons les outils en question qu'avec un mandat de perquisition qui a été autorisé par un juge, à l'exception d'un cas où il y a eu consentement et où une entente de consentement a été rédigée. Cela ne s'est produit qu'une fois.

Nous n'espionnons pas les Canadiens. Nous n'installons pas...

[*Français*]

M. Anthony Housefather: Je veux m'assurer de bien comprendre.

Donc, que je sois à Québec, à Trois-Rivières, à Montréal ou à Baie-Comeau, vous ne pourriez pas voir ce qui est sur mon téléphone. Le Bureau de la concurrence ne va pas m'espionner, n'est-ce pas?

M. Mario Mainville: Non. Nous n'installons aucun logiciel sur les appareils que nous saisissons. C'est même le contraire: quand nous saisissons l'appareil, nous coupons les connexions et nous ne pouvons même pas avoir accès au nuage, parce qu'il faut protéger l'information. Ça fait partie de la procédure. Il n'y a donc aucune activité de surveillance des Canadiens et des Canadiennes.

M. Anthony Housefather: Je vais vous poser la même question qu'aux représentants de Services partagés Canada.

Si vous preniez mon téléphone parce que la cour vous en avait donné le mandat, vous n'y mettriez donc pas de logiciel espion, de logiciel malveillant ou tout autre programme pour voir ce que je fais après m'avoir remis le téléphone.

M. Mario Mainville: Non, pas du tout.

M. Anthony Housefather: La seule manière qui vous permettrait de regarder ce qui est dans mon téléphone serait d'avoir l'équipement en votre possession, dans un laboratoire assez privé. Est-ce exact?

M. Mario Mainville: En effet, ce serait dans un laboratoire complètement détaché du reste du réseau du Bureau de la concurrence ou du gouvernement du Canada.

● (1200)

M. Anthony Housefather: C'est parfait.

[*Traduction*]

Je vais céder mon temps de parole, monsieur le président.

[*Français*]

Le président: Merci, monsieur Housefather.

Nous parlions de Trois-Rivières; justement, je cède maintenant la parole à M. Villemure pour six minutes.

M. René Villemure (Trois-Rivières, BQ): Merci beaucoup, monsieur le président.

Bonjour et bienvenue à tous.

Je suis heureux que nous ayons l'occasion d'éclaircir cette situation. Comme vous le savez, nous sommes ici aujourd'hui à la suite de la parution d'un article de CBC/Radio-Canada mentionnant que 13 organismes et ministères, dont les vôtres, n'avaient pas fait d'évaluation des facteurs relatifs à la vie privée.

Je poserai donc la question à chacun d'entre vous: avez-vous, oui ou non, fait une évaluation des facteurs relatifs à la vie privée?

Commençons par M. Mainville.

M. Mario Mainville: Non.

M. René Villemure: Qu'en est-il de vous, monsieur Jones?

M. Scott Jones: Non, mais nous avons créé un programme d'enquêtes administratives en gardant en tête les concepts relatifs à la vie privée.

M. René Villemure: D'accord. Vous n'avez cependant pas fait d'évaluation des facteurs relatifs à la vie privée.

M. Scott Jones: Non, nous n'en avons pas fait dans le cadre du programme élaboré lors de la création de Services partagés Canada. À l'heure actuelle, cependant, nous avons commencé une évaluation.

M. René Villemure: D'accord.

Qu'en est-il du BST, madame Fox ou monsieur Casault?

M. Luc Casault (directeur général, Services intégrés, Bureau de la sécurité des transports du Canada): Nous avons une évaluation pour notre programme depuis sa mise en place, mais nous n'avons pas fait une évaluation pour l'outil lui-même. À la suite d'une conversation avec le Commissariat à la protection de la vie privée du Canada, nous avons décidé de mettre à jour l'évaluation pour notre programme.

Ça fait longtemps que nous faisons ce genre d'extraction de données. Étant donné qu'une évaluation pour notre programme était déjà en place depuis un bout de temps, nous n'avons pas senti le besoin de faire une évaluation pour l'outil lui-même.

M. René Villemure: Est-ce que le commissaire vous a recommandé de faire l'évaluation pour l'outil ou est-ce que celle pour le programme suffisait?

M. Luc Casault: Le commissaire a recommandé à coup sûr de mettre à jour l'évaluation pour notre programme.

M. René Villemure: Est-ce que ça a débuté?

M. Luc Casault: Oui.

M. René Villemure: D'accord.

Monsieur Mainville, je reviens à vous.

Pourquoi n'avez-vous pas fait d'évaluation des facteurs relatifs à la vie privée?

M. Mario Mainville: Notre programme a été mis en place avant la directive sur l'évaluation des facteurs relatifs à la vie privée. Ça ne veut pas dire pour autant que la vie privée n'est pas importante. Quand la directive a été donnée, en 2010, nous estimions que notre programme n'avait pas subi de changements majeurs depuis sa création en 1996. En 2010, nous utilisions déjà des téléphones pliables et des appareils comme ceux de la marque Nokia ou BlackBerry. Il y a ensuite eu des téléphones intelligents, mais nous ne considérions pas que l'ajout de ces nouveaux appareils plus évolués constituait un changement radical à notre programme.

Cela dit, à la suite du témoignage du commissaire à la protection de la vie privée et des nouvelles sorties en décembre, nous avons contacté le Commissariat à la protection de la vie privée du Canada et entrepris des démarches.

M. René Villemure: Vous avez donc entrepris des démarches au sujet d'une évaluation...

M. Mario Mainville: Oui. En fait, c'était pour le programme d'informatique judiciaire au complet.

M. René Villemure: Est-ce qu'il y aura une évaluation pour l'outil ou est-ce que ce sera seulement une évaluation pour le programme?

M. Mario Mainville: D'après ce que je comprends, l'évaluation concerne le programme et la façon dont les données personnelles sont manipulées. L'outil qui servira à faire le même travail peut changer, alors ce n'est pas nécessairement l'outil qui doit être soumis à une évaluation. La recommandation est de procéder à l'évaluation pour une activité ou un programme. Dans notre cas, nous avons choisi de faire l'évaluation à plus haut niveau, soit pour le programme d'informatique judiciaire.

M. René Villemure: Entre 1996 et 2010 ainsi qu'entre 2010 et 2024, le monde a changé. Il y a eu l'arrivée d'Internet et des médias sociaux, et nous avons maintenant de nouvelles capacités.

Vous nous avez tous mentionné que vous n'utilisiez pas de tels outils sans avoir obtenu une autorisation judiciaire. J'ai bien compris ça. Cependant, l'autorisation judiciaire ne remplace pas l'évaluation des facteurs relatifs à la vie privée et les conseils du commissaire à la vie privée.

Dans ce cas, pourquoi avoir tardé à agir?

M. Mario Mainville: C'est une très bonne question.

J'ai suivi toutes les réunions du Comité, et j'ai remarqué qu'une chose n'avait pas encore été mentionnée: la question de la jurisprudence. Pendant les périodes que vous avez mentionnées, plusieurs cas ont fait jurisprudence, et nous devons nous y adapter. Par exemple, nous devons aller voir un juge pour qu'il signe un mandat de perquisition. Si nous utilisions les mêmes dénonciations qu'en 2000, il ne signerait assurément pas le mandat de perquisition. La jurisprudence nous oblige donc à ajuster notre façon de travailler, au point où il faut expliquer au juge comment nous allons travailler avec les données, afin de le mettre en confiance et qu'il signe le mandat de perquisition.

Alors, au fur et à mesure que la jurisprudence évolue, nous nous adaptons. De plus, nous participons à plusieurs symposiums annuels auxquels participent aussi des gens des secteurs privé et public...

● (1205)

M. René Villemure: Je m'excuse de vous interrompre, mais mon temps de parole est limité.

Êtes-vous d'accord pour dire que la jurisprudence et le mandat obtenu ne remplacent pas l'évaluation des facteurs relatifs à la vie privée?

M. Mario Mainville: Je suis tout à fait d'accord sur cela.

M. René Villemure: D'accord.

Monsieur Jones, lorsqu'on vous a demandé ces outils, vous avez décidé de les acheter. C'est donc vous qui avez été l'intermédiaire.

En tant que fournisseur d'outils, vous êtes-vous préoccupé de la nécessité de faire une évaluation des facteurs relatifs à la vie privée?

M. Scott Jones: Merci de la question.

L'achat d'un outil, c'est une chose; ce qui est le plus important, c'est la manière dont on utilise l'outil. L'outil peut être utilisé à plusieurs fins. Dans notre cas, par exemple, nous l'utilisons pour récupérer l'information nécessaire pour répondre aux demandes.

M. René Villemure: Si le Bureau de la concurrence vous demande l'outil, Services partagés Canada va l'acheter, puisque c'est ce que fait le ministère. Or, Services partagés Canada ne se soucie pas de ce que le Bureau de la concurrence fait de cet outil.

M. Scott Jones: Non, nous n'avons pas...

M. René Villemure: Ça ne relève pas de votre responsabilité.

M. Scott Jones: Non.

M. René Villemure: Donc, quand vous n'avez pas de relations relatives à la vie privée, c'est pour vos opérations à vous.

M. Scott Jones: Exactement.

M. René Villemure: C'est parfait.

Merci beaucoup, monsieur le président.

Le président: Merci, messieurs Villemure et Jones.

[*Traduction*]

Monsieur Green, vous avez six minutes.

M. Matthew Green (Hamilton-Centre, NPD): Merci.

Je veux poursuivre dans la même veine et m'assurer de bien comprendre.

Monsieur Jones, vous avez dit tout à l'heure que votre ministère regroupait les contrats par l'entremise de n'importe quel autre ministère qui utiliserait la technologie.

Est-ce exact?

M. Scott Jones: C'est exact.

M. Matthew Green: À cet égard, vous seriez responsable de l'approvisionnement, mais pas de la mise en œuvre de la technologie.

Est-ce exact?

M. Scott Jones: C'est exact.

M. Matthew Green: Quel serait le poste de la commande pour ce type de technologie?

Peut-être que M. Mills...

M. Scott Jones: Il faudrait que nous vous revenions là-dessus.

Habituellement, selon ce que j'ai vu dans le passé, c'est qu'il y aurait une offre à commandes pour quelque chose de ce genre. Nous dirions: « ils sont disponibles; nous avons lancé un appel d'offres », puis il y aurait une demande...

M. Matthew Green: Nous en connaissons 13.

Monsieur Mills, je vais vous poser directement cette question.

Combien de fois cette technologie a-t-elle été fournie par l'entremise de Services partagés?

[*Français*]

M. Daniel Mills (sous-ministre adjoint, Direction générale de l'approvisionnement en TI pour l'entreprise et des services ministériels, Services partagés Canada): Ces outils ont été achetés par l'entremise de la chaîne d'approvisionnement de Services partagés Canada depuis que le ministère existe. Sur une base annuelle, nous renouvelons les contrats avec les différentes institutions.

[*Traduction*]

M. Matthew Green: Ce n'est pas la question que j'ai posée. La question que j'ai posée était la suivante: combien de fois Services partagés a-t-il sous-traité cette technologie à différents ministères?

[*Français*]

M. Daniel Mills: Nous n'avons pas de contrats de sous-traitance avec les autres organisations. Nous achetons les services, donc la technologie. Cette dernière est accessible à tous les ministères du gouvernement fédéral. Les ministères peuvent utiliser ces outils et...

[*Traduction*]

M. Matthew Green: Je vais poser la question plus directement, monsieur, et j'espère obtenir une réponse directe.

Vous faites ce que vous venez de décrire. Combien de fois ce produit a-t-il été utilisé et par combien de ministères?

[*Français*]

M. Daniel Mills: Je vais devoir vérifier cette information et vous la transmettre plus tard.

Pour notre part, nous achetons des licences pour des outils qui peuvent être utilisés par tous les ministères. Je ne dispose pas d'un rapport qui me dit quel ministère a utilisé quel outil et à quelle fréquence il l'a utilisé. Je n'ai pas cette information, mais je peux vérifier si elle existe.

[*Traduction*]

M. Matthew Green: D'accord.

Pour en revenir au contraste entre cet outil judiciaire particulier et les outils d'enquête sur appareil, que nous avons étudiés ici par l'entremise de la GRC, est-ce que la GRC devrait passer par Services partagés dans le cadre du processus d'approvisionnement, ou se limiterait-elle également au fournisseur?

M. Scott Jones: Cela dépend. Nous fournissons des services de TI à la GRC, mais en général, tout ce qui concerne les mesures de maintien de l'ordre relèverait directement de la GRC dans le cadre de ses processus contractuels normaux ou peut-être de Services publics et Approvisionnement Canada. Il faudrait que je vérifie.

M. Matthew Green: Avez-vous une idée ou un droit de regard concernant les pratiques d'approvisionnement des autres ministères?

M. Scott Jones: Non. C'est seulement lorsque nous offrons un service partagé et que nous offrons une licence partagée que nous pouvons obtenir un avantage sur le plan des coûts.

M. Matthew Green: D'accord, cela suffit.

Permettez-moi de vous poser la question suivante: dans le cadre de votre travail, avez-vous déjà acheté des outils d'enquête sur appareil?

M. Scott Jones: À Services partagés Canada, non, je ne me souviens pas d'avoir déjà fait cela.

M. Matthew Green: D'accord. C'est important.

Monsieur, lorsque vous parliez des évaluations des facteurs relatifs à la vie privée, vous avez mentionné que votre travail datait d'avant... Cela remontait à 1996. Je crois que vous avez même parlé de BlackBerry.

Est-il juste de dire, cependant, que vous n'utilisez pas la même technologie que celle utilisée en 1996?

● (1210)

M. Mario Mainville: Oui.

M. Matthew Green: Vous utilisez une nouvelle technologie.

M. Mario Mainville: Nous utilisons une évolution de ce que nous utilisions à l'époque, oui.

M. Matthew Green: Je pense qu'on peut raisonnablement supposer, compte tenu de la loi de Moore, que cela dépasserait largement la technologie d'il y a 20 ans.

Est-ce exact?

M. Mario Mainville: Oui, en ce qui concerne les façons dont nous pouvons accéder aux données. Auparavant, c'était tout ou rien, et maintenant, nous pouvons faire des choix et choisir ce que nous voyons. Oui, c'est...

M. Matthew Green: S'agit-il d'une technologie beaucoup plus puissante?

M. Mario Mainville: Oui.

M. Matthew Green: Y aurait-il une différence importante par rapport à la technologie que vous utilisiez en 1996?

M. Mario Mainville: Nous n'avions pas de téléphones. Cela correspond vraiment aux téléphones, donc...

M. Matthew Green: Si c'est le cas, c'est complètement différent.

M. Mario Mainville: Oui, il y aurait eu des ordinateurs...

M. Matthew Green: C'est une nouvelle technologie.

M. Mario Mainville: En ce qui concerne la technologie proprement dite, je la fonderais davantage sur l'arrivée des BlackBerry et des téléphones à clapet. Nous les avons traités en 2009 et en 2010.

M. Matthew Green: Pour revenir à ce que je disais, maintenant, en 2024, nous parlons d'une technologie qui dépasse de loin votre mise en œuvre initiale.

Si je soulève cette question, c'est parce que cela me préoccupe lorsque vous dites que votre programme est antérieur à la directive, parce que j'interprète une directive du Conseil du Trésor comme étant une directive — pour tous les ministères. Lorsque des ministères choisissent à quel moment ils sont soumis à une évaluation des facteurs relatifs à la vie privée...

Je vais simplement aller de l'avant et dire que tout cela aurait pu être évité, à mon avis, si ces ministères avaient simplement suivi les directives et effectué les EFVP. En tant que comité, il nous reste à déterminer quels sont les recours, soit en faire une obligation juridique de la part des ministères.

Comment répondriez-vous à une question qui vous demande si le fait d'en faire une exigence juridique vous donnerait des lignes directrices plus claires quant à l'applicabilité de l'EFVP et à l'utilisation de votre technologie?

M. Mario Mainville: Je pense que la réponse est oui, parce que nous avons travaillé avec des produits nouveaux, considérablement modifiés... Nous ne travaillons pas en vase clos. Nous avons consulté le ministère de la Justice pour savoir si notre programme avait été modifié au point où nous avions besoin d'une EFVP, et ce n'est pas le cas.

Nous prenons la décision en fonction des renseignements dont nous disposons, alors plus de clarté...

M. Matthew Green: Si vous me le permettez, je pense que le défi, c'est qu'en permettant à chaque ministère de se soumettre ou non à l'EFVP, nous créons un point de vue inutilement conspirationniste sur la façon dont on utilise ce processus.

Lorsque j'entends l'explication selon laquelle il y a eu une panne et qu'il faut procéder à une vérification judiciaire des données, c'est tout à fait logique. Il y a beaucoup de raisons pour lesquelles vous utiliseriez cette information. Je ne suis pas ici aujourd'hui pour croire que vous espionnez tous les Canadiens ou que cette technologie a quelque chose de répréhensible.

Je crois que c'est le cas pour l'appareil lui-même, soit dit en passant, mais c'est une tout autre histoire.

En ce qui concerne cette étude...

Le président: Monsieur Green, votre temps est écoulé.

M. Matthew Green: Ça va. J'aurai un autre tour.

Le président: Cela met fin à notre première série de questions. Nous allons maintenant passer à notre deuxième série de questions, en commençant par M. Brock, pour cinq minutes.

Vous aurez deux minutes et demie, monsieur Green.

Monsieur Brock, vous avez cinq minutes. Allez-y.

M. Larry Brock (Brantford—Brant, PCC): Merci, monsieur le président.

Je souhaite un bon après-midi aux témoins. Merci d'être avec nous. Je m'excuse, je n'ai pas pu écouter les déclarations liminaires que certains d'entre vous ont probablement faites.

Je voudrais parler du scandale de l'application ArriveCAN qui semble être le sujet qui occupe la Chambre des communes et les conversations des Canadiens d'un bout à l'autre du pays. À l'instar de mon collègue M. Kurek, c'est vers vous que je vais me tourner, monsieur Jones. Il semble que vous possédiez une certaine expertise dans le domaine en ce qui concerne la technologie, les données et ce genre de choses.

Au cœur du scandale — peut-être n'êtes-vous pas au courant —, il y a la question de l'information. Une des questions restées en suspens qui a causé des maux de tête à la vérificatrice générale est que, malgré la documentation qu'elle a reçue de l'Agence des services frontaliers du Canada, l'ASFC, documentation qui n'était pas très étoffée, en raison des problèmes d'administration et de conservation des documents, la vérificatrice générale n'est pas arrivée à déterminer qui avait choisi cette entreprise de deux personnes, qui a reçu 20 millions de dollars du Trésor public pour, essentiellement, ne rien faire de plus que diriger l'ASFC vers des professionnels des TI.

Des indications laissent penser que des renseignements ont été cachés à la vérificatrice générale et ces indications pointent vers une personne appelée Minh Doan, qui est le dirigeant principal de la technologie du gouvernement du Canada. On pourrait penser qu'une personne dont le titre est « dirigeant principal de la technologie » possède les compétences requises en matière de conservation des documents, mais au cœur du scandale, il y a la disparition mystérieuse de près de 1 700 courriels pertinents datant d'une période de quatre années incluant la pandémie, lorsque le coût de la scandaleuse application « ArnaqueCAN » a explosé et dépassé les 60 millions de dollars.

Comment une telle chose a-t-elle pu arriver?

● (1215)

M. Scott Jones: Sans avoir tous les détails, je peux présenter un grand nombre d'hypothèses concernant différentes situations qui peuvent survenir dans l'univers des TI. L'explication peut être aussi simple qu'une défaillance du disque dur d'un ordinateur portable, ce qui m'est déjà arrivé et j'avais perdu tous mes courriels. Sans avoir de détails sur la situation, je ne peux pas répondre à votre question.

M. Larry Brock: C'est une question à laquelle nous n'avons toujours pas de réponse. L'homme en question n'a pas expliqué pourquoi il lui était impossible de retrouver les courriels datant de cette période de quatre ans. Malgré le poste qu'il occupait — il était vice-président de l'ASFC et dirigeant principal de l'information de l'Agence à l'époque —, il n'a pas pu expliquer ce qui s'était passé, alors la présidente de l'ASFC n'a pas pu donner de précisions quant au contenu...

Mme Iqra Khalid (Mississauga—Erin Mills, Lib.): J'invoque le Règlement, monsieur le président.

Le président: Monsieur Brock, Mme Khalid invoque le Règlement. J'ai arrêté le chronomètre. Il vous restera deux minutes.

Allez-y, madame Khalid.

Mme Iqra Khalid: Merci, monsieur le président.

Nous nous interrogeons sur la pertinence des questions. Je sais que le sujet qu'a abordé M. Brock est présentement étudié par un certain nombre de comités. Nous étudions une question bien précise, soit l'utilisation par le gouvernement d'outils technologiques pour la surveillance des fonctionnaires dans les ministères. Je préférerais que M. Brock s'en tienne à cette question et je pense que ce serait également préférable pour le Comité.

Le président: Comme je l'ai déjà dit dans le passé, madame Khalid, je laisse beaucoup de latitude aux députés pendant les tours de questions, parce que je m'attends à ce qu'ils finissent par aborder le sujet de l'étude. Je suis certain que c'est ce que fera M. Brock. C'est ce qu'il fait d'habitude.

Monsieur Brock, vous avez la parole. Il vous reste deux minutes. Allez-y.

M. Larry Brock: Merci, monsieur le président, parce que je ne prépare certainement pas mes questions en fonction des préférences du Parti libéral du Canada. Je sais qu'ils veulent étouffer ce débat. Je sais que c'est important pour eux de nous empêcher de parler...

Mme Iqra Khalid: Monsieur le président, j'invoque le Règlement, c'est tout à fait inacceptable — voyons donc.

Le président: Merci de ce rappel au Règlement.

Monsieur Brock, vous pouvez continuer. J'avais arrêté le chronomètre. Je le relance; il vous reste 1 minute et 50 secondes.

M. Larry Brock: Merci.

Monsieur Jones, je voudrais savoir quels sont les outils que pourrait possiblement employer la GRC, qui pourrait être appelée à faire enquête sur des éléments criminels entourant ArnaqueCAN... Comme on disait à l'époque où j'étais procureur de la Couronne, ce qui saute aux yeux, ce sont les allégations de fraude et d'abus de confiance par un fonctionnaire.

Selon vous, en tant que professionnel, quels sont les outils d'investigation informatique dont la GRC dispose pour récupérer les quatre années de courriels pertinents du vice-président de l'ASFC?

M. Scott Jones: En toute honnêteté, les techniques d'enquête de la GRC ne me sont pas familières. En tant que fournisseurs de services de TI, nous nous assurons de demeurer indépendants des activités de la Gendarmerie.

Nous fournissons effectivement des services de TI de base...

M. Larry Brock: Quels types d'outils utiliseriez-vous?

Par exemple, si Erin O'Gorman, la présidente de l'ASFC, prenait son travail au sérieux et cherchait à retrouver ces courriels, quels sont les outils qu'elle pourrait utiliser à votre avis?

M. Scott Jones: Si un collègue me demandait conseil, c'est certainement l'une des raisons pour lesquelles ces ententes ont été établies concernant les outils nécessaires pour récupérer de l'information sur des appareils du gouvernement. Il existe différents outils, selon le type d'appareil utilisé.

Je n'ai pas de liste de produits sous la main. Je n'ai jamais utilisé ce genre d'outils dans ma carrière.

M. Larry Brock: Est-il possible de récupérer quatre années de courriels?

M. Scott Jones: La façon de récupérer des courriels dépend de ce qui s'est produit et de l'endroit où ils se trouvent. Tout dépend toujours de la situation.

M. Larry Brock: Chaque situation est différente.

M. Scott Jones: Oui, c'est bien cela.

Le président: Merci, monsieur Brock.

Madame Khalid, vous avez cinq minutes. Allez-y.

Mme Iqra Khalid: Merci beaucoup, monsieur le président.

Je remercie les témoins d'être avec nous aujourd'hui.

Pendant que les conservateurs essaient de décider, en fonction des manchettes qu'ils pourraient générer, si c'est une bonne chose ou non de mener une surveillance des téléphones du gouvernement, je vais me tourner vers vous.

Je voudrais une réponse de chacun des témoins, en commençant par M. Jones.

D'après vous, quel est l'objectif d'une évaluation des facteurs relatifs à la vie privée et quel est l'impact d'une telle évaluation sur le travail que vous menez au sein de votre ministère?

● (1220)

M. Scott Jones: Selon moi, l'évaluation des facteurs relatifs à la vie privée répond à de nombreux enjeux.

Elle vise principalement à arriver à un équilibre entre nos objectifs, dans le cadre d'une enquête administrative, par exemple, en matière de protection des renseignements et d'exercice des responsabilités que nous a attribuées le gouvernement en ce qui concerne le droit à la vie privée des employés. De plus, l'évaluation sert à nous assurer que nous avons bien examiné la situation afin de bien comprendre les répercussions et de mettre en place des mesures de contrôle ou de trouver des façons d'arriver à l'équilibre dont je parlais.

S'il faut utiliser un outil qui est plus invasif que ce que nous voudrions, il faut s'assurer de trouver une façon d'arriver à cet équilibre. C'est l'une des raisons pour lesquelles, par exemple, nous utilisons un laboratoire dans un lieu gardé secret à accès très restreint où les employés ont une cote de fiabilité. Je n'ai pas accès aux laboratoires d'investigation informatique. Je ne peux pas y entrer.

Mme Iqra Khalid: Merci.

Le commissaire à la protection de la vie privée a affirmé qu'obtenir une autorisation judiciaire ne pouvait remplacer l'évaluation des facteurs relatifs à la vie privée. Dans votre déclaration préliminaire, vous avez parlé du fait que vous devez obtenir un mandat avant d'employer des mesures invasives.

Que pensez-vous de cette obligation?

M. Scott Jones: Nous ne sommes pas un service de police, alors nous ne pouvons pas obtenir de mandat judiciaire. C'est la Loi sur la gestion des finances publiques qui me donne, ainsi qu'au vice-président, le pouvoir de mener des enquêtes administratives. Comme je l'ai dit, ces enquêtes sont très circonscrites et ces outils ne sont utilisés qu'en cas de nécessité.

Je vais donner un exemple. Les employés de Services partagés ne peuvent pas apporter un téléphone du gouvernement à l'étranger. Si des téléphones, des ordinateurs portables, etc., doivent être apportés à l'étranger, nous nous servons de ces outils pour vérifier qu'aucun document n'a été pris sur l'appareil ou qu'aucun logiciel malveillant n'a été installé, par exemple. Ces outils sont utilisés pour vérifier la sécurité et les paramètres de sécurité. C'est un exemple de situation où on emploierait ces outils.

Mme Iqra Khalid: Merci.

Monsieur Mainville, je vous poserais les deux mêmes questions, si vous n'y voyez pas d'inconvénient.

M. Mario Mainville: En tant qu'organisme gouvernemental, l'évaluation nous aide à trouver un équilibre entre notre programme, nos responsabilités relatives à l'application de la Loi sur la concurrence, et les exigences relatives à la protection des renseignements personnels des Canadiens. C'est à cela que sert l'évaluation. L'objectif principal est de mener une évaluation systématique et de répondre en amont aux risques potentiels liés aux nouveaux programmes ou aux programmes modifiés.

Mme Iqra Khalid: Merci.

M. Luc Casault: Nous sommes d'accord avec le commissaire. Cela ne remplace pas l'évaluation. Obtenir le consentement ne nous dégage pas de nos obligations concernant la tenue d'une évaluation.

Nous utilisons l'évaluation depuis que notre programme a été créé. Nous l'avons mise à jour au fil des années. L'évaluation concerne les données que nous recueillons. Nous nous assurons que toutes les données collectées soient visées par une évaluation et que les enjeux relatifs à la protection des renseignements personnels aient été évalués.

Après avoir discuté avec le Commissariat à la protection de la vie privée, comme le commissaire, nous sommes arrivés à la conclusion que, en fonction de la situation actuelle, il serait bon de faire une mise à jour.

Les outils ne remplacent pas une évaluation. Acheter un nouvel outil ne change pas nécessairement la façon dont on se sert des données. C'est pour cette raison que l'outil ne sert pas d'évaluation. Par contre, nous croyons qu'il serait temps de mettre à jour l'évaluation, notamment en raison des nouvelles orientations qui nous viennent du Conseil du Trésor à ce sujet.

Mme Iqra Khalid: Je vous remercie de votre réponse.

Je reviens à vous, madame Fox.

Que pouvez-vous faire de plus pour collaborer avec le commissaire à la protection de la vie privée afin d'assurer le maintien de la confiance dans les institutions publiques, en particulier lorsque le gouvernement utilise des technologies intrusives pour surveiller les téléphones des gens?

Mme Kathy Fox: Comme je l'ai dit, nous n'utilisons pas du tout l'outil mentionné dans le rapport pour interagir avec les téléphones des employés, qu'ils soient fournis par le gouvernement ou non. Nous n'utilisons cet outil que pour extraire des données dans le cadre de notre mandat afin de mener nos enquêtes, et uniquement les données pertinentes dont nous avons besoin. L'appareil est rendu à son propriétaire sans avoir été altéré. Encore une fois, nous avons pris des mesures de sécurité appropriées en ce qui concerne les ordinateurs autonomes, l'accès limité, la mise en oeuvre appropriée des politiques de conservation et ainsi de suite.

Nous avons pris contact avec le Commissariat à la protection de la vie privée, pas plus tard que la semaine dernière, pour reconfirmer notre position à ce sujet.

● (1225)

Mme Iqra Khalid: Merci.

Monsieur Jones, je vous pose la même question.

Le président: Soyez bref, s'il vous plaît.

M. Scott Jones: J'ai rencontré le commissaire à la protection de la vie privée. C'est l'une des premières choses que j'ai faites lorsque j'ai pris mes fonctions, et c'était pour discuter de la manière dont nous commençons à envisager les technologies émergentes. C'est l'un des domaines où, franchement, il s'agit d'une pratique exemplaire que nous aurions dû mettre en œuvre, et c'est pourquoi nous le faisons maintenant.

Le président: Merci, madame Khalid et monsieur Jones.

[*Français*]

Monsieur Villemure, vous avez la parole pour deux minutes et demie.

M. René Villemure: Merci beaucoup, monsieur le président.

Monsieur Jones, d'après ce que je comprends, vous êtes nouveau à Services partagés Canada.

M. Scott Jones: J'y suis depuis septembre.

M. René Villemure: D'accord. Merci beaucoup.

J'aimerais maintenant revenir à M. Mainville en suivant le même ordre d'idées que mon collègue.

La capacité d'action liée aux outils d'aujourd'hui est extrêmement différente de celle des outils de 1996. Vous avez dit ne pas avoir fait d'évaluation des facteurs relatifs à la vie privée parce qu'il y avait déjà une évaluation pour le programme, notamment.

Une évaluation des facteurs relatifs à la vie privée est-elle considérée comme étant un peu trop compliquée, comme n'étant pas importante, ou encore comme une tâche qu'on peut remettre au lendemain? Qu'est-ce qui est entré en ligne de compte?

M. Mario Mainville: Une évaluation a été faite pour déterminer si nous devions réaliser une EFVP complète. Pendant cette évaluation, nous avons déterminé que les changements apportés quant aux données que nous recueillons et à leur traitement ne nécessitaient pas une EFVP.

Comme je l'ai mentionné tantôt, après le témoignage du commissaire à la protection de la vie privée, nous avons fait des démarches pour demander des conseils à ce sujet.

M. René Villemure: Vous êtes donc demeurés en contact avec le commissaire à la protection de la vie privée à cet égard.

M. Mario Mainville: Oui.

M. René Villemure: Dans le contexte d'une autre étude du Comité, il était question des outils utilisés par la GRC. Je comprends qu'on ne parlait pas des mêmes outils que ceux dont nous discutons aujourd'hui, mais on nous avait dit que c'était comme lorsqu'on insérait un microphone dans une lampe, autrefois. Honnêtement, je dois dire que ce n'est pas la même chose. Je pense qu'aujourd'hui les attentes en matière de vie privée sont différentes.

Vous allez de l'avant et je vous en félicite, mais je suis quand même déçu de constater qu'autant de ministères et organismes ne l'ont pas fait.

Monsieur Mills, mon collègue vous a demandé tantôt combien de ministères et organismes avaient utilisé l'outil en question. J'aimerais que vous répondiez par écrit à cette question afin que nous puissions prendre une décision éclairée.

Monsieur le président, combien de temps de parole me reste-t-il?

Le président: Il vous reste 30 secondes.

M. René Villemure: C'est parfait.

Madame Fox, vous dites n'utiliser ce type d'outil que lors d'une enquête. C'est assez précis. Le fait que ce soit une enquête vous dispense-t-il de l'obligation de faire une évaluation des facteurs relatifs à la vie privée?

Mme Kathy Fox: Non. Nous sommes quand même tenus de nous conformer à la Loi sur le Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports ainsi qu'à la loi traitant de la protection de la vie privée. Cela dit, notre loi habilitante nous autorise à recueillir des informations pour les enquêtes dans le cadre de notre mandat, mais nous devons aussi protéger ces renseignements et utiliser uniquement l'information dont nous avons vraiment besoin pour déterminer ce qui s'est passé dans le cadre de l'événement dont il est question.

M. René Villemure: Est-ce que ces deux lois se contredisent?

Mme Kathy Fox: Non. Je pense qu'il devra toujours y avoir des lois donnant accès aux renseignements pour des fins ou des mandats précis, par exemple les enquêtes sur la sécurité des transports. Si nous n'avons pas accès aux renseignements, nous ne pouvons pas déterminer ce qui s'est passé et ce qui doit être fait pour éviter qu'un accident survienne. C'est une situation où l'intérêt public est important. Il faut aussi respecter la loi traitant de la protection de la vie privée, mais c'est une question d'équilibre.

M. René Villemure: Merci beaucoup.

Le président: Merci, monsieur Villemure et madame Fox.

Monsieur Green, je vais vous accorder trois minutes également, étant donné que c'est ce que j'ai alloué à M. Villemure.

[*Traduction*]

M. Matthew Green: Merci.

Je vais vous poser à tous les deux les questions suivantes.

Premièrement, dans le cas où vous utilisez un outil sur un appareil mobile ou un ordinateur auquel vos employés ont accès — je ne vous demande que votre avis —, pensez-vous qu'il serait judicieux que vos institutions consultent le Commissariat à la protection de la vie privée avant de déployer cet outil?

Deuxièmement, l'ajout dans la Loi sur la protection des renseignements personnels d'une obligation légale de réaliser des évaluations des facteurs relatifs à la vie privée et de les soumettre au Commissariat à la protection de la vie privée du Canada rendrait-il le processus plus clair pour votre institution et pour les institutions gouvernementales en général, donc pour votre ministère et pour tous les autres ministères?

Si je pose ces questions, ce n'est pas pour vous prendre en défaut. Il s'agit d'obtenir un rapport qui fournira des recommandations claires au gouvernement pour améliorer les processus, de sorte que vous n'ayez plus à vous présenter ici pour ce genre d'enjeu.

M. Luc Casault: En ce qui concerne l'utilisation de cette technologie pour les employés, oui, bien sûr, nous consulterons le Commissariat à la protection de la vie privée, car il s'agirait d'une utilisation totalement nouvelle. Je n'envisage pas vraiment que nous le fassions un jour.

En ce qui concerne votre deuxième question, je pense que le meilleur mécanisme pour parvenir à nos fins, c'est une plus grande sensibilisation et une meilleure formation des employés, et ce comité fait du bon travail en organisant ces séances et en mettant cette sensibilisation en avant. Je pense que la directive est en cours de révision. Si nous pouvions y ajouter la sensibilisation et la formation, je pense que cela aiderait beaucoup, plus que...

● (1230)

M. Matthew Green: Il faut passer aux autres ministères. Merci.

M. Scott Jones: En ce qui concerne les enquêtes administratives, je pense qu'il est important que nous mettions continuellement à jour nos processus en y ajoutant les pratiques exemplaires et les enseignements tirés des autres ministères et en consultant les experts en relations de travail du Conseil du Trésor. Il est certain que l'avis du commissaire à la protection de la vie privée est important pour la mise en place du programme. Nous n'utilisons ces outils que très rarement dans ce cas.

En ce qui concerne l'accès à l'information et la protection de la vie privée, il est important de souligner qu'une fois que ces dossiers sont sous contrôle, il s'agit pour nous de répondre à l'obligation légale, et nous les utilisons donc de manière très restrictive. Cependant, de temps en temps, nous recevons, par exemple, une demande pour tous les messages textes envoyés depuis mon téléphone. Nous utilisons cet outil pour les obtenir...

M. Matthew Green: Bon nombre de ces demandes émanent de notre comité.

M. Scott Jones: ... afin d'accélérer les choses, parce que c'est très difficile à réaliser. D'ailleurs, je ne peux même pas vous dire comment les extraire de mon téléphone.

M. Matthew Green: Je vous remercie. Nous passons maintenant au dernier ministère.

Monsieur Mainville, allez-y.

M. Mario Mainville: Pour votre première question, nous sommes un organisme chargé de l'application de la loi. L'article 29 de la Loi sur la concurrence nous oblige à mener nos enquêtes en privé. La protection de la vie privée part donc de là. Sur une base transactionnelle, il nous serait très difficile de nous adresser au commissaire à la protection de la vie privée.

Pour ce qui est de la deuxième question, oui, je pense qu'il serait bénéfique que nous soyons tous censés réaliser des évaluations des facteurs relatifs à la vie privée sur nos programmes — pas sur des outils en particulier — puis, si ces outils changent radicalement, de refaire les évaluations des facteurs relatifs à la vie privée.

M. Matthew Green: Nous avons établi que votre outil a changé radicalement par rapport à celui de 1996.

M. Mario Mainville: Nous cherchons d'ailleurs à instaurer une évaluation des facteurs relatifs à la vie privée.

Le président: Merci, monsieur Green.

Il reste deux périodes de questions de cinq minutes, une pour les conservateurs et une autre pour les libéraux.

Monsieur Kurek, vous disposez de cinq minutes. Allez-y. Veuillez commencer maintenant.

M. Damien Kurek: Merci beaucoup, monsieur le président.

Pour les gens de Services partagés Canada, l'une des entreprises dont il est question s'appelle Cellebrite. Je sais que les médias ont rapporté que la technologie peut porter atteinte à la vie privée, mais il y a aussi eu une transgression technologique. Je crois qu'il s'agit de 1,7 téraoctet de données, de renseignements, qui ont été rendus publics. L'un de vos principaux rôles est de fournir un outil très puissant dans ce cas-ci.

Quels processus avez-vous mis en place pour vous assurer que les outils que vous vous procurez respectent bien le droit à la vie privée des Canadiens, à la fois ceux qui pourraient être utilisés ailleurs que pour les fins administratives du gouvernement dans le cadre d'enquêtes, par exemple — qu'il s'agisse des organismes que nous avons ici ou d'autres que ce comité a entendus —, ou à des fins administratives, afin de s'assurer que, pour une entreprise qui fait l'objet d'accusations assez graves, la vie privée et les droits sont protégés dans le cadre de ce processus? Quel est votre processus?

M. Scott Jones: Cette question comporte plusieurs éléments. Tout d'abord, lorsque nous passons des marchés, nous le faisons pour répondre à des besoins. Il nous faut donc certains moyens pour agir. C'est ce que nous recherchons. Dans la foulée, une évaluation de la sécurité est également réalisée. Nous travaillons avec nos partenaires du Centre de la sécurité des télécommunications pour assurer l'intégrité de la chaîne d'approvisionnement et veiller à la propriété...

Enfin, il s'agit de savoir comment ces outils sont utilisés et comment nous les déployons. Par exemple, tous les outils de ce type sont utilisés dans un laboratoire isolé afin que les données restent sous notre contrôle et en notre possession matérielle et qu'elles sont également isolées physiquement.

M. Damien Kurek: Est-ce un protocole que vous avez mis en place?

M. Scott Jones: Cette dernière étape relève de nous au ministère. La façon dont nous évaluons les logiciels fait partie d'un processus établi de collaboration avec le Centre de la sécurité des télécommunications.

M. Damien Kurek: Lorsque l'article a été publié, des révélations ont été faites, des questions très graves ont été posées et beaucoup de questions ont été soulevées. On a pu répondre à quelques-unes d'entre elles. Encore une fois, je recommanderai qu'on procède de manière proactive à des évaluations des facteurs relatifs à la vie privée. Avec tout le respect que je vous dois, vous êtes tous régis par des lois adoptées par le Parlement, et le commissaire à la protection de la vie privée est un fonctionnaire du Parlement. Il faut utiliser le service étant donné que le gouvernement est une fonction du Parlement, et non l'inverse.

Il s'agit de protocoles que vous avez créés pour vous assurer que cette technologie est utilisée dans une salle sécurisée sans être reliée à Internet, ou quelque chose du genre. Est-ce que c'est ce qu'a fait Services partagés Canada?

● (1235)

M. Scott Jones: C'est ce que nous avons fait pour les enquêtes administratives, mais en ce qui concerne les évaluations en matière d'investigation, oui.

M. Damien Kurek: Je suis curieux de savoir quelque chose. On a fait référence à 13 ministères et organismes. Certains n'étaient pas étonnants, comme le BST et la GRC, mais il y en avait d'autres pour lesquels des questions restent en suspens sans que nous sachions si c'était à des fins administratives et ainsi de suite.

Y a-t-il d'autres ministères, hormis les 13 qui ont été mentionnés dans l'article, qui ont utilisé le logiciel dont vous disposez par l'intermédiaire de Services partagés Canada? Y a-t-il d'autres ministères qui auraient utilisé ce logiciel, en plus des 13 qui sont mentionnés dans l'article?

M. Scott Jones: Je n'ai pas de liste.

Monsieur Mills, je ne sais pas si vous en avez vu une, mais je ne pense pas que ce soit le cas.

M. Daniel Mills: Je ne pense pas, mais, comme je l'ai dit plus tôt, nous pouvons fournir au Comité une liste de tous les ministères qui l'ont utilisé, s'il y en a plus que les 13 qui ont été énumérés dans l'article.

M. Damien Kurek: Je pense qu'il y a deux aspects très distincts. Il y a le côté administratif, qui consiste notamment à veiller à ce que les droits des employés soient protégés, et il y a les enquêtes, qui découlent d'un accident d'avion ou d'une affaire de concurrence, comme c'est le cas pour notre autre témoin ici présent.

Je pense qu'il serait très utile que vous fassiez la distinction entre ces deux aspects, à savoir le côté administratif et les enquêtes.

Par ailleurs, il serait intéressant d'en savoir davantage au sujet de l'autorisation judiciaire, bien que je suppose que cela dépasse du mandat de Services partagés. Ai-je raison de supposer que c'est le cas?

M. Scott Jones: Je ne pense pas que nous puissions connaître l'objectif de cet outil sans émettre d'hypothèse concernant le mandat de Services partagés Canada. Nous pouvons certainement vérifier quels ministères ou agences ont fait des achats par notre entremise, mais il nous est impossible de savoir à quelles fins.

Par exemple, la GRC ne divulgue jamais les outils qu'elle utilise dans le cadre de ses enquêtes.

M. Damien Kurek: Puisque vous êtes un fournisseur de services informatiques, vous n'obtiendrez pas de réponses. Si vous pouviez fournir ces renseignements et si vous connaissiez les objectifs administratifs et les objectifs des enquêtes, cela nous serait très utile pour répondre aux sérieuses questions que se posent les Canadiens, et qui demeurent toujours sans réponse.

Le président: Je vous remercie.

Monsieur Bains, vous avez cinq minutes. Allez-y s'il vous plaît.

M. Parm Bains (Steveston—Richmond-Est, Lib.): Merci, Monsieur le président.

Je remercie tous nos témoins de s'être joints à nous aujourd'hui. Ma première question s'adresse au Bureau de la concurrence.

Vous avez mentionné certaines des fonctions que vous exercez. Vous avez parlé notamment de truquage d'offres et de fixation des prix. Vous enquêtez sur ces pratiques.

Ces outils pourraient-ils être utilisés dans le cadre de ce type d'enquête ?

M. Mario Mainville: Oui.

M. Parm Bains: À titre d'organisme d'application de la loi qui tente de lutter contre la fixation des prix, le truquage d'offres et ce genre de pratiques, vous devez cibler une personne d'intérêt et obtenir l'autorisation judiciaire de la poursuivre ou de mener une enquête sur elle, avant de pouvoir utiliser ces outils dans le cadre de votre travail.

M. Mario Mainville: C'est exact.

M. Parm Bains: Au Canada, je pense que nous avons un problème en ce qui concerne les oligopoles. Par exemple, nous nous intéressons aux chaînes de supermarchés et au secteur des télécommunications, des domaines dans lesquels un nombre restreint de grandes sociétés contrôle le marché. Par exemple, en ce qui concerne les supermarchés, nous avons entendu à la Chambre des communes que si quelqu'un était responsable de contrôler les prix, ceux-ci pourraient baisser.

S'agit-il d'un dossier sur lequel vous pourriez vous pencher?

M. Mario Mainville: Je céderai la parole à mon collègue, Pierre-Yves.

M. Pierre-Yves Guay (commissaire délégué, Direction des cartels, Bureau de la concurrence Canada): C'est certainement un dossier sur lequel nous pourrions nous pencher. Cela ne fait aucun doute.

M. Parm Bains: Il faudrait qu'une plainte soit déposée, et ainsi de suite. Quelle serait la procédure à suivre?

M. Pierre-Yves Guay: Dans le cadre d'une enquête, nos procédures sont très similaires à celles de la police. Par exemple, un citoyen peut porter plainte auprès de nous et nous fournir des renseignements. Si nous avons suffisamment de renseignements, et si nous avons de bonnes raisons de le faire, nous utilisons nos outils à des fins d'enquête — en procédant à des perquisitions, par exemple. Supposons que nous saisissions le téléphone cellulaire d'une personne visée. À ce moment-là, nous pouvons utiliser ces outils.

● (1240)

M. Parm Bains: Que pouvez-vous extraire d'un téléphone cellulaire?

Nous avons assisté à certaines démonstrations lors de réunions précédentes du comité. Il faut obtenir le téléphone, s'y brancher et en extraire toutes les données. Est-ce bien le cas? Avez-vous accès à toutes les données et à toutes les applications qui s'y trouvent?

M. Mario Mainville: Nous pouvons avoir accès à toutes les données contenues dans un téléphone. Dans le cas de truquage d'offres, nous chercherions à savoir si le propriétaire du téléphone a communiqué avec quelqu'un d'une autre société à des fins de fixation des prix — ce genre de communications.

Comme d'autres témoins l'ont souvent indiqué, nos procédures font en sorte que seuls les renseignements pertinents sont versés au dossier. Par exemple, à titre d'expert en criminalistique, je ne peux transmettre à mon collègue Pierre-Yves, enquêteur, que les renseignements pertinents pour son dossier. Par exemple, il ne pourrait obtenir l'intégralité du carnet d'adresses contenu dans le téléphone sans motif valable. Les renseignements auxquels il a accès sont strictement limités à ce que prescrit le mandat de perquisition.

M. Parm Bains: Le mandat de perquisition doit donc être très précis, et l'enquêteur est le seul à avoir accès à ces données.

Combien de personnes ont accès à ces renseignements au sein de votre service? Combien y a-t-il d'enquêteurs?

M. Mario Mainville: Initialement, à l'issue d'une fouille, le nombre de personnes qui ont accès au contenu de ces téléphones est de 8 à 10, selon les effectifs du moment. En ce moment, nous avons huit experts en criminalistique.

Seules les données pertinentes sont mises à la disposition exclusive de l'équipe chargée du dossier. Comme dans le cas des autres agences d'application de la loi qui ont témoigné, ces données ne sont pas mises à la disposition de l'ensemble de la Direction des cartels. Elles sont uniquement mises à la disposition de l'équipe chargée de l'enquête sur cette affaire.

M. Parm Bains: Par ailleurs, nous sommes informés de toute tentative de consultation de ces renseignements par un tiers. Des mécanismes sont en place à cette fin.

M. Mario Mainville: Les services de criminalistique informatique sont branchés à un réseau entièrement autonome, qui n'est branché à aucun autre réseau ni à Internet. Ils se trouvent dans un local sécurisé, à l'intérieur d'un autre local sécurisé, et l'accès physique y est strictement restreint.

Le président: Monsieur Bains, vous venez tout juste de dépasser votre temps.

M. Parm Bains: Merci.

Merci beaucoup.

Le président: Merci, monsieur Bains.

Je tiens à remercier les témoins de leur présence aujourd'hui.

Certains ont demandé à ce que des renseignements soient envoyés au Comité. La greffière communiquera avec vous, mais j'aimerais que ces renseignements lui parviennent d'ici mardi prochain à 17 heures, si possible. C'est dans une semaine. Comme je l'ai indiqué, la greffière fera le suivi nécessaire.

Je tiens à tous vous remercier de votre présence aujourd'hui. Je vais devoir vous excuser, car le comité doit discuter de ses travaux.

Merci beaucoup.

En ce qui concerne les travaux du comité, je crois comprendre que les députés sont intéressés à accepter l'offre de la GRC d'organiser une séance d'information technique dans ses locaux.

Monsieur Motz, en tant qu'ancien agent de la GRC, est-ce que c'est quelque chose qui vous intéresse?

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Absolument.

Le président: Deux possibilités s'offrent à nous. Nous pouvons en faire la demande officielle, ce qui signifie que nous avons jusqu'au 16 pour en faire la demande au comité de liaison en vue d'obtenir son approbation.

L'autre possibilité qui s'offre à nous est de faire une visite informelle à la GRC, ce qui, si je comprends bien, est le souhait des députés. Je tiens à m'assurer que les choses soient claires à ce sujet. Ce qui sera abordé au cours d'une visite informelle à la GRC afin de discuter notamment de la collecte de renseignements personnels ne sera pas reflété dans le rapport. Rien de ce qui découlera de cette visite informelle ne sera repris dans le rapport. Cette visite est uniquement destinée à éclairer le comité.

Madame Damoff, je vois que vous avez la main levée, de même que M. Brock.

Y a-t-il quelqu'un d'autre qui souhaite intervenir?

Allez-y, madame Damoff, à ce sujet.

Mme Pam Damoff (Oakville-Nord—Burlington, Lib.): Merci, monsieur le président.

Après la dernière séance, je me suis entretenue avec Bryan Larkin et avec Michael Barrett, qui n'est pas ici en ce moment. Cependant, dans le cadre des travaux du comité de la sécurité publique, nous — et je crois que Glen y est allé également — sommes allés visiter l'armurerie de la GRC à titre non officiel, simplement pour en apprendre davantage à ce sujet. Je pense que Bryan a lancé l'idée de mieux nous informer sur la protection de la vie privée, les téléphones cellulaires et ce qu'il est possible de faire.

Ce qui me préoccupe, monsieur le président, c'est que si nous procédons de manière officielle, cela risque de prendre un certain temps, et nous ne sommes pas certains d'y être autorisés. Il se pourrait que nous devions attendre le mois de juin pour obtenir l'autorisation. D'ici là, nous aurons déjà terminé notre étude et nous serons passés à autre chose. Par conséquent, je serais heureuse de m'organiser avec les quatre autres partis.

Cette visite aurait lieu ici, à Ottawa, et ne nécessiterait donc pas de transport. La GRC est en mesure d'organiser ces visites dans les deux langues officielles, ce qui nous éviterait des problèmes liés à l'interprétation en français.

Voilà ce que nous recommandons, monsieur le président. Je me ferai un plaisir de m'organiser avec Michael et les autres.

● (1245)

Le président: Merci, madame Damoff.

À titre d'information pour le comité, le siège de la GRC se trouve à Orléans, ce qui n'est donc pas très loin.

Monsieur Brock, vous avez levé la main. Nous passerons ensuite à M. Kurek.

M. Larry Brock: Je voulais des précisions sur le site et je les ai obtenues.

Je suis tout à fait d'accord avec Mme Damoff. C'est la bonne approche à adopter.

Le président: Merci.

Monsieur Kurek, la parole est à vous.

M. Damien Kurek: Merci.

J'ai eu une brève conversation avec M. Barrett et je crois comprendre qu'il y a eu des discussions ici. Je pense que la visite informelle est certainement la meilleure option et elle n'a pas besoin de coûter un centime aux contribuables. Nous pouvons le faire.

Je tiens simplement aussi à souligner officiellement que, si des informations s'avéraient pertinentes pour l'étude, je pense qu'il conviendrait tout à fait de demander à la GRC de nous les fournir dans le cadre d'un suivi. Bien que la visite elle-même ne soit pas nécessairement officielle, les informations que nous apprendrons pourront certainement être incluses dans le futur rapport. Je suis reconnaissant à la GRC de nous avoir donné l'occasion de mieux comprendre ces outils.

Le président: Merci, monsieur Kurek.

Il me semble qu'il y a un consensus pour une visite informelle.

[*Français*]

Monsieur Villemure, vous avez la parole.

M. René Villemure: Monsieur le président, je voudrais proposer officiellement la motion suivante, dont j'ai donné avis la semaine dernière:

> Que, conformément à l'article 108(3)h) du Règlement, le Comité entreprenne une étude sur la désinformation et la mésinformation et les impacts de celles-ci sur le travail des parlementaires, que le Comité consacre les trois prochaines séances disponibles à cette étude; que le Comité invite des experts en matière de désinformation et mésinformation; et que le Comité fasse rapport de ses observations et recommandations à la Chambre.

Le président: Votre motion est recevable, puisque vous avez déjà donné avis de cette motion au Comité.

Voulez-vous dire quelque chose au sujet de la motion, monsieur Villemure?

M. René Villemure: Certainement, monsieur le président. Merci beaucoup.

Quand on consulte des études prospectives, on remarque que la désinformation et la mésinformation représentent maintenant un risque presque aussi grand que les changements climatiques, parmi les inquiétudes des dirigeants et des gouvernements actuels.

Au Parlement, nous avons à prendre des décisions éclairées. Or, il est probable que nous soyons nous-mêmes la cible de désinformation et de mésinformation. Alors, afin de permettre au Comité et au Parlement de prendre des décisions plus éclairées, je nous invite à mener cette étude avec des experts, sur la base de l'intérêt public. Cela nous aidera à avancer et permettra à tous les parlementaires concernés de mieux faire leur travail.

Le président: Merci, monsieur Villemure.

Je veux juste clarifier une chose, étant donné que les travaux du Comité ont déjà été établis et que nous commençons une étude que nous avons déjà décidé d'entreprendre.

Si j'ai bien compris, monsieur Villemure, l'étude que vous proposez se ferait lors de futures séances. Est-ce bien le cas?

M. René Villemure: Oui.

Le président: D'accord.

[*Traduction*]

Passons maintenant à Mme Khalid, qui sera suivie par M. Green.

Je vois que vous levez la main, monsieur Barrett.

Madame Khalid, la parole est à vous.

Mme Iqra Khalid: Merci beaucoup, monsieur le président.

Par votre entremise, je remercie M. Villemure d'avoir présenté cette motion. Je siège à l'Association parlementaire du Commonwealth en tant que vice-présidente. Dans le cadre des discussions entre les pays du Commonwealth, il s'agit de la principale préoccupation parmi les parlementaires du monde entier. Comment lutter contre la mésinformation et la désinformation? Quelles en sont les répercussions sur nos institutions démocratiques? Quelles en sont les répercussions sur notre processus décisionnel?

Je suis tout à fait d'accord avec M. Villemure sur l'importance de cette question. J'espère que nous passerons un peu plus de temps que trois réunions sur ce sujet. Je pense que nous devons examiner en profondeur la manière dont nous pouvons veiller à ce que les gouvernements soient préparés à l'évolution des technologies et des médias numériques et à leurs répercussions sur la diffusion de l'information, de la désinformation et de la mésinformation. Je peux citer au moins 10 témoins dans ce domaine qui, à mon avis, contribueraient grandement à la formulation de recommandations sur la manière dont le gouvernement canadien peut traiter cette question en vue d'assurer non seulement la sécurité des Canadiens en ce qui concerne les informations qu'ils absorbent si rapidement de nos jours, mais aussi l'exactitude, la véracité et l'objectivité des informations qu'ils reçoivent et l'absence d'objectifs malveillants.

Je serais vraiment heureuse d'avoir le consensus du Comité pour convenir de tenir « au moins » trois réunions sur ce sujet. Après ces trois réunions, nous pourrions revenir sur le sujet et déterminer le nombre de témoins supplémentaires qui souhaiteraient en parler et le nombre de renseignements ou de domaines supplémentaires dans ce sujet que nous devons examiner un peu plus en profondeur. Nous pourrions réévaluer l'orientation que nous souhaitons donner à cette étude.

Je félicite M. Villemure d'avoir soulevé ce sujet très important. Je pense que nous devons vraiment effectuer une étude approfondie. Je propose un amendement favorable visant à tenir « au moins » trois réunions et à réévaluer la situation à la fin de ces trois réunions.

Merci, monsieur le président.

● (1250)

Le président: Je considère qu'il s'agit d'un amendement officiel. Il est difficile de faire un amendement favorable à une motion.

Je considère qu'il s'agit d'un amendement officiel et je demande l'adoption par consensus de la modification proposée par Mme Khalid, qui tend à remplacer « les trois » réunions par « au moins trois des » réunions.

Nous en sommes toujours à l'amendement, si quelqu'un souhaite en parler.

Monsieur Barrett, vous avez la parole au sujet de l'amendement qui remplacerait « les trois » réunions par « au moins trois des » réunions.

M. Michael Barrett (Leeds—Grenville—Thousand Islands et Rideau Lakes, PCC): Oui. Trois est acceptable. Je voulais simplement obtenir aussi des précisions sur la motion que nous amendons.

Je crois comprendre que le libellé est...

Le président: Le libellé de la motion se lit comme suit: « les trois prochaines séances disponibles ». Nous avons des réunions prévues, dont je parlerai une fois que nous aurons réglé cette question, mais M. Villemure propose l'expression « les trois prochaines séances disponibles ».

S'il n'y a pas d'autres interventions, je demande au Comité s'il y a consensus pour l'adoption de l'amendement.

(L'amendement est adopté.)

Le président: Nous revenons maintenant à la motion principale modifiée.

Monsieur Green, vous avez la parole.

M. Matthew Green: Merci.

Je suis reconnaissant à mon collègue bloquiste René Villemure du bon travail qu'il a fait pour tracer la voie de notre prochaine étude.

Je vais jouer cartes sur table et dire que je suis satisfait des résultats de l'étude en cours. J'ai l'impression que nous pourrions interroger huit autres ministères et obtenir des réponses très similaires. Je suis convaincu qu'il ne s'agit pas d'une technologie de l'information sur appareils, d'un logiciel espion ou d'un logiciel malveillant. Je suis convaincu qu'il est utilisé dans le cadre des mandats respectifs des ministères en tant qu'outils d'enquête et de vérification. Je suis satisfait des paramètres dans lesquels ils l'utilisent. Je ne suis pas satisfait de l'absence d'évaluation des facteurs relatifs à la vie privée, comme je l'ai dit.

Cela dit, monsieur le président, combien de réunions supplémentaires ont été prévues pour cette étude particulière? Serait-il peut-être avantageux pour le Comité de présenter une motion visant à demander à l'analyste de commencer à rédiger un rapport préliminaire sur le travail que nous avons effectué jusqu'à présent?

Le président: J'allais vous informer. Votre question arrive à point nommé.

Nous avons encore une réunion à ce sujet. Vous avez exprimé le souhait d'inviter les syndicats à discuter de cette question dans le contexte de la fonction publique. Nous avons pris des dispositions pour que des représentants de l'Association canadienne des employés professionnels et l'Institut professionnel de la fonction publique du Canada viennent témoigner jeudi. Malheureusement, l'Alliance de la fonction publique du Canada a refusé notre invitation.

Ces témoins comparaîtront. Un témoin que M. Villemure voulait voir est la source de l'article de CBC/Radio-Canada. Il témoignera également jeudi. Merci de me l'avoir rappelé. La présidente du Conseil du Trésor s'est engagée à comparaître le 21 mars. Cela aura pour effet de clore l'étude. Voilà où nous en sommes.

● (1255)

M. Matthew Green: Je suppose que ma prochaine question est la suivante: quelles sont les trois prochaines dates disponibles?

Le président: Si cette motion particulière est adoptée, la seule date que je puisse envisager en ce moment pour le début des séances qui y sont prévues est probablement le 29 février. Le 27 février, le commissaire de la GRC témoignera au sujet de SNC-Lavalin.

Veuillez me donner un instant.

La greffière vient à nouveau de me le rappeler. J'en parlais à Alexandra. Le commissaire de la GRC comparaîtra le 27 février et ensuite le rapport préliminaire sur l'étude des médias sociaux sera publié d'ici le 19 février. Pour le moment, j'estime qu'il y aura probablement jusqu'à trois réunions à ce sujet. Cela pourrait être moins. J'espère que ce sera moins. Il y a quelques recommandations à cet égard.

Attendez un instant, monsieur Kurek. Je suis sur une bonne lancée.

Voilà où nous en sommes pour l'instant. Les représentants des syndicats et l'invité de M. Villemure comparaîtront le jeudi de la semaine de relâche, le commissaire de la GRC comparaîtra le 27 février et je m'attends à ce que nous commencions le rapport préliminaire sur l'étude des médias sociaux le 29 février. Ensuite, le 21 mars, c'est au tour de la présidente du Conseil du Trésor de comparaître.

Il est peu probable que nous puissions nous pencher sur la question. Nous avons également des semaines de relâche au mois de mars. Il est possible que nous puissions seulement nous pencher sur la question une fois que la plupart de ces semaines de relâche sont terminées. Cela vous convient-il? C'est bon.

Monsieur Kurek, vous avez la parole.

M. Damien Kurek: Vous avez répondu à ma question.

Mme Iqra Khalid: Vous avez également répondu à ma question.

Le président: C'est pour cette raison que j'étais sur une bonne lancée. Le seul problème, c'est que je ne l'ai pas fait en français. Je suis désolé, monsieur Villemure.

M. René Villemure: M. Kurek vous interrompait.

Le président: Impoliment... Il m'interrompait impoliment.

Des députés: Oh, oh!

Le président: Nous en sommes à la motion principale modifiée. Y a-t-il un consensus pour la motion principale modifiée ou voulons-nous procéder à un vote? Est-ce que cela convient pour tout le monde?

(La motion modifiée est adoptée.)

[*Français*]

Le président: Merci d'avoir proposé cette motion, monsieur Villemure.

J'avais...

[*Traduction*]

M. Michael Barrett: Monsieur le président, c'est la semaine nationale de la gentillesse. Je tiens simplement à le souligner.

En tant que parrain de la semaine nationale de la gentillesse à la Chambre des communes, j'aimerais simplement profiter de ce moment pour souhaiter à tout le monde une bonne semaine nationale de la gentillesse. L'adoption de cette motion à l'unanimité est un bon signe de la merveilleuse possibilité qu'offre notre grand pays.

Le président: Permettez-moi d'interpréter cela pour vous: M. Barrett proposera une motion à un moment donné.

Des députés: Oh, oh!

Le président: Je ne sais pas quand cela se produira, mais il recherchera le même type de gentillesse.

L'ordre du jour semble épuisé.

Je remercie la greffière, les analystes et les techniciens.

Je lève la séance. Nous nous reverrons tous jeudi.