CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

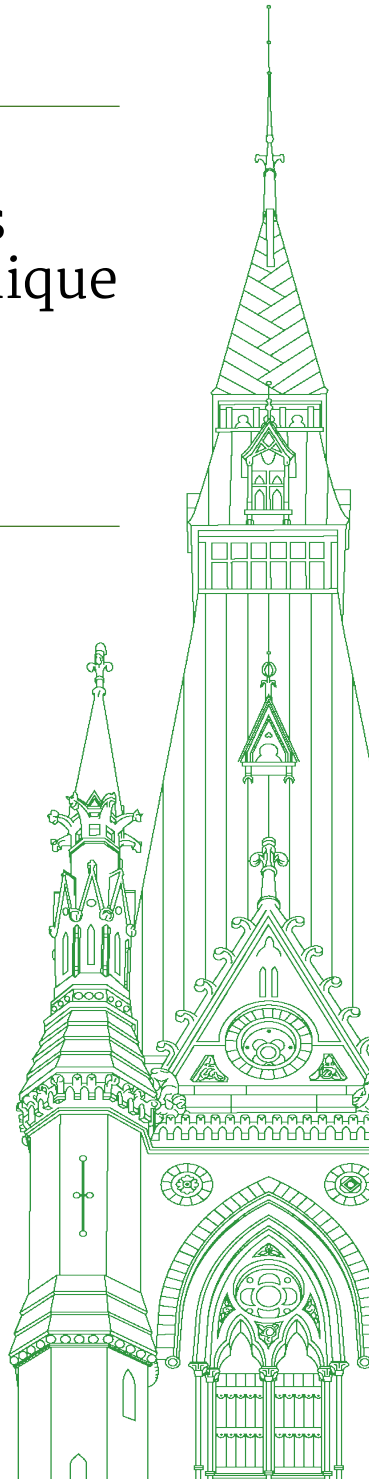
44e LÉGISLATURE, 1re SESSION

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

TÉMOIGNAGES

NUMÉRO 104

Le jeudi 15 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 jeudi 15 février 2024

● (1105)

[*Traduction*]

Le président (M. John Brassard (Barrie—Innisfil, PCC)): Bonjour à tous.

La séance est ouverte.

[*Français*]

Je vous souhaite la bienvenue à la 104e 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 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 au moyen de l'application Zoom.

[*Traduction*]

Je veux juste rappeler à tout le monde, comme je le fais toujours, de s'assurer de tenir les écouteurs loin des microphones pour ne pas blesser nos interprètes ou M. Light.

J'aimerais maintenant souhaiter la bienvenue à notre témoin pour la première heure. Nous accueillons M. Evan Light, qui est professeur agrégé et comparaît à titre personnel.

Monsieur Light, je vous souhaite la bienvenue au Comité. Vous avez cinq minutes pour faire un exposé.

Allez-y, s'il vous plaît.

[*Français*]

M. Evan Light (professeur agrégé, à titre personnel): Bonjour, mesdames et messieurs.

Je suis Evan Light, professeur agrégé au Collège universitaire Glendon de l'Université York.

[*Traduction*]

Je suis professeur agrégé en communications.

Je vais faire ma déclaration liminaire en anglais, mais je serai également heureux de répondre aux observations ou aux questions en français.

Comme l'un de vous l'a mentionné mardi, je suis la source des documents à partir desquels Radio-Canada fait ses reportages depuis novembre 2023 sur l'utilisation d'outils capables d'extraire des données personnelles des appareils mobiles et des ordinateurs.

Je suis très impressionné par la vitesse à laquelle vous avez relevé le défi d'enquêter sur l'utilisation répandue d'appareils d'analyse de dispositifs mobiles dans l'ensemble du gouvernement fédéral. Cela montre un profond respect pour le droit fondamental à la vie privée. La protection des renseignements personnels n'est pas une chose abstraite. C'est un droit fondamental qui est lié à d'autres droits de la personne. Au Canada, c'est un droit de la personne depuis 1977. Nous parlons de quelque chose qui est très fondamental.

Pour moi, cela signifie que c'est un droit qui ne devrait pas être violé à moins d'avoir une raison très bonne et bien documentée. Je pense que le témoignage des représentants des organismes que vous avez entendus jusqu'à maintenant ne nous permet pas nécessairement de qualifier l'utilisation qu'ils en font de « nécessaire et proportionnée », une expression utilisée à diverses reprises pendant vos dernières réunions.

Depuis 1977, les gouvernements qui se sont succédé n'ont pas protégé notre droit fondamental à la vie privée. Ce comité, en ce moment, a vraiment une excellente occasion — pas juste une occasion, mais aussi une obligation — d'agir et d'examiner comment le gouvernement protège le droit fondamental à la vie privée.

J'ai transféré de nombreux documents au Comité. Certains ont été traduits, d'autres pas, ce qui signifie que vous n'avez pas toute la documentation sur les sujets que je vais aborder aujourd'hui. Je veux parler de ces questions et de certains témoignages des représentants des organismes avec qui vous avez discuté jusqu'à maintenant.

J'ai vu ces appareils pour la première fois en 2020 en faisant de la recherche pour un cours. Un groupe aux États-Unis a documenté leur utilisation dans plus de 2 000 corps policiers du pays. De la documentation supplémentaire sur l'utilisation de ces outils par différents régimes partout dans le monde et sur leur intégration étroite avec des logiciels espions nous vient du Carnegie Endowment aux États-Unis.

Rapidement à propos de la terminologie, je ne considère pas les appareils d'analyse de dispositifs mobiles comme des logiciels espions. Il en a été question à maintes reprises à votre comité. Ils ont toutefois essentiellement les mêmes capacités. Ils sont vendus par les mêmes fournisseurs et sont utilisés par les mêmes entités. Je ne pense pas que nous devons prêter trop d'importance à la terminologie. Je pense que ce qui compte, c'est que leur utilisation est tout autant intrusive et non réglementée.

Ce qui me préoccupe, ce n'est pas l'existence de ces appareils, mais le fait que leur utilisation n'est pas réglementée. Divers organismes qui ont témoigné devant vous ont dit qu'ils ne savent pas vraiment comment ils s'en servent. Ils n'ont pas de chiffres. Le représentant de l'Agence des services frontaliers du Canada a dit qu'ils s'en servent tout le temps, mais ils ne peuvent pas nous dire le nombre de fois. Quant aux représentants de Services partagés Canada qui ont témoigné mardi, ils ont dit qu'il n'ont pas de politiques ou de procédures sur leur utilisation. Scott Jones décide lui-même à quel moment leur utilisation est justifiée.

Comme des témoins l'ont fait remarquer devant le Comité, l'utilisation des appareils est pertinente. Je crois que M. Mainville, du Bureau de la concurrence, a mentionné mardi qu'ils s'en servent depuis 1996, ce qui a été une révélation étonnante pour moi. Cela montre que le gouvernement se sert régulièrement de ces choses depuis des dizaines d'années. Cela n'a jamais été réglementé ni jamais fait l'objet d'une surveillance.

Tout au long des réunions que le Comité a consacrées à cette étude, des membres du Comité et des témoins ont utilisé l'expression « nécessaire et proportionnée », ou un des deux adjectifs. Je pense que cette expression est vraiment essentielle pour comprendre l'utilisation des appareils d'analyse de dispositifs mobiles ou toute autre technologie de surveillance par le gouvernement. En fait, c'est lié à un document publié en 2014 et préparé par 16 organisations de la société civile de partout dans le monde. C'est appuyé par environ 600 organisations et 300 000 particuliers. Le document s'intitule: « Nécessaire et proportionnée: Principes internationaux sur l'application des droits de l'homme à la surveillance des communications ».

Il faut se pencher sur des cadres juridiques. Il y a des normes pour comprendre comment faire la surveillance tout en respectant les droits de la personne, et je pense que le Canada peut en apprendre quelque chose et qu'il devrait peut-être le faire.

Je serai bref. Mes cinq minutes sont presque écoulées. Je vais terminer par un bref commentaire sur certains des témoignages entendus récemment.

Services partagés Canada et d'autres organisations ont dit qu'ils utilisent seulement les appareils d'analyse de dispositifs mobiles dans des laboratoires isolés, ce qui donne l'impression qu'ils sont vraiment coupés du monde. D'après les moyens et les appareils à leur disposition, c'est manifestement faux. Dans les contrats que j'ai transmis à votre comité, on voit que diverses entités, y compris l'Agence des services frontaliers du Canada, l'Agence du revenu du Canada, Environnement et Changement climatique Canada, la GRC et le Bureau de la sécurité des transports ont tous, ce qui s'appelle, UFED Cloud, un progiciel de Cellebrite qui permet essentiellement d'avoir accès à toutes les applications infonuagiques d'un téléphone. C'est présenté comme un moyen de contourner les mandats.

De plus, pour terminer, je mentionne que différents organismes ont des versions renforcées de ces appareils, ce qui signifie qu'on peut se rendre sur le terrain et les échapper, les utiliser çà et là. Ils n'achèteraient pas ces appareils renforcés s'ils s'en servaient uniquement dans des laboratoires cliniques isolés.

C'est avec plaisir que je vais répondre aux questions.

● (1110)

Le président: Merci, monsieur Light. Vous avez pris un peu plus de temps. C'est bon pour un témoin. Je veux bien en accorder un peu plus à un seul témoin.

À propos des documents dont M. Light a parlé, il y en a carrément des milliers, y compris certains qui sont plutôt volumineux. Ce serait toute une tâche de les faire traduire, comme vous pouvez l'imaginer, mais certains documents sont distribués au Comité en fonction de ce que M. Light nous a remis, et on a commencé à les traduire.

Nous allons commencer notre première série d'interventions de six minutes par M. Kurek.

Allez-y, monsieur, pour six minutes.

M. Damien Kurek (Battle River—Crowfoot, PCC): Merci beaucoup, monsieur le président.

Merci, monsieur Light, de votre présence ici ainsi que de l'information et de l'analyse qui ont mené à cette enquête.

Je voudrais simplement souligner — je suppose que c'est une demande, car il est parfois difficile de s'attaquer à l'essentiel dans le temps accordé aux questions — que vous avez mentionné qu'il existe des recommandations sur la façon dont un gouvernement peut garantir que les droits sont respectés pendant les enquêtes. Je me demande si vous pouvez, compte tenu de votre expertise, faire parvenir aux comités des recommandations précises — en général, une recommandation peut comprendre deux ou trois phrases — et si vous pouvez décortiquer cela au point de permettre au Comité d'avoir quelque chose à recommander au gouvernement.

Je fais juste remarquer, pour votre gouverne, monsieur Light, que j'ai déposé une question à inscrire au Feuilleton pour demander des détails supplémentaires sur l'ampleur de la situation dans l'ensemble de l'appareil gouvernemental. Je sais qu'on a mentionné 13 ministères. Services partagés Canada a dit qu'il pourrait y en avoir plus, et j'ai donc posé cette question, et j'espère que le gouvernement donnera cette information. Je crois qu'il a 45 jours pour répondre, donc probablement environ un mois et demi.

Vous avez parlé du droit à la vie privée et dit que c'est reconnu comme un droit de la personne au Canada depuis les années 1970. Une chose que je trouve très intéressante et qui a soulevé tout un éventail de préoccupations est la distinction entre l'utilisation de ces outils d'analyse très puissants à des fins administratives lorsqu'un ministère fouille l'appareil d'un employé dans le cadre d'enquêtes administratives ou quelque chose du genre et leur utilisation à la suite d'une ordonnance d'un tribunal pour fins d'enquête lorsque la personne n'est pas à l'emploi du ministère, n'a pas signé de contrat et fait plutôt l'objet d'une enquête ou qu'elle est un témoin indirect.

Puis-je vous demander d'expliquer un peu la différence et de dire comment quelqu'un peut réconcilier la distinction entre l'utilisation de ces outils puissants à des fins administratives, disons, dans un ministère ou un organisme, et leur utilisation pour obtenir des renseignements de Canadiens dans le cadre d'enquêtes, que ce soit avec une autorisation judiciaire ou les différents autres formulaires qui pourraient être utilisés selon ce qu'on nous a dit?

M. Evan Light: À propos de leur usage à l'interne, je pense que la plupart des représentants des organismes qui ont témoigné jusqu'à maintenant disent qu'ils s'en servent pour leurs employés et qu'ils obtiennent leur consentement. Il est difficile, voire impossible pour ces employés de donner leur consentement éclairé dans ces situations, car il y a un déséquilibre des pouvoirs ainsi qu'un déséquilibre des connaissances. Nous avons vu dans les réunions du Comité à quel point il est difficile d'expliquer ce que ces appareils peuvent faire. Prenez la situation suivante: un jeune employé se fait dire par un gestionnaire qu'on va utiliser un de ces appareils sur son téléphone. Il n'a pas vraiment le choix d'accepter. Je pense que cette utilisation à l'interne est plutôt périlleuse et déséquilibrée.

Lorsque la technologie est utilisée avec des mandats, je pense qu'il doit y avoir des étapes à suivre avant d'en obtenir un. Si nous parlons d'une utilisation « nécessaire et proportionnée », il y a des questions que nous devrions poser. D'entrée de jeu, l'utilisation de cette technologie est-elle valide? C'est ici qu'interviennent les évaluations des facteurs relatifs à la vie privée, qui sont inutiles selon moi dans une certaine mesure.

Elles expliquent l'autoréglementation actuelle. Les organismes ou les ministères ne sont pas tenus de suivre le moindre processus qui leur interdirait d'utiliser une technologie donnée. Nous avons vu pendant le témoignage de Scott Jones mardi qu'il achètera cette technologie pour toute personne au gouvernement qui veut l'obtenir. Il n'y a pas de norme, ce qui est effarant.

● (1115)

M. Damien Kurek: Il est intéressant que vous en parliez. J'ai été très franc quand j'ai conseillé — j'ai dit que ce n'était pas sollicité — de prendre le téléphone et d'appeler le commissaire à la protection de la vie privée. Nous avons un mandataire indépendant du gouvernement, et l'ensemble des ministères et des organismes sont une fonction du gouvernement. Je pense qu'on l'oublie souvent.

Plus précisément pour ce qui est des évaluations des facteurs relatifs à la vie privée, si les ministères, les organismes et le gouvernement en général étaient plus ouverts, qu'ils faisaient, par exemple, les évaluations et qu'ils communiquaient avec le commissaire à la protection de la vie privée avant d'utiliser ces outils, pensez-vous que cela aiderait beaucoup les Canadiens à rétablir la confiance qu'ils doivent avoir selon eux dans leur gouvernement?

M. Evan Light: Personnellement, je ne pense pas que ce serait assez.

Le Commissariat à la protection de la vie privée devrait avoir les ressources, y compris financières, et l'autorité judiciaire nécessaires pour être un organisme de réglementation proactif. Dans tout le processus d'approvisionnement, le Commissariat devrait être l'organisme qui décide si une technologie doit être utilisée ou non et dans quelles circonstances. Je pense vraiment que les organismes sont eux-mêmes dans une situation de conflit d'intérêts lorsqu'ils prennent leurs propres décisions sur l'utilisation ou non de certaines choses. Il devrait y avoir un arbitre objectif, qui pourrait être le Commissariat.

M. Damien Kurek: Je vois.

Vous proposez d'aller au-delà des évaluations des facteurs relatifs à la vie privée et de veiller à ce que le Bureau ait plus d'étapes à suivre et d'outils à sa disposition.

M. Evan Light: Absolument. Je pense que l'évaluation des facteurs relatifs à la vie privée est un outil utile pour amener les particuliers et les organismes à réfléchir à ces idées. Je ne pense toutefois pas que c'est un outil réglementaire utile.

M. Damien Kurek: Si vous avez ces recommandations précises, n'hésitez pas à les transmettre au Comité. Il faut souvent juste une ou deux phrases pour articuler exactement ce qu'on propose, et compte tenu de votre expertise et de vos connaissances, je vous invite également à nous faire parvenir des documents d'appui. Je sais qu'il y a beaucoup plus d'information, et n'hésitez surtout pas à la transmettre au Comité après votre témoignage d'aujourd'hui.

Le président: Merci, monsieur Kurek.

Monsieur Light, généralement, ce que nous essayons de faire au Comité, c'est établir une échéance pour le dépôt de l'information. Je vais la fixer à une semaine à partir d'aujourd'hui, à 17 h. La greffière fera un suivi auprès de vous pour vous rappeler ce que M. Kurek a demandé.

Monsieur Housefather, vous avez six minutes. Allez-y, s'il vous plaît.

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

Merci de votre présence parmi nous aujourd'hui, monsieur Light.

Selon le reportage de CBC, vous vous êtes dit troublé — profondément préoccupé, je suppose — lorsque la journaliste vous a mentionné que les évaluations des facteurs relatifs à la vie privée n'étaient pas effectuées dans les 13 ministères. J'imagine que vous avez entendu les témoignages des représentants des différents ministères.

Vous ne rejetez aucunement leur analyse voulant qu'ils n'utilisent pas de logiciels espions ou malveillants et ne cherchent pas à espionner les Canadiens en général, n'est-ce pas?

M. Evan Light: Je n'ai pas de preuve dans un sens comme dans l'autre. Je n'ai pas fait cette recherche. Je me suis penché un peu sur la question.

Il est difficile d'étudier l'approvisionnement. Nous nous servons de contrats qui ont été rendus publics. Je pense que beaucoup d'entreprises de logiciels espions vendent leurs produits par l'entremise de tiers, et il est donc difficile d'étudier la question au sein du gouvernement.

Cependant, dans les données à ma disposition, je n'ai rien vu dans un sens comme dans l'autre, et je ne peux donc pas...

M. Anthony Housefather: Non, mais ils ont dit qu'ils n'en utilisent pas.

Vous n'avez absolument rien pour contredire ce témoignage, n'est-ce pas?

M. Evan Light: En effet.

M. Anthony Housefather: D'accord. Donc, vous n'avez aucune raison d'affirmer le contraire. Vous ne le savez tout simplement pas. Vous dites que vous ne pouvez pas affirmer avec certitude que leurs témoignages étaient véridiques.

M. Evan Light: Exactement.

M. Anthony Housefather: D'accord.

À propos de la technologie d'extraction de données, vous devez avoir l'appareil en votre possession. Êtes-vous d'accord? Ce n'est pas un logiciel espion ou malveillant.

● (1120)

M. Evan Light: Il faut avoir l'appareil au départ. Des composants matériels des appareils d'analyse de dispositifs mobiles permettent de créer une image du téléphone. Imaginez qu'on vous arrête à la frontière et qu'on vous demande votre téléphone. Il faut peut-être cinq minutes pour faire une copie d'un téléphone. On a ensuite une image, comme une image CD, que l'on peut sauvegarder sur une clé USB et transmettre à d'autres organismes. Les données deviennent portables.

M. Anthony Housefather: Vous dites maintenant que les gens agissent totalement en marge de la loi, à l'extérieur des limites d'un mandat et de leur autorité.

Vous n'avez entendu aucun témoignage qui montre que cela s'est déjà produit, n'est-ce pas?

M. Evan Light: C'est exact.

M. Anthony Housefather: Vous n'avez pas de raison de le croire, mais vous supposez que c'est hypothétiquement possible.

M. Evan Light: En effet.

De plus, je m'appuie seulement sur les capacités de ces technologies et sur la façon dont elles sont présentées. Par exemple, dans les documents promotionnels de Cellebrite, vous verrez que l'entreprise présente ses capacités infonuagiques comme moyen de contourner les mandats. Dans le passé, il fallait obtenir un mandat pour pouvoir consulter le compte infonuagique d'une personne, pour avoir accès à ses informations bancaires par l'entremise de son téléphone, pour consulter son historique sur Google Maps, sur ses applications GPS, etc. Au sujet de la fonctionnalité infonuagique que possèdent ces cinq organismes, comme je l'ai dit, c'est présenté comme un moyen de contourner les mandats. Ils ne sont plus nécessaires. Il faut seulement un téléphone et son image.

M. Anthony Housefather: Encore une fois, je comprends ce qu'on peut faire hypothétiquement avec la technologie. Tout ce que je dis, c'est que nous avons entendu de nombreux témoins, et aucun d'entre eux n'a dit quoi que ce soit de tel. Comme vous le savez, lorsqu'on participe à une réunion d'un comité, qu'on soit assermenté ou non, on est tenu de dire la vérité sous peine de parjure ou d'outrage au Parlement.

Personne n'a témoigné à ce sujet. En fait, je vais simplement lire ce que l'ASFC a dit:

> Les appareils examinés par les équipes d'informatique judiciaire de l'ASFC ont été saisis en vertu d'ordonnances judiciaires précises, comme des mandats de perquisition ou des autorisations judiciaires, délivrées aux enquêteurs de l'Agence. Les données extraites des appareils numériques saisis sont traitées uniquement dans les laboratoires judiciaires numériques de l'ASFC et ne sont fournies qu'aux personnes légalement autorisées à y accéder.

L'ASFC a aussi déclaré ce qui suit:

> J'aimerais également préciser qu'on définit généralement les logiciels espions comme des logiciels installés sur un appareil dans le but d'intercepter, de surveiller ou de recueillir secrètement les activités ou les données d'un utilisateur. Je tiens à assurer au Comité et à la population canadienne que les outils judiciaires numériques utilisés par les enquêteurs de l'ASFC ne sont pas des logiciels espions. Nous utilisons du matériel et des logiciels judiciaires pour déverrouiller et décrypter les appareils numériques saisis, et ce sont des outils importants dans nos efforts visant à faire respecter la législation frontalière et à protéger les Canadiens.

Vous n'avez aucune raison de contester ces propos, n'est-ce pas?

M. Evan Light: Non, je n'en ai pas.

M. Anthony Housefather: D'accord. Tout ce que je voulais établir, c'est que je comprends. C'est une technologie qui fait vraiment peur à beaucoup de gens, car elle peut être utilisée de façon inappropriée, et nous devons mettre en place des mesures de protection pour nous assurer qu'elle n'est pas utilisée de façon inappropriée. Beaucoup de mauvaises choses peuvent se produire, mais nous n'avons aucune preuve de mauvais usages, et je ne veux pas effrayer les Canadiens en leur faisant croire qu'il y en a.

M. Evan Light: En même temps, il n'y a pas nécessairement de surveillance ou de transparence quant à l'utilisation de ces outils, qui remonte à près de quatre ans maintenant.

M. Anthony Housefather: Encore une fois, c'est ce que vous prétendez. Je dirais que nous avons une surveillance du fait que les dirigeants des ministères et certaines personnes sont assujettis à des règles d'éthique assez strictes, mais je comprends ce que vous dites. Bien sûr, il y a des craintes, et nous devons nous assurer qu'il existe des mesures de protection. Notre travail en tant que comité est de formuler des recommandations pour veiller à ce que des politiques et des règlements soient en place pour atténuer toute préoccupation qui pourrait exister.

Me reste-t-il du temps, monsieur le président?

M. Larry Brock (Brantford—Brant, PCC): J'invoque le Règlement, monsieur le président.

Le président: Allez-y.

M. Larry Brock: Je me demande si M. Housefather souhaite comparaître comme témoin et si nous pouvons l'interroger, car il est certes en train de présenter des témoignages...

Mme Iqra Khalid (Mississauga—Erin Mills, Lib.): Je ne pense pas que ce soit un rappel au Règlement, monsieur le président.

M. Larry Brock: Il est en train de présenter des témoignages que le Comité n'a pas entendus de la part de témoins.

Mme Iqra Khalid: Je ne sais pas pourquoi nous arrêtons cela...

M. Anthony Housefather: En fait, je viens de lire un extrait du témoignage...

Le président: Un instant, monsieur Housefather.

Ce n'est pas un rappel au Règlement, monsieur Brock.

M. Housefather a la parole et, comme tous les membres, il a le droit de donner son opinion, de formuler des commentaires et de poser ses questions. Comme les membres du Comité le savent, chaque député est maître de son temps de parole.

Allez-y, monsieur Housefather.

M. Anthony Housefather: Combien de temps me reste-t-il, monsieur le président?

Le président: J'ai arrêté le chronomètre à 1:14.

M. Anthony Housefather: Merci.

J'apprécie les commentaires de mon collègue, M. Brock. Il est probablement la personne la plus loquace quand vient le temps de donner son opinion, alors je suis un peu surpris.

Je vais revenir à vous, monsieur Light, au sujet d'une question plus générale. Je comprends les nombreux problèmes que vous avez soulevés dans vos documents, et j'ai hâte d'obtenir les copies traduites lorsque nous les recevrons. Nous ne les avons pas encore reçues.

Si vous aviez une recommandation à faire pour modifier les politiques actuelles du Conseil du Trésor ou d'autres politiques existantes, quelle serait-elle? Quelle serait votre principale recommandation?

M. Evan Light: Je dirais que les évaluations des facteurs relatifs à la vie privée du Conseil du Trésor devraient être obligatoires selon la loi, et qu'elles devraient être effectuées avant tout achat. À ce jour, dans le cadre de mes recherches plus générales, nous avons présenté environ 250 à300 demandes d'accès à l'information concernant des centaines de contrats, qui représentent environ 800 millions de dollars d'achats liés à la surveillance. C'est une somme énorme.

Tout récemment, j'ai reçu un contrat mis à jour de Teel Technologies pour des appareils judiciaires mobiles d'une valeur de 11 millions de dollars. La Commission du droit d'auteur faisait partie pour la première fois des organismes auxquels ce genre d'appareils est destiné. Il s'agissait d'un contrat récent, d'un renouvellement. Si nous nous préoccupons des dépenses, nous devrions vraiment poser de sérieuses questions sur les acquisitions en matière de technologie avant l'achat.

● (1125)

M. Anthony Housefather: Merci.

[*Français*]

Le président: Merci, messieurs Housefather et Light.

Je demande à tous les intervenants de parler un peu plus lentement, afin de faciliter la tâche des interprètes.

[*Traduction*]

Je ne savais pas que vous étiez encanteur, monsieur Housefather. Est-ce vrai? Non.

Si vous le pouvez, parlez un peu plus lentement pour les interprètes, si vous n'y voyez pas d'inconvénient. Merci beaucoup.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

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

Monsieur Light, je vous remercie de votre présence.

Vos travaux ont mené à la rédaction d'un article, et c'est la raison pour laquelle nous sommes ici aujourd'hui. Les témoignages que nous avons entendus jusqu'à maintenant se ressemblent beaucoup. On dit avoir acquis l'outil et avoir fait des vérifications par le passé. On nous dit aussi qu'on n'a pas fait d'évaluation des facteurs relatifs à la vie privée, mais qu'on en fera une. C'était l'essence de plusieurs témoignages que nous avons reçus.

En matière de protection de la vie privée, une telle attitude vous semble-t-elle normale?

M. Evan Light: Non.

Je rappelle que, dans l'article de Radio-Canada, publié en novembre dernier, je parlais de la normalisation de la surveillance au sein du gouvernement.

[*Traduction*]

Je pense qu'on m'a cité ici au Comité pour avoir parlé de ce qui me semblait être une normalisation de la surveillance au sein du gouvernement.

[*Français*]

Il s'agit de quelque chose qui m'inquiète. On dit que la surveillance est quelque chose de normal, mais, en fait, ce devrait plutôt être quelque chose d'extraordinaire. Le droit à la vie privée est fondamental et doit être protégé par défaut.

M. René Villemure: La plupart des témoins nous ont également dit avoir demandé un mandat judiciaire et avoir agi dans les limites de celui-ci. Je leur ai demandé si le mandat judiciaire remplaçait l'évaluation des facteurs relatifs à la vie privée, mais les réponses que j'ai reçues étaient moyennement satisfaisantes. J'avais l'impression de poser une question inutile.

Selon vous, l'évaluation des facteurs relatifs à la vie privée doit-elle précéder le mandat, le suivre ou le remplacer?

M. Evan Light: Selon moi, ça doit absolument précéder un mandat.

M. René Villemure: Est-ce que vous croyez que, s'il y avait un changement à la loi, cette évaluation des facteurs relatifs à la vie privée devrait être imposée en tout temps comme première étape?

M. Evan Light: Oui.

M. René Villemure: D'accord.

Vous parliez un peu de proportionnalité plus tôt. Dans la recherche d'information, est-ce que c'était le seul outil disponible pour obtenir l'information en question, ou était-ce trop invasif? Vous avez touché un mot de la proportionnalité dans votre mot d'ouverture. J'aimerais que vous précisiez un peu votre pensée à ce sujet.

M. Evan Light: Je crois qu'il en a aussi été question dans le témoignage des représentants des agences. Mardi, par exemple, Scott Jones et Mario Mainville ont parlé de la nécessité de trouver un équilibre entre la violation de la vie privée des employés et les données dont on a besoin ou qui existent. Dans leurs usages, il y a une tentative de trouver cet équilibre.

M. René Villemure: Personnellement, si j'utilise un appareil fourni par le gouvernement, mes attentes quant au respect de ma vie privée seront moindres que si j'ai mon propre appareil, mais elles ne seront pas nulles.

M. Evan Light: Non, pas du tout.

M. René Villemure: D'accord.

Vous avez parlé de l'usage illégal de l'infonuagique, tantôt, notamment dans le cas de Cellebrite. Est-ce que vous pourriez nous en dire un peu plus à ce sujet, s'il vous plaît?

M. Evan Light: Oui, absolument. Je vais le faire en anglais pour être plus efficace.

[*Traduction*]

Cellebrite et d'autres entreprises, par exemple Magnet Forensics, ont la capacité d'extraire ce qu'on appelle des « jetons ». Lorsque des applications sur un téléphone se connectent au nuage, ce sont des jetons qui essentiellement permettent la connexion. Ils servent d'identifiants uniques pour se connecter à un service infonuagique.

En fait, Cellebrite vient de mettre à jour son UFED Cloud, qui est utilisé par au moins cinq ou six organismes, afin qu'il puisse avoir accès aux registres de Lyft et d'Uber. Il peut aussi accéder aux registres de vol des drones de DJI, aux comptes bancaires, aux historiques des recherches sur Google et aux historiques des GPS.

Dans le passé, il aurait fallu obtenir un mandat pour pouvoir accéder à chaque élément relié à une société, et peut-être que cette société aurait reçu un mandat et aurait dû fournir l'information en question. Au lieu de cela, avec un appareil ou une image d'un appareil, on peut maintenant accéder à cette information sans mandat.

● (1130)

[*Français*]

M. René Villemure: Cela représente donc une violation possible de la vie privée.

M. Evan Light: Oui.

M. René Villemure: D'accord.

Tous les témoins ont dit qu'ils avaient compris et qu'ils feraient une évaluation des facteurs relatifs à la vie privée.

Selon vous, est-ce qu'il y avait de la négligence ou était-ce un oubli? Quelle est la raison pour laquelle on ne l'a pas fait, selon vous? Je ne tente pas de faire des reproches à qui que soit, ici. Je tente juste de comprendre, parce qu'ils ont tous dit qu'ils ne l'avaient pas fait, mais qu'ils le feraient à l'avenir. J'en conclus qu'ils reconnaissent le bien-fondé de la chose.

M. Evan Light: Si ça ne s'était produit qu'à une agence, ce serait un petit bémol. Cependant, si ça se produit à toutes les agences, c'est un problème. C'est quelque chose de systématique, ce n'est pas juste un oubli. Ça devient assez normal d'oublier que le droit à la vie privée est un droit fondamental.

M. René Villemure: C'est peut-être dans la culture des organisations publiques.

Vous aviez trouvé 13 ministères et organismes. Depuis, est-ce que vous avez trouvé d'autres organisations du domaine public? Est-ce qu'il y en a plus, selon vous?

M. Evan Light: Parmi les contrats que je mentionnais il y a quelques minutes, il y en a notamment un avec Teel Technologies. Récemment, j'ai vu que Services partagés Canada avait changé sa pratique d'approvisionnement. Maintenant, on n'achète plus cette technologie directement des fournisseurs comme Cellebrite, mais plutôt de Teel Technologies, une entreprise qui est située à Victoria, en Colombie-Britannique. Le contrat actuel durera jusqu'à l'été 2024.

La Commission du droit d'auteur du Canada est aussi maintenant parmi les agences…

M. René Villemure: Il y en a donc plutôt 14.

M. Evan Light: Il y a plus de 13 ministères et organismes. J'étais assez inquiet d'entendre M. Jones dire mardi qu'il pouvait acheter cette technologie pour n'importe où et pour n'importe qui. Si on est au gouvernement, on peut passer la commande et acheter ça.

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

Le président: Merci, messieurs Villemure et Light.

[*Traduction*]

Monsieur Green, vous avez six minutes. Allez-y, s'il vous plaît.

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

J'ai pris bonne note de l'utilisation que mon bon ami, M. Villemure a faite de son iPad pour chronométrer le temps de parole, alors j'espère être efficace, même si je ne procéderai certainement pas avec la même rapidité que celle avec laquelle mon ami M. Housefather a pu poser ses questions.

Notre étude est déjà bien entamée. Habituellement, lorsque des experts témoignent, nous leur donnons le temps de présenter leur domaine d'expertise. Dans votre déclaration préliminaire, vous n'avez pas eu l'occasion de le faire. Je veux vous donner la possibilité de le faire maintenant. Je crois savoir, d'après votre profil, que vous publiez beaucoup d'articles sur les questions de protection de la vie privée, de surveillance et de communications. Pour mettre les choses en contexte, vous pourriez peut-être nous faire part de votre expertise.

M. Evan Light: Oui, avec plaisir.

Je suis professeur agrégé en communications au Collège Glendon de l'Université York. J'ai étudié le domaine des politiques relatives au spectre des radiofréquences, ce qui m'a amené à me pencher sur la surveillance. Bon nombre des ondes radioélectriques que nous utilisons servent également à la surveillance. Je détiens une archive des documents d'Edward Snowden. Depuis une dizaine d'années, je participe très activement à des recherches sur les questions de surveillance et de protection de la vie privée.

M. Matthew Green: Diriez-vous que vous préconisez un gouvernement ouvert et transparent?

M. Evan Light: Absolument.

J'ai aussi une formation en informatique. Avant de devenir universitaire, j'ai travaillé dans le domaine des TI pendant une dizaine d'années. J'ai terminé ma carrière en TI en tant que technicien de réseau en chef à la Faculté de droit de l'Université McGill, alors j'envisage les enjeux du point de vue de l'arrière-plan...

M. Matthew Green: C'est un point de vue unique.

M. Evan Light: Oui, c'est juste.

M. Matthew Green: Ce qui me frappe, entre autres, c'est qu'en tant que législateurs, nous sommes souvent chargés d'essayer de faire des propositions concernant des technologies et des domaines que nous ne connaissons pas bien. Je reconnais que je ne suis pas un spécialiste des domaines que vous venez de mentionner, dans lesquels vous avez une expertise.

S'il est vrai qu'il y a de bons fonctionnaires qui, au mieux de leurs capacités, posent des jugements au quotidien sur la protection de la vie privée et la proportionnalité des outils qu'ils utilisent, peut-on dire que la technologie dont vous parlez dépasserait probablement la portée des connaissances d'une personne moyenne au sein du gouvernement et probablement même des gens autour de cette table?

M. Evan Light: C'est une technologie assez ésotérique.

M. Matthew Green: Et c'est une technologie de pointe.

● (1135)

M. Evan Light: Oui.

M. Matthew Green: Vous avez dit plus tôt que l'un des signaux d'alarme — je vais dire un signal d'alarme, mais ce n'est pas ce que vous avez dit — que vous avez relevés en examinant les entreprises auprès desquelles les appareils ont été achetés, c'est qu'elles commercialisent en fait des moyens d'utiliser subrepticement des dispositifs pour faire des choses qu'on ne peut pas faire directement au moyen d'un mandat. Est-ce bien ce que vous affirmez?

M. Evan Light: Oui.

M. Matthew Green: C'est d'ailleurs ce qu'indiquent leurs documents de marketing.

M. Evan Light: Oui.

M. Matthew Green: C'est un problème. C'est un problème pour moi, parce que je me fie aux témoignages des gens qui comparaissent ici, mais je ne m'attends pas à ce qu'ils connaissent toutes les façons dont la technologie qu'ils achètent pourrait avoir une incidence sur leurs travailleurs ou sur la population. Je parle de toutes les façons dont les atteintes à la protection des données se produisent dans les entreprises de haute technologie et, en fait, au sein du gouvernement, lors desquelles des renseignements de nature très délicate sont communiqués à grande échelle au moyen d'attaques malveillantes.

En vous fondant sur votre expertise en la matière, avez-vous des préoccupations quant à la possibilité que cette technologie soit utilisée de manière à entraîner des atteintes importantes à la vie privée des personnes?

M. Evan Light: Absolument. Je pense que son utilisation au sein des organismes du gouvernement fédéral et par ces organisations constitue vraiment la pointe de l'iceberg. Personne, y compris moi-même... Je n'ai pas eu l'occasion, jusqu'à présent, d'examiner l'utilisation de cette technologie dans les services de police de l'ensemble du Canada et au sein de tous les ordres de gouvernement, mais je peux dire qu'il y a un grand risque d'abus.

M. Matthew Green: L'un des problèmes auxquels nous sommes confrontés — et c'est mon opinion personnelle —, c'est le manque de confiance et le cynisme à l'égard du gouvernement et dans certains domaines, qui favorisent des théories du complot. En tant que défenseur d'un gouvernement ouvert, seriez-vous d'accord pour dire qu'une plus grande transparence, une plus grande ouverture, laisse moins de place aux théories du complot ou au cynisme? Autrement dit, un gouvernement ouvert engendre-t-il une plus grande confiance envers les institutions gouvernementales?

M. Evan Light: Absolument.

M. Matthew Green: Pour ce qui est d'essayer de faire le suivi des approvisionnements — je me suis occupé d'un dossier qui portait sur les approvisionnements au gouvernement, et j'ai trouvé cela très difficile —, pouvez-vous nous parler de certaines des difficultés que vous avez éprouvées à cet égard? Par exemple, lors d'une réunion antérieure, vous vous souviendrez peut-être que j'ai demandé au directeur de l'approvisionnement d'un ministère à quoi correspondait le poste de dépenses en technologie, et il n'a pas été en mesure de me répondre. Je voulais aussi savoir à quoi correspondaient les postes de dépenses concernant l'approvisionnement en technologie sur appareil, à savoir les logiciels espions.

Pouvez-vous nous parler des raisons pour lesquelles il est très difficile, même pour quelqu'un possédant votre expertise et votre expérience en recherche, de suivre la balle au bond lorsqu'il s'agit de faire le suivi de ce que fait le gouvernement et des dépenses qu'il effectue?

M. Evan Light: Bien sûr. Heureusement, j'ai une adjointe à la recherche qui a déjà travaillé dans le secteur privé et qui rédigeait des contrats passés avec le gouvernement, alors elle comprend l'approvisionnement d'une autre façon que moi.

Lorsque nous faisons une recherche, nous nous retrouvons essentiellement avec une longue liste d'entreprises qui, nous le savons, ne produisent à peu près rien d'autre que des outils de surveillance. Nous fouillons dans la base de données du gouvernement ouvert sur les contrats gouvernementaux de plus de 10 000 $. Cela ne nous donne accès qu'à un ou deux contrats de plus de 10 000 $. Les contrats d'une moindre valeur ne figurent pas dans les bases de données, alors on ne peut pas effectuer des recherches concernant ces contrats. De toute façon, la description des contrats est très générique. Il est difficile de tout décortiquer et de déterminer ce qui est utilisé, à moins d'obtenir cette information grâce à une demande d'accès à l'information.

Au cours des trois dernières années, nous avons déposé des centaines de demandes d'accès à l'information. Notre taux de réponse est d'environ 37 %, alors nous avons des centaines de demandes d'accès à l'information en suspens concernant des contrats d'une valeur totalisant des centaines de millions de dollars.

M. Matthew Green: Ne réglerions-nous pas le problème en procédant à une divulgation proactive de ces contrats, en ayant une base de données que l'on pourrait consulter, au lieu de devoir recourir à des demandes d'accès à l'information?

M. Evan Light: Oui, tout à fait, et j'ai vu cela ailleurs. À titre d'exemple, en Uruguay en 2010, on développait des technologies du gouvernement ouvert très intéressantes, où l'on pouvait voir en temps réel les dépenses au sein de chaque ministère, et l'on pouvait effectuer un suivi de ce qui se passait.

M. Matthew Green: J'ai terminé. Je vous remercie beaucoup.

Le président: Je vous remercie, monsieur Green, et je vous remercie aussi, monsieur Light.

C'est ce qui met fin à notre série de six minutes. Nous passons à la série de cinq minutes, en commençant par M. Brock.

Monsieur Brock, allez-y.

M. Larry Brock: Je vous remercie, monsieur le président.

Bonjour, monsieur Light.

Je ne veux pas parler de l'outil comme tel ou du logiciel qui y est rattaché — le sujet principal de cette séance du Comité —, mais plutôt de l'enjeu de la protection des renseignements personnels en général. Vous avez dit grosso modo qu'il s'agit d'un droit de la personne fondamental. C'est un droit fondamental au Canada depuis 1977.

Monsieur, j'aimerais avoir votre opinion d'expert sur le désastre que constitue l'application ArriveCAN qui, comme on vient de le découvrir, s'est révélé être un gaspillage de fonds publics de plus de 60 millions de dollars.

Souvenez-vous de l'époque où le gouvernement faisait activement la promotion de l'application ArriveCAN. C'était la solution pour lutter contre la COVID, pour mieux protéger les Canadiens, etc. J'aimerais avoir votre avis sur le préambule de l'application quand on s'y inscrit. Il s'intitule: « Comment vos renseignements sont utilisés et divulgués », et on dit:

> Les renseignements personnels peuvent être communiqués à des entrepreneurs travaillant pour l'Agence de la santé publique du Canada et Service Canada, ainsi qu'aux entités suivantes: d'autres institutions gouvernementales, ainsi que les gouvernements provinciaux, territoriaux, municipaux ou des organisations internationales de la santé et leurs institutions servant à ces fins.
>
> Les renseignements personnels peuvent également être utilisés pour l'évaluation du programme. Dans d'autres circonstances limitées et particulières, les renseignements personnels peuvent être utilisés ou communiqués sans consentement, conformément à l'article 7 et au paragraphe 8(2) de la Loi sur la protection des renseignements personnels.

Il semble que des millions de Canadiens qui ont été forcés par le gouvernement Trudeau de s'inscrire à l'application ArriveCan ont vu leurs renseignements personnels largement...

● (1140)

Mme Iqra Khalid: J'invoque le Règlement, monsieur le président.

Le président: Monsieur Brock, arrêtez-vous un instant. Il y a un rappel au Règlement.

Madame Khalid, allez-y.

Mme Iqra Khalid: Je vous remercie, monsieur le président.

Je m'interroge sur la pertinence des questions de M. Brock. Je suis certaine que le témoin n'a pas été convoqué pour répondre aux questions que M. Brock veut explorer.

Le président: Un instant, je vous prie. Quand quelqu'un invoque le Règlement, je suis constant dans mes décisions. Je l'ai fait dans le cas de M. Housefather, et je fais la même chose dans le cas de M. Brock.

C'est son temps de parole. Nous avons un expert sur les questions de protection des renseignements personnels avec nous. Je vais permettre à M. Brock de poursuivre. Il a la parole, et je suis certain que son intervention arrivera à son but.

Monsieur Brock, vous avez la parole.

Mme Iqra Khalid: J'aimerais apporter une petite précision...

Le président: Madame Khalid, c'est inutile d'insister. Je préside ce comité depuis près d'un an et demi, et j'ai toujours été constant dans mes décisions en toute circonstance et à l'égard de tous les membres du Comité.

Monsieur Brock, il vous reste trois minutes et deux secondes. Allez-y.

M. Larry Brock: Vous avez entendu ce qui vient d'être dit. Certains députés libéraux ne se soucient pas de la protection des renseignements personnels, mais les députés conservateurs s'en soucient assurément.

Mme Iqra Khalid: Je m'oppose à ces propos.

Le président: Monsieur Brock, c'est une question d'opinion.

Mme Iqra Khalid: Monsieur le président, j'allais m'abstenir de le dire, mais je vais le faire maintenant. M. Brock a commencé son intervention en disant qu'il allait poser des questions qui ne portent pas sur le sujet à l'étude aujourd'hui.

Le président: Je ne suis pas certain de l'avoir entendu dire cela, mais je peux certainement le vérifier.

Monsieur Brock, il vous reste 2 minutes et 50 secondes.

M. Larry Brock: Je parle de la protection des renseignements personnels.

Monsieur Light, pouvez-vous me donner votre opinion sur ce que je viens de vous lire? Cela présente-t-il ou présentait-il un danger?

M. Evan Light: Certainement. Je tiens juste à préciser auparavant que je ne suis membre d'aucun parti politique, et je crois que la question de la protection des renseignements personnels est un enjeu totalement non partisan. On parle ici d'un droit de la personne.

M. Larry Brock: Oui.

Mr. Evan Light: C'est n'est pas négociable et ce n'est pas discutable.

Le préambule que vous avez lu est vraiment intéressant parce qu'il renvoie — si vous vous souvenez du projet de loi C-51 — à la loi du gouvernement Harper qui a porté l'échange de données entre les organismes gouvernementaux à un tout autre niveau.

Le préambule énonce en quelque sorte comment cela s'est produit. Il nous montre comment l'information circule entre les organismes et comment cela est devenu une pratique courante. Cela remonte très loin. Ce n'est rien de nouveau. Cela remonte probablement avant les années Harper. C'était sans doute une pratique informelle qui est maintenant plus officielle.

Cela me fait peur, en effet. Comme j'ai utilisé moi-même ArriveCAN quand l'application est sortie parce que je trouvais cela plus simple — je n'avais pas de papier à remplir dans l'avion —, je pense que les technologies que l'on utilise dans nos aéroports et à la frontière sont très intrusives. Elles le sont aussi ailleurs dans le monde. Je suis allé dans des aéroports en Europe où je ne pouvais pas obtenir une connexion sans un balayage de mon visage et de mes mains.

Je ne pense pas qu'on ait atteint ici un tel niveau d'intrusion, mais oui, je pense que c'est un problème.

M. Larry Brock: Je pense, principalement en raison des mots « sans consentement », que c'est extrêmement problématique.

Êtes-vous d'accord avec moi sur ce point?

M. Evan Light: Oui, je pense que cela place un voyageur dans une position, par exemple, comme dans le cas où l'on utilise des appareils judiciaires mobiles au sein des organismes à des fins administratives... On se trouve dans une position où l'on ne peut pas nécessairement consentir, où il y a un déséquilibre du pouvoir, alors on le fait parce que...

M. Larry Brock: On peut seulement en déduire que le gouvernement a actuellement en sa possession des renseignements qui ne sont pas utilisés pour protéger la population contre la COVID.

Je veux aussi vous parler d'un autre problème...

Combien de temps me reste-t-il, monsieur le président?

Le président: Il vous reste 45 secondes, monsieur Brock, et je suis strict.

M. Larry Brock: Je vous remercie.

Vous savez que la vérificatrice générale a publié un rapport. Elle y parle de la cybersécurité, des fuites et du fait que les fournisseurs n'avaient pas la cote de sécurité requise.

Quelle importance accordez-vous à cela? Qu'en pensez-vous?

M. Evan Light: Je ne peux pas vous répondre. Je n'ai pas lu le rapport en détail.

M. Larry Brock: Vous ne l'avez pas lu.

M. Evan Light: Non.

M. Larry Brock: D'accord. Il dit: « Même si l'Agence nous a affirmé que les ressources n'avaient pas eu accès aux renseignements personnels des voyageuses et des voyageurs, le fait qu'il y ait eu des ressources ne disposant pas d'une autorisation de sécurité a exposé l'Agence à un risque accru d'atteintes à la sécurité. » On mentionne cela en lien avec le fait que l'agence a accordé à des fournisseurs qui n'avaient pas la cote de sécurité requise le pouvoir d'avoir accès à des renseignements sur les voyageurs.

Que pensez-vous de cela, monsieur?

● (1145)

M. Evan Light: Je dirais que c'est problématique.

Le président: Je vous remercie, monsieur Brock.

Madame Khalid, allez-y, s'il vous plaît.

Mme Iqra Khalid: Je vous remercie beaucoup, monsieur le président.

Monsieur Light, je vous remercie d'être avec nous aujourd'hui.

Le député de Brantford—Brant a déclaré dernièrement au comité des opérations gouvernementales qu'il n'y a pas de problème lié à la protection des renseignements personnels dans le cas des fonctionnaires.

Croyez-vous que les fonctionnaires ont droit à la protection de leurs renseignements personnels?

M. Evan Light: Oui, et il y a quelques semaines, Brigitte Bureau, de Radio-Canada, a publié un article qui portait exactement sur cette question et elle a interviewé deux experts juridiques à ce sujet. Je ne suis pas avocat et je ne me considère pas comme un expert juridique, mais un professeur de droit et un avocat ont tous les deux dit que les employés, les fonctionnaires, s'attendent à ce que leurs renseignements personnels soient protégés, et y ont droit, même lorsqu'ils utilisent des appareils émis par le gouvernement. Il y a une différence entre l'appareil comme tel et son contenu.

Mme Iqra Khalid: Lorsqu'un fonctionnaire, par exemple, reçoit un appareil qu'il utilise pour son travail, ce dont nous parlons dans ces 13 ministères, a-t-il une attente raisonnable en matière de protection des renseignements personnels sur ces téléphones du gouvernement, qu'il utilise et qui lui ont été fournis pour qu'il puisse mieux faire son travail?

M. Evan Light: Je crois que oui.

Mme Iqra Khalid: Compte tenu des attentes raisonnables en matière de protection des renseignements personnels et du consentement, quel est le rôle de l'évaluation des facteurs relatifs à la vie privée dans la manière dont les ministères gèrent leurs relations avec leurs employés?

M. Evan Light: À l'heure actuelle, je pense que les évaluations des facteurs relatifs à la vie privée ne sont pas nécessairement la norme. Elles poussent une agence à poser des questions qui l'aident à réfléchir à la manière de trouver un équilibre entre les violations et les protections de la vie privée.

Cependant, ce processus n'est pas forcément clair pour les employés. Je pense qu'il y a des directives à un haut niveau, mais qu'on ne comprend pas ce qui doit être fait sur le terrain.

Mme Iqra Khalid: Pour être clair, les téléphones personnels des employés ne sont pas touchés par ce dont nous parlons aujourd'hui. Il est question plus précisément des appareils qui appartiennent au gouvernement, n'est-ce pas?

M. Evan Light: Je pense que le Comité a parlé d'un certain nombre d'utilisations possibles. Il y a les utilisations administratives pour l'évaluation interne des téléphones appartenant au gouvernement, et la plupart des organisations que vous avez convoquées ont parlé de l'utilisation sur les appareils des non-employés. Le MPO, le Bureau de la sécurité des transports, l'ASFC et la GRC l'utilisent également pour les non-employés.

Mme Iqra Khalid: Je ne sais pas si c'est ce que je pense des témoignages que nous avons entendus.

Cependant, à ce sujet, la relation entre les mandats et les hypothèses, comme ce qui pourrait être fait ou ce qui est possible par rapport à ce qui est réellement fait... Pensez-vous que la confiance du public est brisée? Il est clair que vous vous méfiez de la manière dont les ministères utilisent ces appareils avec leurs employés. Comment pensez-vous que nous puissions travailler à instaurer une plus grande confiance afin que vous et d'autres ne pensiez pas que ce qui pourrait être fait l'est en réalité?

M. Evan Light: En tant que chercheur, je veux des preuves claires.

Dans le processus de préparation des demandes d'accès à l'information pour ces agences, pour leurs politiques internes, pour leurs registres, il faut ceci: montrez-moi à quelles fins vous utilisez ces appareils, pourquoi vous les utilisez, quelles politiques existent et quelles politiques n'existent pas, quelles lois existent et quelles lois n'existent pas.

Mme Iqra Khalid: Si j'ai bien compris, tout ce qui est fait sur les téléphones des employés est fait soit avec leur consentement, soit par l'entremise de mandats. Pensez-vous que cela n'est pas suffisant pour protéger un employé?

M. Evan Light: Je ne pense pas que le consentement soit suffisant. Je ne pense pas que les gens sachent nécessairement à quoi ils consentent.

Mme Iqra Khalid: Si le consentement n'est pas suffisant, qu'est-ce qui l'est?

M. Evan Light: Nous revenons à mes observations sur les évaluations des facteurs relatifs à la vie privée en tant qu'outils d'autoréglementation. Nous avons besoin d'un organisme externe, comme le CPVP, qui décide si ces appareils doivent être utilisés ou non. Un organisme comme le CPVP pourrait décider du type de processus à mettre en place pour que les gens donnent leur consentement éclairé à l'examen de leurs appareils.

Mme Iqra Khalid: Avez-vous le même point de vue pour les organismes privés en ce qui concerne leurs employés, ou pensez-vous que seuls les ministères publics doivent faire l'objet de ces mesures supplémentaires?

● (1150)

M. Evan Light: Vous voulez dire des sociétés?

Mme Iqra Khalid: Oui.

M. Evan Light: Je serais troublé si les sociétés étaient en mesure d'acheter ces technologies. Le cas échéant, j'aurais les mêmes attentes pour ce qui est du consentement.

Mme Iqra Khalid: Enfin, je voudrais juste passer en revue vos définitions des logiciels espions et des logiciels de criminalistique. Vous avez dit qu'ils étaient fondamentalement identiques, mais ce n'est pas ce que nous avons entendu dans d'autres témoignages. Pouvez-vous clarifier votre position à ce sujet, je vous prie?

M. Evan Light: Leurs capacités sont à peu près les mêmes. Avec les logiciels espions, vous avez des applications qui sont installées subrepticement sur les téléphones des gens afin de les espionner en temps réel. Les appareils mobiles de criminalistique vous permettent d'accéder aux mêmes données détaillées après coup. Ce n'est donc pas du tout la même chose, mais ils offrent essentiellement le même accès à des données auxquelles vous n'auriez pas autrement accès sans devoir obtenir un mandat, dans la mesure où vous auriez besoin d'un mandat pour accéder à chaque connexion à un fournisseur de services infonuagiques.

Mme Iqra Khalid: Vous n'avez pas de preuve que c'est ce qui se fait actuellement dans les ministères.

M. Evan Light: Non, mais j'ai la preuve qu'ils ont acheté la technologie pour le faire. Pourquoi achèterait-on une technologie qui permet d'accéder à ces choses si on n'a pas l'intention de le faire? Il s'agit de technologies distinctes. Les dispositifs mobiles de criminalistique sont constitués de divers logiciels et pièces de matériel. Ils peuvent être achetés à la pièce, et une technologie permettant de le faire a été achetée récemment. Les licences sont actives jusqu'au milieu de l'été 2024.

Le président: Merci, monsieur Light.

Merci, madame Khalid.

[*Français*]

Un bruit semble provenir d'un téléphone. Pourriez-vous mettre vos téléphones en mode silencieux s'il vous plaît?

Monsieur Villemure, vous avez deux minutes et demie.

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

Monsieur Light, ce que vous soulevez est quand même inquiétant. La technologie se développe rapidement. On a vu que certaines organisations se disent qu'autrefois, il suffisait de cacher un micro dans la lampe, mais qu'aujourd'hui, on utilise des outils d'informatique judiciaire. Compte tenu du développement des technologies, l'évaluation des facteurs relatifs à la vie privée est-elle suffisante?

M. Evan Light: Je ne crois pas.

Les témoignages que nous avons entendus jusqu'à maintenant soulèvent tous la même préoccupation, à savoir que l'évaluation des facteurs relatifs à la vie privée aborde le programme, pas la technologie. Comme nous avons pu le voir mardi lors du témoignage des gens du Bureau de la concurrence, on utilise ce genre de technologie depuis 1996, avant l'instauration de la directive du Conseil du Trésor. Dans d'autres organisations, comme à Services partagés Canada, on a des directives relatives à la vie privée qui datent d'avant le recours à de telles technologies. Il est faux de croire que les données sont restées pareilles avec le temps, car les nouvelles technologies permettent d'avoir accès à de plus en plus de données.

M. René Villemure: Pensez-vous que le commissaire à la vie privée lui-même va devoir accroître sa vigilance, compte tenu des développements technologiques?

M. Evan Light: Oui, absolument.

M. René Villemure: D'accord.

Vous faites référence à plusieurs témoignages. Êtes-vous rassuré par les témoignages que vous avez entendus cette semaine? Est-ce que tout va bien aller?

M. Evan Light: Non.

M. René Villemure: Non?

M. Evan Light: Je suis rassuré parce que je connais la situation beaucoup mieux qu'auparavant.

M. René Villemure: Trouvez-vous que, en soi, tout ce qui est autour de la vie privée, ce n'est pas un peu sous-estimer la valeur de la vie privée?

M. Evan Light: Je crois que oui. En raison de notre usage des technologies, des médias sociaux et des nouvelles formes de communication, nous avons de nouvelles normes sociales et en matière de communication, mais nous n'avons pas mis à jour nos lois.

M. René Villemure: La vie privée existe-t-elle encore?

M. Evan Light: Je crois que oui, mais elle est menacée.

M. René Villemure: D'accord, et merci beaucoup.

Le président: Merci, monsieur Villemure.

[*Traduction*]

Nous allons maintenant entendre M. Green pour deux minutes et demie. Nous céderons ensuite la parole à Mme Kusie pour deux minutes et demie, puis à Mme Damoff. La série de questions sera alors terminée.

Monsieur Green.

M. Matthew Green: Je vous remercie.

Je pense que l'un des problèmes auquel nous sommes confrontés est que nous ne participons jamais à ces comités et que nous ne discutons de ces questions qu'après coup. Nous savons qu'en ce qui concerne la technologie de l'appareil utilisée par la GRC, il n'y a pas eu de divulgation proactive. Il a fallu des révélations concernant l'approvisionnement pour que nous le découvrions. Aujourd'hui, nous sommes dans le même bateau.

Pour en revenir à nos conversations précédentes sur la recherche et l'établissement de recommandations clés pour ce comité, compte tenu de votre expérience en matière d'accès à l'information et d'approvisionnement, quels sont les moyens de créer une culture de divulgation proactive afin que les citoyens aient une meilleure compréhension de ce que le gouvernement fait?

● (1155)

M. Evan Light: Si nous revenons au modèle selon lequel le Commissariat à la protection de la vie privée, le CPVP, aurait un rôle à jouer dans l'approvisionnement, nous aurions alors un mécanisme de reddition de comptes. Au lieu que les agences décident elles-mêmes de ce qu'elles font, il y a un obstacle. Il y a une étape que tout le monde doit franchir pour que l'information devienne publique et pour qu'un comité comme celui-ci puisse être invité à examiner une certaine technologie avant qu'elle soit utilisée. À l'heure actuelle, tout cela est fragmentaire.

M. Matthew Green: Oui, c'est très fragmentaire. C'est ce que nous ont dit les ministères. Chacun d'entre eux choisissait sa propre aventure. Certains d'entre eux ont dit qu'ils disposaient de diverses formes d'évaluations des facteurs relatifs à la vie privée. J'ai également constaté que certains d'entre eux n'évaluaient pas l'outil, mais ils évaluaient leurs « programmes ».

Pourquoi pensez-vous qu'il serait problématique d'effectuer une évaluation des facteurs relatifs à la vie privée, ou EFVP, sur un programme plutôt que de s'intéresser à la particularité de l'outil?

M. Evan Light: Les outils évoluent en permanence et leurs capacités changent aussi en permanence. Les programmes sont probablement trop généraux pour tenir compte de l'évolution des capacités des outils.

M. Matthew Green: À votre avis, si l'on considère l'ensemble de ce secteur technologique, peut-on dire que, tant dans le secteur privé que dans le secteur public, il s'agit d'un domaine qui n'est pas complètement réglementé?

M. Evan Light: Tout à fait.

M. Matthew Green: Est-ce qu'on peut dire qu'en raison de la désinformation, de la mésinformation et de la capacité de surveillance subreptice à créer des profils qui forment des algorithmes, tant dans le secteur public que dans le secteur privé, nous devons mettre en place un cadre qui protège la souveraineté des Canadiens en matière de données?

Pouvez-vous nous parler un peu de la souveraineté des données en tant que moyen efficace de protéger nos institutions démocratiques?

M. Evan Light: Je ne pourrais pas dire si la souveraineté des données cadre dans la portée de la conversation ou non. Je pense que...

M. Matthew Green: Je l'ai simplement intégrée dans le cadre de la conversation. Que pensez-vous de la souveraineté des données?

Le président: Nous allons avoir besoin d'un avis très rapide, s'il vous plaît, ou vous pouvez répondre par écrit.

M. Evan Light: Je fournirai une réponse écrite.

Le président: D'accord, c'est la même procédure pour vous, monsieur Light. Soumettez votre opinion d'ici une semaine, à 17 heures, si vous n'y voyez pas d'inconvénient.

Merci, monsieur Green.

[*Français*]

Madame Kusie, vous avez la parole pour deux minutes et demie.

[*Traduction*]

Mme Stephanie Kusie (Calgary Midnapore, PCC): Merci, monsieur le président.

Merci, monsieur Light, d'être ici aujourd'hui.

Étant donné vos préoccupations liées au manque de transparence et de surveillance du gouvernement actuel, êtes-vous inquiet lorsque la présidente du Conseil du Trésor, la personne censée être responsable de l'application de ces évaluations des facteurs relatifs à la vie privée, affirme qu'il incombe à chaque organisation et à chaque ministère de faire respecter cette règle?

M. Evan Light: Oui, c'est un problème, mais je ne pense pas nécessairement que mes inquiétudes s'appliquent seulement au gouvernement actuel.

Cette directive remonte en fait à 2002. Ce fait a été déformé par divers témoins qui ont comparu devant le Comité et qui se fondaient sur la directive de 2018. La directive initiale remonte à 2002. Je crois qu'on n'en tient pas compte depuis 2002.

Mme Stephanie Kusie: Pour faire suite à vos commentaires sur la surveillance et la transparence, nous nous heurtons à ce problème dans le cadre de notre étude au comité des opérations gouvernementales. Pensons par exemple à la personne qui a récemment mené une enquête interne, le directeur général de l'intégrité professionnelle, qui relève de la présidente de l'ASFC.

Nous avons récemment été témoins de deux atteintes à la protection des données au sein du gouvernement. Le 18 novembre 2023, CTV a rapporté que les renseignements personnels et financiers de la GRC et des Forces armées canadiennes avaient été compromis, cette atteinte remontant à 1999. Deuxièmement, il y a quelques jours à peine, le 12 février, on a appris qu'un sous-traitant de Canada Vie avait également été victime d'une atteinte à ses renseignements. Ces deux exemples très précis touchent à la fois les fonctionnaires et les organismes gouvernementaux.

Diriez-vous que l'environnement infonuagique et les outils que vous avez mentionnés sont susceptibles de donner lieu à un plus grand nombre d'atteintes de ce genre?

M. Evan Light: Oui, tout à fait. Par exemple, si l'information gouvernementale est dans le nuage et que les utilisateurs y accèdent par le nuage sur un appareil, ce pourrait être une possibilité.

Mme Stephanie Kusie: Excellent.

Vous avez dit récemment que le Canada est entré dans une ère de « normalisation » de la surveillance. Pouvez-vous nous en dire plus à ce sujet, s'il vous plaît?

M. Evan Light: Bien sûr. Je ne pense pas que nous soyons entrés dans cette ère; je pense que nous y sommes depuis très longtemps. Par exemple, dans le cadre de mon travail sur notre utilisation des ondes radioélectriques pour faire de la surveillance au Canada, j'ai appris que le SCRS a reçu dès 1991, du ministère des Communications, à l'époque, le pouvoir d'utiliser les ondes pour la surveillance au niveau national.

Je pense que la surveillance sera toujours une réalité à l'intérieur et à l'extérieur du gouvernement. Je ne dirais pas que la surveillance soit nécessairement devenue la norme. Je pense que c'est [*inaudible*] qu'on l'utilise. Je pense que le manque de réglementation et de transparence à cet égard est devenu la norme.

● (1200)

Mme Stephanie Kusie: Merci.

Merci, monsieur le président.

Le président: Merci, madame Kusie et monsieur Light.

Madame Damoff, vous avez la parole pendant deux minutes et demie.

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

Merci à notre témoin d'être ici aujourd'hui.

Je voulais aborder l'utilisation des téléphones professionnels. J'en ai déjà parlé. En 1996, avant même que nous ayons des téléphones cellulaires, je travaillais pour Midland Walwyn. J'ai dû signer un document stipulant que mon ordinateur de travail ne devait être utilisé qu'à des fins professionnelles.

Au sujet du consentement, je pense que les employés devraient bien comprendre que le téléphone de travail qu'on leur fournit ne doit être utilisé qu'à des fins professionnelles. Adhérez-vous à cette affirmation?

M. Evan Light: Oui, mais j'apporterais la nuance que le perfectionnement de la technologie amène la sphère privée et la sphère professionnelle à vraiment s'immiscer l'une dans l'autre.

Mme Pam Damoff: Je ne dis pas que les employés n'utilisent pas leurs téléphones pour des raisons personnelles, mais l'employeur s'attend, au gouvernement ou dans les banques d'investissement, à ce que l'outil fourni aide les employés dans leur travail, et non pas à ce qu'il soit utilisé en dehors du travail.

J'aimerais vous faire part d'une partie du témoignage que nous avons entendu précédemment de la part de Services partagés Canada. Le témoin a dit: « [B]ien 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. »

Il a ajouté:

> 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.

Nous avons entendu un témoignage semblable de l'ASFC, dans les situations où il n'y a qu'un mandat. Les procédures ne s'enclenchent pas lorsqu'on vous prend votre téléphone au cours d'un deuxième contrôle, mais seulement lorsqu'il y a un mandat.

Puis, la GRC a dit: « [L]es informations diffusées dans les médias selon lesquelles ces outils de criminalistique numérique sont assimilables à des logiciels espions sont inexactes, et je vous fournirai des éclaircissements à ce sujet. » Il a ajouté: « Ces outils sont utilisés sur des appareils numériques saisis légalement dans le cadre d'enquêtes criminelles. »

Je suppose que ma question est la suivante: pensez-vous que ces témoins disent la vérité lorsqu'ils formulent ces propos en comité?

M. Evan Light: Je crois qu'ils disent la vérité, mais je pense que la loi et les politiques n'ont pas évolué au même rythme que les capacités et le potentiel de ces appareils.

Mme Pam Damoff: D'accord. Je comprends.

M. Evan Light: Je ne crois pas que les employés comprennent cette réalité.

Mme Pam Damoff: Eh bien, je pense que les employés doivent assumer une certaine responsabilité lorsqu'ils exécutent une tâche pour leur travail. Je pense également que si un employé est visé par une allégation de harcèlement ou d'acte répréhensible, quel que soit le lieu de travail, l'employeur devrait pouvoir utiliser les outils juridiques appropriés, y compris les téléphones, pour lancer une enquête.

Mon temps est écoulé, monsieur le président. Merci.

Le président: Merci, madame Damoff.

Monsieur Light, je tiens à vous remercier de votre témoignage devant le Comité aujourd'hui.

Nous devons nous préparer pour le prochain groupe de témoins, alors nous allons suspendre la séance pendant quelques minutes. Nous reprendrons sous peu.

Merci.

● (1200)

_____(Pause)_____

● (1210)

Le président: Bienvenue à la deuxième heure de notre séance. Nous avons eu besoin d'un peu plus de deux minutes, mais reprenons.

Je souhaite la bienvenue à nos témoins pour la deuxième heure de notre séance d'aujourd'hui. Nous accueillons des représentants de l'Association canadienne des employés professionnels: le président, Nathan Prier, et la conseillère principale pour la Défense de l'intérêt public et les campagnes, Laura Shantz. Nous recevons aussi Jennifer Carr, de l'Institut professionnel de la fonction publique du Canada.

Je vous souhaite la bienvenue à tous les trois et je vous remercie d'être parmi nous aujourd'hui. Vous avez un maximum de cinq minutes pour vos déclarations liminaires.

Nous allons commencer par l'Association canadienne des employés professionnels. Allez-y, monsieur.

M. Nathan Prier (président, Association canadienne des employés professionnels): Bonjour et merci de me donner l'occasion de comparaître devant le Comité aujourd'hui.

Je m'appelle Nathan Prier. Je suis le président de l'Association canadienne des employés professionnels, ou ACEP, qui représente plus de 25 000 fonctionnaires des services économiques, des services des sciences sociales et des groupes de traduction, ainsi que des employés de la Bibliothèque du Parlement, du Bureau du directeur parlementaire du budget et des membres civils de la GRC.

Nous sommes choqués et consternés d'apprendre que des logiciels espions ont été utilisés dans de nombreux ministères fédéraux sur des appareils fédéraux utilisés par des travailleurs de la fonction publique, sans même suivre les politiques du gouvernement. L'utilisation de ces logiciels espions a été mise au jour, comme nous venons de l'entendre, grâce à une demande d'accès à l'information présentée par M. Light. Les fonctionnaires ont appris la violation potentielle de leurs droits dans les médias plutôt que par le biais d'évaluations obligatoires des facteurs relatifs à la vie privée ou d'une divulgation proactive par l'employeur.

Ce genre de comportement secret mine la confiance entre les travailleurs du secteur public et leur employeur. M. Light a décrit l'utilisation de ces logiciels espions comme étant « exagérée » et « ridicule, mais aussi dangereuse, » et nous venons d'entendre quelques exemples des raisons expliquant pourquoi il est de cet avis. À notre avis, l'utilisation de tels logiciels est assez répressive et brise la confiance de nos membres.

La Directive du gouvernement sur l'évaluation des facteurs relatifs à la vie privée est en place pour veiller à ce que toute collecte de données se fasse par les méthodes les moins intrusives possible. De plus, le commissaire à la protection de la vie privée du gouvernement a indiqué que des évaluations sont nécessaires chaque fois que des outils portant atteinte à la vie privée sont utilisés, même lorsqu'une autorisation judiciaire permet le recours à une mesure donnée. Les 13 ministères en question n'ont pas effectué d'évaluation des facteurs relatifs à la vie privée avant d'utiliser ces logiciels espions, malgré leurs propres politiques exigeant une telle évaluation. Selon nous, c'est tout à fait inacceptable.

[*Français*]

Les employés du secteur public fédéral doivent jouir des mêmes droits à la vie privée et à un traitement équitable que les autres Canadiens et Canadiennes. Leur employeur doit renforcer leur confiance, afin qu'ils puissent fournir des services de qualité aux Canadiens. Afin de rétablir cette confiance et de garantir que les employés du secteur public fédéral conservent leur droit à la vie privée et à un traitement équitable, nous demandons au gouvernement fédéral de mettre en œuvre un plan visant à mettre à jour et à respecter, de manière cohérente, son cadre de politique numérique.

● (1215)

[*Traduction*]

L'ACEP, mon syndicat, est ici pour présenter trois demandes précises.

Premièrement, nous demandons au gouvernement de mettre fin à l'utilisation de logiciels espions sur les appareils fédéraux allant à l'encontre de ses propres règles et d'utiliser les mesures les moins invasives qui soient. Tous les fonctionnaires ont droit à l'application régulière de la loi pendant les enquêtes.

Deuxièmement, nous voulons savoir quand le gouvernement prévoit d'effectuer des évaluations des facteurs relatifs à la vie privée dans tous les ministères touchés et de rendre publics les résultats de ces évaluations afin d'aider les fonctionnaires à rétablir la confiance envers leur employeur après ces violations. L'utilisation de logiciels espions entraîne une érosion du droit à la vie privée qu'aucun fonctionnaire ne devrait accepter au premier abord.

Enfin, nous demandons au gouvernement de procéder à un examen approfondi de toutes ses politiques numériques afin de s'assurer que le cadre stratégique actuel est suffisamment robuste pour protéger les droits numériques des employés, y compris leur droit à une protection raisonnable de leur vie privée, leur droit d'être informés de tout outil de surveillance numérique utilisé en milieu de travail et leur droit de se déconnecter du travail après les heures travaillées.

Les membres de l'ACEP fournissent des conseils stratégiques judicieux au gouvernement et ils ne peuvent faire leur meilleur travail que lorsque l'employeur démontre sa volonté d'être ouvert, transparent et respectueux de la fonction publique.

Le président: Merci, monsieur Prier.

Madame Carr, vous avez cinq minutes. Veuillez débuter.

Mme Jennifer Carr (présidente, L'Institut professionnel de la fonction publique du Canada): Merci, monsieur le président.

Je vous remercie de m'avoir invitée à m'adresser à vous aujourd'hui.

Je m'appelle Jennifer Carr, et je suis la fière présidente de l'Institut professionnel de la fonction publique du Canada. Nous représentons 75 000 fonctionnaires fédéraux et certains fonctionnaires provinciaux. Nous représentons également des travailleurs des technologies de l'information, ou TI.

D'entrée de jeu, je veux exprimer très clairement notre position. Le droit à la vie privée des employés doit être protégé. Les employés du gouvernement, nos membres, sont des citoyens canadiens comme vous et moi. Nous avons tous le droit de savoir quand nos renseignements sont consultés, quels renseignements sont recueillis, comment ils seront utilisés, qui les détient et qui y aura accès, et comment ils sont stockés et protégés. J'espère que nous pouvons tous convenir que le gouvernement fédéral, qui est l'un des plus grands employeurs, devrait donner l'exemple à tous les autres employeurs et être tenu de respecter les normes les plus élevées.

Malheureusement, comme vous l'avez entendu, il semble que de nombreux ministères et organismes gouvernementaux n'ont pas atteint cette norme. Ils n'ont pas respecté les politiques et règles du gouvernement. Il semblerait qu'ils ont fait fi de la directive du Conseil du Trésor exigeant que des évaluations des facteurs relatifs à la vie privée soient effectuées avant d'utiliser ce genre d'outils.

Il est question de ministères et d'organismes fédéraux qui pourraient utiliser ces outils pour avoir accès à des messages textes, à des courriels, à des photos et à des antécédents de voyages; pour accéder à des données infonuagiques et révéler des antécédents de recherche sur Internet, du contenu supprimé et des activités dans les médias sociaux; et possiblement pour récupérer des renseignements chiffrés ou protégés par un mot de passe.

Pensez à tous les renseignements qui se trouvent actuellement sur votre téléphone, vos tablettes, votre montre ou votre ordinateur: des données sur la santé, des renseignements financiers, des messages supprimés de vos amis et de votre famille, ou des données infonuagiques comme vos photos de famille stockées sur Dropbox, Google ou OneDrive. Il est absurde d'avancer que l'utilisation d'un téléphone ou d'un ordinateur fourni par l'employeur signifie de renoncer à tous les droits à la vie privée.

Nous sommes profondément préoccupés d'apprendre que certains employeurs, comme Pêches et Océans Canada, ont prétendu que l'utilisation de ces outils était justifiée parce que les données appartiennent au ministère.

Même si l'appareil appartient à l'employeur, ce dernier ne possède pas les données personnelles qui s'y trouvent pour autant. Le commissaire à la protection de la vie privée et les juristes ont été on ne peut plus clairs à ce sujet. Le commissaire a également précisé que, même lorsqu'une autorisation légale est accordée, les ministères ne sont pas exemptés de faire l'évaluation des facteurs relatifs à la vie privée. Ces évaluations sont essentielles pour cerner les risques en matière de protection de la vie privée et déterminer comment ils peuvent être atténués ou éliminés.

Le commissaire à la protection de la vie privée devrait indiquer sans équivoque que son bureau doit être consulté avant que ces outils ne soient utilisés, et qu'il ne doit pas entendre parler de leur utilisation dans les médias après coup.

Nous avons également besoin de transparence quant à la fréquence à laquelle les évaluations doivent être menées et aux facteurs qui devraient déclencher une nouvelle évaluation. La technologie évolue plus rapidement que jamais. Par conséquent, nos lois, nos règlements et nos pratiques en matière de protection de la vie privée doivent évoluer tout aussi rapidement.

De plus, les ministères et organismes gouvernementaux devraient être tenus de consulter le commissaire à la protection de la vie privée avant d'adopter de nouvelles règles en matière de protection de la vie privée, surtout lorsqu'elles concernent l'utilisation d'outils logiciels intrusifs. À défaut de cela, les députés devraient modifier la Loi sur la protection des renseignements personnels pour en faire une exigence en vertu de la loi.

Les employés que nous représentons sont aussi préoccupés par les témoignages que vous avez entendus de la part de certains de leurs ministères. Les représentants de Santé Canada ont d'abord dit que le ministère avait acheté ces outils, mais qu'il ne les avait jamais utilisés, avant d'admettre qu'il les avait utilisés, mais sans dire à quelles fins. Des représentants du ministère de la Défense ont témoigné ne pas vraiment savoir si les évaluations des facteurs relatifs à la vie privée avaient été effectuées ou non. Les représentants de la GRC vous ont dit qu'ils utilisaient les outils, mais qu'ils ne feraient l'évaluation des facteurs que plus tard cette année.

En tant que syndicat représentant des dizaines de milliers d'employés fédéraux, ces messages contradictoires accentuent nos préoccupations au sujet de la surveillance électronique dans nos milieux de travail.

En terminant, je tiens à remercier les membres du Comité d'avoir lancé cette étude. Nos membres vous sont reconnaissants d'avoir décidé de vous pencher sur cette question. Nous vous exhortons à formuler des recommandations fermes et claires sur la façon de mieux protéger les données personnelles des employés du gouvernement. Ces recommandations devraient comprendre ce qui suit.

Les ministères et organismes gouvernementaux devraient être tenus par la loi d'effectuer des évaluations des facteurs relatifs à la vie privée avant d'utiliser l'un ou l'autre de ces outils, que des autorisations légales aient été données ou non, comme l'a recommandé le commissaire à la protection de la vie privée. De plus, des méthodes moins intrusives devraient être utilisées pour recueillir des renseignements, comme l'exige la Directive sur l'évaluation des facteurs relatifs à la vie privée.

● (1220)

En cas de non-respect des directives du Conseil du Trésor, il devrait y avoir des répercussions et des mesures claires pour veiller à ce que les ministères et organismes gouvernementaux s'y conforment davantage à l'avenir.

Deuxièmement, il faut fournir des lignes directrices plus claires sur les programmes nouveaux ou modifiés qui nécessiteront de nouvelles évaluations des facteurs relatifs à la vie privée et mettre à jour les lignes directrices actuelles. La technologie évolue rapidement, et nos pratiques doivent refléter cette réalité.

Enfin, le gouvernement doit reconnaître qu'il ne détient pas les données personnelles se trouvant sur les appareils utilisés par les employés. À mesure que les outils sur lesquels le Comité se penche dans le cadre de cette étude deviennent plus puissants et intrusifs, les mesures de protection de la vie privée doivent elles aussi être renforcées.

Nous exhortons tous les députés à s'unir pour veiller à ce que le gouvernement maintienne les normes les plus élevées en matière de protection de la vie privée des employés. Faisons de notre gouvernement un modèle d'employeur partout au pays sur le plan de la protection des renseignements personnels en milieu de travail.

Merci.

Le président: Merci.

Je tiens à vous remercier tous les deux de vos remarques liminaires, et surtout, d'avoir proposé des solutions. Nous ne recevons pas souvent ce type de solutions et de recommandations de la part de témoins au Comité, alors je vous en remercie.

Nous commençons le premier tour. Vous disposez de six minutes, monsieur Kurek. Allez-y, je vous prie.

M. Damien Kurek: Merci beaucoup.

Je remercie les témoins d'être des nôtres.

J'aimerais devancer ce qui semble être l'argument du gouvernement dans certains cas. Ma question est précise et je veux vous donner l'occasion d'y répondre. Le gouvernement a dit: « Oh! Ne vous inquiétez pas, ce n'est pas un logiciel espion. » Cette affirmation est troublante, puisqu'il s'agit d'outils incroyablement puissants qui donnent accès à des renseignements personnels.

Ma première question s'adressera à M. Prier et ma deuxième à Mme Carr. Tout d'abord, il est question d'un appareil gouvernemental. Les utilisateurs n'ont donc pratiquement aucun droit. Je paraphrase les questions qu'a posées une secrétaire parlementaire au cours de la dernière heure. Je sais que vous étiez présents. J'aimerais donc vous demander votre avis à ce sujet. Pourriez-vous également nous expliquer votre caractérisation de ces éléments dans vos remarques liminaires? J'aimerais ensuite vous poser quelques autres questions.

Je commence par vous, monsieur Prier.

M. Nathan Prier: Nous pourrions débattre de la définition d'un logiciel espion. Cela dit, cette technologie porte atteinte au droit à la vie privée de nos membres, peu importe si elle en est un ou non. Voilà la ligne qui a été franchie.

Les lignes directrices du Conseil du Trésor stipulent qu'il aurait fallu divulguer de façon proactive l'utilisation de cette technologie, mais cela ne s'est pas fait. Nous l'avons appris après coup.

Le fait que ce sont des appareils gouvernementaux signifie-t-il la suspension du droit à la vie privée de tous nos membres? Le gouvernement fédéral est l'un des plus gros employeurs au pays. Il doit placer la barre haut et donner l'exemple. Il devrait montrer aux employeurs comment se comporter à l'égard de tous les citoyens canadiens et de leur droit à la vie privée. Nous avons l'impression que, dans ce cas comme dans beaucoup d'autres, nous apprenons peu à peu que la politique de base n'a pas été respectée.

Le commissaire à la protection de la vie privée a été très clair: il convient de mener une évaluation des facteurs relatifs à la vie privée pour tout nouvel outil présentant des risques pour la vie privée et d'en divulguer l'utilisation de façon proactive. J'estime qu'il existe des moyens très simples de communiquer de façon proactive l'utilisation de ces technologies dans un langage clair afin que les fonctionnaires sur le lieu de travail — nos membres — puissent être nettement plus en mesure de respecter les normes de base en matière de partage sur un appareil gouvernemental et être conscients de leur droit à la vie privée et des violations potentielles de ce droit afin que la discussion puisse avoir lieu avant que ces technologies ne soient installées.

● (1225)

M. Damien Kurek: Je déteste vous interrompre, mais comme vous le savez, le temps est limité.

Vous avez peut-être entendu mon conseil pas si subtil aux dirigeants des ministères. Je leur ai conseillé de décrocher le téléphone et d'appeler le commissaire à la protection de la vie privée. C'est ce qu'ils devraient faire pour commencer à rétablir la confiance des Canadiens et de ceux qui travaillent fort dans notre fonction publique.

Je vous écoute, madame Carr.

Mme Jennifer Carr: Je serai brève.

Vous ne savez peut-être pas qu'il existe déjà une politique sur l'utilisation des appareils numériques. Elle stipule que vous pouvez utiliser les appareils du gouvernement à des fins personnelles si cela n'interfère pas avec votre travail et si vous le faites pendant votre temps libre. Je ne suis pas certaine que quelqu'un d'autre l'ait déjà souligné.

Il existe de nombreuses politiques au sein du gouvernement. Ce qui nous pose problème, c'est leur décentralisation. Au lieu de les centraliser par l'entremise du Conseil du Trésor pour en assurer un suivi, on les a réparties dans divers ministères qui sont chargés de les appliquer.

M. Damien Kurek: Merci. Je pense que c'est important de le souligner, surtout parce que les cellulaires et les appareils mobiles sont devenus des outils de communication très puissants. Ils ne servent plus qu'à faire des appels ou envoyer des courriels. Ils nous permettent de faire bien plus que cela.

J'aimerais connaître votre avis sur une chose. Je suis curieux de savoir si vous pourriez nous donner des exemples de cas où ces outils d'investigation ont été utilisés pour trouver des lanceurs d'alerte ou des personnes qui ont été ciblées en raison de leurs actions au sein d'un ministère en particulier. J'insiste particulièrement sur les recherches pour trouver un lanceur d'alerte. Auriez-vous des exemples à nous donner à cet égard? J'aimerais également avoir votre avis sur la façon dont cela pourrait empiéter sur la capacité d'un travailleur à dénoncer ce qui pourrait être une inconduite au sein d'un ministère, d'une agence, etc.

Mme Jennifer Carr: Certains témoignages m'ont inquiétée. J'ai entendu des témoins dire qu'ils ont le logiciel, mais qu'ils ne l'utilisent pas; qu'ils l'envoient plutôt à un autre ministère. Si la technologie existe et que nous ignorons comment elle est utilisée, et s'ils n'ont en plus pas à divulguer quand et comment elle est utilisée, c'est très inquiétant.

Je ne peux pas vous donner d'exemple précis, mais il est très inquiétant que des gens disposent de cette technologie sans avoir à préciser quand il est nécessaire de l'utiliser ou à obtenir l'approbation d'un directeur ou d'un directeur général. Si personne ne surveille l'utilisation de cette technologie, elle peut être utilisée à notre insu.

M. Damien Kurek: Souhaitez-vous ajouter quelque chose, monsieur Prier? Il reste environ une minute.

M. Nathan Prier: Non, je voulais simplement dire que je suis d'accord avec Mme Carr. De plus, l'employeur a tendance à être nettement plus réactif que proactif en matière de politique numérique et de protection de la vie privée. De nombreuses politiques du Conseil du Trésor ont désespérément besoin d'être mises à jour pour être adaptées au contexte numérique et devront probablement continuer à l'être régulièrement.

Je pense que le cadre politique dont nous disposons est suffisamment solide; il faudrait simplement le suivre de plus près.

M. Damien Kurek: Merci. La proactivité par rapport à la réactivité... Je pense que c'est le message que devraient retenir les ministères.

En ce qui concerne l'utilisation de ces outils et le consentement des employés, le premier groupe de témoins nous a parlé du déséquilibre des pouvoirs.

Pourriez-vous nous le contextualiser brièvement?

Mme Jennifer Carr: C'est une excellente question.

Compte tenu de la date à laquelle ces politiques ont été mises en place... Bon, qu'est-ce que le consentement? Lors de la mise en place de la politique originale, je ne crois pas que... Lorsqu'il ne s'agissait que de votre cellulaire, la technologie permettait d'avoir accès à la liste de personnes que vous aviez appelées et à la durée de chaque appel. Ils n'ont pas élaboré la politique en fonction des activités infonuagiques. Ces outils vous permettent d'accéder aux informations sur le nuage. Ils vous donnent accès à des données chiffrées, protégées par mot de passe, etc. Ils ont accès à tout votre historique.

Cela n'a pas été envisagé à l'époque. Nous devons donc mettre nos politiques à jour. Cet outil peut potentiellement être utilisé pour trouver n'importe quoi. J'espère que vous conviendrez donc qu'il est absurde de penser qu'ils [*inaudible*] la vie privée.

Le président: Merci, madame Carr.

Nous avons un peu dépassé le temps. Je tente de respecter le temps qui est accordé à chacun.

Vous disposez de six minutes, monsieur Bains. Allez-y, je vous prie.

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

Je remercie les témoins d'être des nôtres aujourd'hui. Je vous remercie de nous avoir fait part de vos recommandations. Une partie du travail de notre comité consiste à en formuler. Je vous remercie tous deux de nous en avoir fait part.

Le commissaire à la protection de la vie privée s'est exprimé à propos de l'utilisation du terme « logiciel espion ». Il a déclaré ce qui suit pendant son témoignage au Comité: « [dans] les premiers reportages, ces outils étaient qualifiés d'outils de surveillance secrète ou de “logiciels espions”. Depuis, il a été précisé qu'il ne s'agit pas de logiciels espions, mais plutôt d'outils d'investigation informatique. » Il a également déclaré que « [les] outils d'investigation informatique se distinguent des logiciels espions par le fait que ces derniers sont généralement installés à distance sur l'appareil d'une personne à l'insu de celle-ci ».

Nous avons entendu dire que ces appareils sont utilisés dans le cadre de la réglementation, par l'entremise d'un mandat et au su des employés. Plusieurs agences nous ont répondu que... Je crois que je leur ai demandé s'il était possible d'accéder à distance à des renseignements d'employés avec ces outils et elles ont répondu non. Elles ont dit qu'il fallait obtenir un mandat et se procurer l'appareil physiquement et s'y connecter pour extraire les renseignements dont nous avons parlé.

Qu'en pensez-vous, madame Carr?

● (1230)

Mme Jennifer Carr: Nous avons entendu cela, mais ce n'est pas clair. Chaque ministère vous a donné une version différente de l'utilisation qu'il en fait. S'il est vrai que l'on confie son appareil à un tiers, pourquoi les ministères achètent-ils et se procurent-ils ce logiciel à l'interne? Leur témoignage a soulevé quelques inquiétudes chez moi. Ils ont dit qu'il est impossible d'extraire des données à distance, mais cela me préoccupe.

Il y a également la question de ce qu'ils extraient. Peuvent-ils tout extraire? Ces agences disposent-elles d'un mandat exhaustif ou recueillent-elles seulement certains renseignements?

M. Parm Bains: Nous avons entendu plusieurs agences qui mènent des enquêtes. Nombre d'entre elles doivent fournir des preuves de conformité aux ministères dont elles relèvent. Elles s'en tiennent à l'enquête et c'est ce sur quoi porte le mandat. Elles ne peuvent obtenir que des renseignements liés à leur enquête. C'est ce que nous avons entendu.

Avise-t-on les employés qui utilisent ces appareils qu'ils sont destinés à un usage professionnel et non à un usage personnel? Nous avons deux appareils, de notre côté.

Mme Jennifer Carr: J'ai fait référence à une politique. Je vous en trouverai le nom. Cette politique stipule que les appareils professionnels peuvent être utilisés à des fins personnelles si cela n'interfère pas avec le travail et si c'est fait en dehors des heures de travail. Il est faux de dire qu'il s'agit uniquement de l'appareil de l'employeur. Certains ministères encouragent — et ce, depuis longtemps — l'utilisation des appareils professionnels à des fins personnelles.

M. Parm Bains: Avise-t-on les employés que les renseignements contenus dans leur appareil professionnel peuvent être consultés?

Mme Jennifer Carr: Je ne crois pas, non.

J'ai parlé de décentralisation. Chaque ministère chargé de distribuer ces appareils est responsable de ces divulgations, et cela ne se fait pas de façon cohésive à un plus haut niveau.

M. Parm Bains: Serait-il utile d'en avoir une à ce niveau?

Mme Jennifer Carr: Il serait utile qu'ils divulguent ces informations. Si c'est possible de le faire en vertu d'une politique, il faudrait vraiment être précis et spécifier quel type de renseignement pourrait être recueilli sur un téléphone lors d'une enquête.

M. Parm Bains: Je pense que vous nous avez dit que vous croyiez en un juste équilibre entre la sécurité et la protection de la vie privée. Vous avez dit qu'il serait nécessaire d'instaurer une mesure à cet effet. Nous avons également entendu que les ministères utilisent ce logiciel pour des enquêtes internes. Ils ont notamment fait référence à des allégations d'actes répréhensibles commis par des employés et des cas de harcèlement sexuel. Pensez-vous qu'il soit justifié de l'utiliser dans de tels cas?

Mme Jennifer Carr: Oui, je pense qu'il faut pouvoir utiliser des outils lors d'une enquête, mais il faut aussi que l'employé sache très clairement à quoi les enquêteurs auront accès. Je ne pense pas que les politiques actuelles soient claires à ce sujet. Je ne pense pas que les employés savent que les enquêteurs peuvent aller dans leur historique et le supprimer, le chiffrer ou autre. Je pense donc qu'il faudrait plus de divulgation, une plus grande transparence et une meilleure reddition de comptes des deux côtés. Je crois que cela serait bénéfique pour toutes les parties.

M. Parm Bains: Quel est le pourcentage de fonctionnaires qui reçoivent des appareils fournis par le gouvernement?

Mme Jennifer Carr: Je ne saurais vous le dire. Vous devriez probablement plutôt poser la question aux ministères. Il n'existe pas de politique cohérente concernant ceux qui peuvent y avoir accès. Ces appareils sont fournis au cas par cas.

● (1235)

M. Parm Bains: A-t-on fixé un niveau de confidentialité pour les appareils émis par le gouvernement?

Mme Jennifer Carr: Je ne crois pas, non.

M. Parm Bains: Je vous remercie de votre temps.

Le président: Merci, monsieur Bains.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

M. René Villemure: Merci, monsieur le président.

J'aimerais profiter de l'occasion pour déposer un avis de motion.

Le président: D'accord.

M. René Villemure: a motion se lit ainsi:

> Que, conformément à l'article 108(3)h), le Comité entreprenne une étude sur l'éthique et la conformité aux règles de déontologie dans le cadre de l'attribution de contrats conclus par le gouvernement et les entreprises GCStrategies et Coredal systems consulting inc, ce, en regard des obligations déontologiques qui découlent du Code de valeur et d'éthique du secteur public;
>
> Que le Comité alloue un minimum de quatre rencontres à cette étude;
>
> Que le Comité invite à témoigner:
>
> > a) Conjointement, pour deux heures, Anita Anand présidente du Conseil du Trésor et Jean-Yves Duclos ministre des Services publics et de l'approvisionnement Canada ainsi que des fonctionnaires;
> >
> > b) Pour deux heures, la Présidente de l'Agence des services frontaliers du Canada, Erin O'Gorman ainsi que des fonctionnaires;
> >
> > c) Et tous autres témoins que le Comité jugera nécessaires.
>
> Que le comité fasse rapport de ses observations et recommandations à Chambre.

La motion a été transmise à la greffière dans les deux langues officielles.

Le président: Merci de cet avis de motion, monsieur Villemure. Si je comprends bien, le texte a été transmis aux membres du Comité.

Vous avez la parole pour quatre minutes quarante-cinq secondes.

M. René Villemure: Monsieur Prier, est-ce que vous étiez surpris quand vous avez entendu parler de ces pratiques?

M. Nathan Prier: Nous étions surpris que les politiques établies n'aient pas été suivies. Nous étions surpris que les valeurs qui étaient intégrées dans ces politiques aient été complètement mises de côté.

M. René Villemure: D'accord.

M. Nathan Prier: Par contre, nous n'étions pas surpris que notre employeur ait installé de telles technologies sans en discuter.

M. René Villemure: D'accord.

Madame Carr, étiez-vous surprise?

[*Traduction*]

Mme Jennifer Carr: Je n'ai pas été surprise. Je suis déçue, mais pas surprise. La décentralisation de la fonction publique fédérale est à l'origine de la plupart des violations que nous constatons. Les ministères ne surveillent à peu près pas certaines de ces politiques. Nous avons besoin de meilleures mesures de surveillance.

[*Français*]

M. René Villemure: Avez-vous été rassurée par les réponses des gens qui sont venus témoigner jusqu'à maintenant?

[*Traduction*]

Mme Jennifer Carr: Pas du tout.

[*Français*]

M. René Villemure: Que répondez-vous, monsieur Prier?

[*Traduction*]

M. Nathan Prier: Non, et nous nous attendons à beaucoup plus à l'avenir.

[*Français*]

M. René Villemure: D'accord.

Les gens qui sont venus témoigner nous ont dit qu'ils utilisaient ces outils, que ça faisait longtemps qu'ils les avaient et qu'ils allaient faire une évaluation des facteurs relatifs à la vie privée. Je pense que nous avons été surpris de les entendre dire qu'ils allaient faire cette évaluation. Nous verrons bien si ce sera fait.

Croyez-vous que c'est une façon de banaliser la situation, que c'est de la négligence de leur part? Est-ce un problème de culture au sein de l'organisation, selon vous?

[*Traduction*]

M. Nathan Prier: Je crois qu'il s'agit d'un problème pangouvernemental. Je pense que le Conseil du Trésor devrait donner des lignes directrices fermes pour expliquer comment les politiques en matière de protection de la vie privée seront appliquées.

Cela dit, toute nouvelle technologie déployée qui aura un impact sur la vie privée de nos membres doit faire l'objet d'une EFVP. Son utilisation devrait également être divulguée de façon proactive. La consigne et le commissaire à la protection de la vie privée ont clairement indiqué ce qui doit être fait à cet égard.

Qu'il soit installé à distance ou...

[*Français*]

M. René Villemure: Cependant, il y avait déjà des directives.

[*Traduction*]

M. Nathan Prier: En effet.

[*Français*]

M. René Villemure: Les directives n'ont pas été suivies. Je ne sais pas ce qui va se passer.

Madame Carr, selon vous, est-ce un problème de culture et d'organisation?

[*Traduction*]

Mme Jennifer Carr: Absolument.

Si les ministères peuvent décider quoi faire sans qu'il y ait de surveillance, ils ne font rien.

En ce qui concerne l'EFVP, j'ai entendu dire: « Ils ont dit que nous en avions fait une il y a longtemps. » Nous devons faire une mise à jour et commencer à utiliser les nouvelles versions et les nouvelles technologies au fur et à mesure qu'elles sortent. J'ai comparé cela au fait d'être toujours abonné à Napster alors que tout le monde est maintenant sur Spotify ou Apple Music.

Nous ne pouvons pas nous contenter d'une évaluation qui a été faite sur une technologie très ancienne.

[*Français*]

M. René Villemure: C'est une bonne comparaison.

Il y a déjà des politiques en place, et ces politiques font partie de la structure des organisations. Il me semble donc que le problème ne vient pas de la structure, puisqu'il y avait des directives et des politiques, mais du fait que celles-ci n'ont pas été suivies.

Devrait-on appliquer plus de directives et de politiques ou, au contraire, devrait-on travailler sur la culture qui est en place? J'écoute les témoins et je me dis que l'exemple doit venir d'en haut. Toutefois, ce n'est pas le cas. Qu'est-ce qu'on doit faire, par conséquent?

[*Traduction*]

Mme Jennifer Carr: Parlons de répercussions. Treize ministères ont dit avoir eu des manquements à cet égard. Ils ont dit: « Oups, désolé. » Sauf qu'il n'y a pas eu de répercussions.

Il en faudra. Il va falloir que vous retiriez l'autorité aux sous-ministres et que vous alliez au fond des choses. Il vous faudra leur expliquer que vous allez leur révoquer leur autorité puisqu'ils n'ont pas suivi les politiques.

● (1240)

[*Français*]

M. René Villemure: Croyez-vous qu'avec ces pratiques, on va pouvoir restaurer la confiance de vos 75 000 membres?

[*Traduction*]

Mme Jennifer Carr: S'il y a des répercussions pour ceux qui ne suivent pas les politiques et les lignes directrices, oui, absolument.

Nous sommes tout à fait capables de veiller à ce que les fonctionnaires respectent les politiques. Pourquoi ne pas exercer le même type de surveillance auprès des sous-ministres?

[*Français*]

M. René Villemure: D'accord.

Monsieur Prier, je vais vous poser la même question: pour restaurer la confiance, croyez-vous que ces situations pourraient aider?

[*Traduction*]

M. Nathan Prier: Je suis tout à fait d'accord avec Mme Carr sur ce point.

Il faut prendre au sérieux les mesures de conformité et les conséquences graves des violations de la vie privée. Les prochaines étapes à franchir se situent entièrement au niveau de la haute direction qui doit être sanctionnée pour avoir permis ces violations.

Nous parlons d'un changement de culture. La culture est une chose très vague à changer. Je pense que nous avons besoin de conséquences graves pour les violations à la vie privée et que nous devons énoncer clairement ce qui arrivera lors de chaque violation.

[*Français*]

M. René Villemure: Dans les attentes signifiées aux sous-ministres, croyez-vous qu'on pourrait inclure une composante relative à la vie privée?

[*Traduction*]

Mme Jennifer Carr: Je répète que tous les fonctionnaires sont des citoyens canadiens, tout comme vous. Je crois qu'il faut tracer une ligne claire en matière de vie privée. Il faut s'attendre à une certaine protection des renseignements personnels. Vous ne devriez pas pouvoir regarder les photos de mes enfants simplement parce que...

[*Français*]

M. René Villemure: Je me permets de vous interrompre. Veuillez m'en excuser.

Mme Jennifer Carr: Oui, allez-y.

M. René Villemure: Il ne me reste plus beaucoup de temps et je vais être rapide.

Les sous-ministres ont des attentes qui sont signifiées par le gouvernement. Est-ce qu'une composante relative à la vie privée devrait faire partie de ces attentes?

Mme Jennifer Carr: Il n'y a pas de réponse courte à cette question.

M. René Villemure: Je vais considérer votre réponse comme un oui.

Mme Jennifer Carr: D'accord.

Des voix: Ha, ha!

M. René Villemure: Merci beaucoup, madame Carr et monsieur Prier.

Le président: Merci, monsieur Villemure.

[*Traduction*]

Madame Carr, vous serez heureuse d'apprendre que M. Brock et moi jouons encore à Pong sur notre Commodore 64.

Des voix: Ha, ha!

Mme Jennifer Carr: Et vous avez encore Napster.

Le président: Non. Je suis abonné à Apple Music. C'est 14,95 $ par mois; je le sais.

Monsieur Green, vous disposez de six minutes. Allez-y.

M. Matthew Green: Merci beaucoup.

Je suis fier de dire que j'ai téléchargé le premier album de Wu-Tang sur Napster il y a plus de 20 ans. Le groupe fait maintenant des tournées de réunion. Voilà où nous en sommes.

J'aimerais reprendre là où s'est arrêté mon collègue, au sujet d'une notion que je crois généralement acceptée: le consentement éclairé.

Est-ce que vous convenez que vos membres — selon la directive du Conseil du Trésor voulant que les technologies mises en œuvre au sein du gouvernement fédéral fassent l'objet d'une évaluation des facteurs relatifs à la vie privée — pourraient raisonnablement s'attendre à ce que toutes les technologies passent par ce processus, en vertu de la directive du Conseil du Trésor?

Est-ce qu'on peut parler d'une attente raisonnable?

Mme Jennifer Carr: Je ne suis pas de cet avis, puisque selon les politiques en place, l'usage personnel est permis. Il n'y a pas de précision à ce sujet.

Si les sous-ministres ne respectent pas leurs propres directives, comment pouvons-nous nous attendre à ce que les employés...

M. Matthew Green: Je veux être certain que vous compreniez bien ma question.

Je dis que le Conseil du Trésor a mis en place une directive. Nous avons entendu des témoignages voulant que certains ministères ne respectent pas cette directive. Donc, est-ce que vos membres...? Puisque c'est ce qu'exige la politique, est-il raisonnable pour les ministères de présumer que ces mesures sont prises, même si nous avons entendu dire qu'elles ne l'étaient pas?

Mme Jennifer Carr: Oui, s'il y a une directive... Le Conseil du Trésor dit tout le temps qu'il y a des directives à suivre. Je m'attends à ce que les ministères les respectent. Ce sont des cadres supérieurs.

M. Matthew Green: Monsieur Prier.

M. Nathan Prier: Nos membres s'attendent au respect des directives. Ils sont d'avis qu'il y a eu abus de confiance, en raison de la violation d'une politique très claire sur le sujet. Ils craignent maintenant d'utiliser les appareils qui devraient être associés à des mesures de protection de la vie privée, comme l'énonce la politique.

M. Matthew Green: Croyez-vous que le Commissariat à la protection de la vie privée doive examiner par défaut toutes ces technologies, surtout celles qui pourraient recueillir discrètement des données?

M. Nathan Prier: Oui.

M. Matthew Green: Je soulève la question parce que vous avez parlé du retrait des pouvoirs.

Est-ce qu'ils auraient dû avoir ces pouvoirs?

Mme Jennifer Carr: Qu'il s'agisse du commissaire à la protection de la vie privée ou des sous-ministres dans leur ministère... Vous avez vu que les 13 ministères se sont démenés pour vous donner l'information, pour savoir comment elle était utilisée et pour vous fournir des témoignages. Il faut une responsabilité claire à l'échelon des sous-ministres; sinon, les pouvoirs doivent revenir au commissaire.

M. Nathan Prier: Le Commissariat à la protection de la vie privée est le bon endroit pour cela. Dans de nombreux cas, et dans le cas des directives du Conseil du Trésor, les sous-ministres ont leurs divergences et leurs propres pouvoirs décisionnels, lorsque c'est utile pour l'employeur, et ensuite...

● (1245)

M. Matthew Green: C'est un peu le far west.

M. Nathan Prier: Oui, c'est un peu le far west dans le domaine de l'application des politiques, sauf lorsque c'est utile pour...

M. Matthew Green: Rapidement, y a-t-il eu des griefs?

Mme Jennifer Carr: Nous n'avons pas entendu parler de griefs, mais pour se rendre là, il faut savoir exactement ce qui se passe.

M. Matthew Green: C'est exact.

Est-ce qu'une absence de grief équivaut à une permission de contrevenir à la Loi sur la protection des renseignements personnels?

Mme Jennifer Carr: Pas du tout.

On ne peut pas déposer un grief si on ne sait pas ce qui se passe. Lorsqu'on comprend ce qui se passe, alors on peut déposer un grief, mais sinon, il est impossible de protéger ses droits.

M. Matthew Green: Monsieur Prier.

M. Nathan Prier: Un grief pourrait faire un peu bouger les choses. Nous voulons trouver des façons de faire respecter les droits de nos membres dans le cas présent, mais le fait est qu'il y a des politiques en place et qu'elles devraient être respectées par la direction.

M. Matthew Green: Est-ce qu'il faudrait examiner la Loi sur la protection des renseignements personnels?

Mme Jennifer Carr: Oui, sans aucun doute.

M. Matthew Green: Qu'est-ce qu'elle devrait contenir, selon vous?

Mme Jennifer Carr: Il faut que les lignes directrices établissent clairement quand et comment les nouveaux besoins ou les besoins modifiés doivent faire l'objet d'une évaluation relative à la protection de la vie privée, et quand les besoins actuels doivent être mis à jour. Il faut aussi veiller à ce que les lignes directrices soient respectées. Les outils logiciels doivent faire l'objet d'une évaluation avant d'être utilisés, et il faut d'abord envisager toutes les méthodes moins invasives.

M. Matthew Green: Monsieur Prier, voulez-vous ajouter quelque chose?

M. Nathan Prier: L'employeur doit prendre au sérieux ses responsabilités envers les travailleurs et envers la population canadienne. On a fait valoir à maintes reprises qu'il s'agissait de citoyens canadiens et de fonctionnaires. Lorsque les politiques numériques sont désuètes et ne sont pas respectées, on se retrouve avec des logiciels espions sur les appareils du gouvernement. De toute évidence, les droits constitutionnels ne sont pas respectés.

La Loi sur la protection des renseignements personnels pourrait être mise à jour de toutes sortes de façons, mais il y a beaucoup de bons outils en place. Il n'y a toutefois aucun mécanisme d'application et aucune conséquence associée à leur violation.

M. Matthew Green: Je veux que vous puissiez répondre à une question que d'autres ministères ont posé de façon générale. On a recours à des outils pour examiner les cas de violation des politiques gouvernementales comme la fraude ou le harcèlement au travail. Le gouvernement ne devrait-il pas avoir le droit de se pencher sur ces cas de violations graves?

Mme Jennifer Carr: S'ils utilisent les outils de la bonne façon, pour les fonctions pour lesquelles ils ont été conçus et selon l'évaluation de la protection des données qui a été réalisée, nous devons veiller à ce que... Nous avons entendu trois ministères. Leurs représentants nous ont dit qu'ils y avaient recours sans réaliser les évaluations préalables. Nous devons veiller à ce que les évaluations soient faites de la bonne façon.

M. Matthew Green: Monsieur Prier.

M. Nathan Prier: Je n'ai rien à ajouter.

M. Matthew Green: Alors que nous en sommes à nos recommandations finales, et nonobstant le fait que vos membres suivront probablement le dossier, quelles sont les mesures que nous pouvons prendre pour rétablir la confiance au sujet de quelque chose qui est pleinement intégré à tous les aspects de la vie, à mon avis? Vous avez parlé de la façon dont les applications sur les téléphones... J'ai un iPhone. J'ai une montre Apple. J'ai des données biométriques. Toutes les façons dont... J'ai mes renseignements bancaires. Tout est là.

Comment pouvons-nous aider à rétablir la confiance de vos membres à l'égard de la haute direction?

Mme Jennifer Carr: C'est une question de reddition de comptes. S'il y a des directives en place, qu'arrive-t-il lorsque les gens ne les respectent pas, alors qu'on leur demande de prendre certaines mesures avant...?

Comme je l'ai dit dans ma déclaration préliminaire, le gouvernement doit reconnaître que nous sommes des citoyens canadiens et que lorsque nous utilisons les appareils de notre employeur, cela ne signifie pas qu'il est propriétaire des données qu'ils contiennent.

M. Nathan Prier: Un examen complet des politiques numériques et un mécanisme pour les mettre à jour en fonction des nouvelles technologies seraient l'idéal.

Je veux simplement souligner encore une fois qu'en tant que plus grand employeur au Canada, le gouvernement fédéral a le pouvoir — et des pouvoirs assez précis — d'imposer des politiques visant la divulgation proactive, le consentement éclairé et l'application des politiques de protection de la vie privée d'une manière qui n'est peut-être pas imposée au secteur privé. Par conséquent, nous devons établir les points de référence, en tant que l'un des plus grands employeurs du pays et aussi en tant que gouvernement du Canada, pour avoir recours à des pouvoirs qui pourraient être moins évidents dans le secteur privé. Il y a là un point de référence important à établir pour tous les Canadiens et pour nos membres.

Le président: Merci, monsieur Prier.

Monsieur Green, votre question était importante, alors je vous ai donné un peu plus de temps pour que nous entendions la réponse. J'avais aussi peur que M. Green dépose un grief contre l'association internationale des présidentes de comités.

Monsieur Brock, vous disposez de cinq minutes.

Nous allons tenir deux rondes de cinq minutes et deux rondes de deux minutes et demie.

Allez-y, monsieur Brock.

M. Larry Brock: Merci, monsieur le président.

Je remercie les témoins de leur présence.

Comme vous le savez, la vérificatrice générale a publié plus tôt cette semaine un rapport qui a eu l'effet d'une bombe en exposant l'incompétence et la corruption au sein de l'ASFC. Je pense que le problème le plus flagrant a trait à la façon dont le gouvernement, malgré une promesse en 2015 de réduire le recours à des consultants externes et de miser sur la fonction publique professionnelle... Nous savons qu'au fil des ans, il a augmenté la taille de la fonction publique de près de 40 %.

Comment vous sentez-vous, en tant que dirigeants syndicaux, et comment vos membres se sentent-ils, sachant que GC Strategies — une entreprise formée de deux personnes qui travaillent dans un sous-sol et qui n'ont aucune expérience en TI — se contentait de mettre le gouvernement en contact avec des professionnels des TI? Que pensez-vous de cet abus flagrant de l'expertise de vos membres?

● (1250)

Mme Jennifer Carr: Je vais répondre à cette question parce que je représente les travailleurs du secteur des TI.

Je dirais que nous sommes furieux. J'aimerais revenir en témoigner devant le Comité. Je pourrais vous en dire long sur ce processus.

L'un de nos membres m'a dit cette semaine qu'il ne pouvait même pas avoir un crayon et un cahier sans une autorisation signée par deux personnes. Comment a-t-on pu laisser passer quelque chose d'aussi gros que cela?

J'aimerais vraiment revenir vous en parler. Je ne me suis pas préparée pour cela aujourd'hui, mais j'aimerais le faire à un autre moment.

M. Larry Brock: Vous disposez de trois minutes et demie. Pouvez-vous nous en dire plus? J'aimerais vous entendre sur le sujet.

Mme Jennifer Carr: La sous-traitance représente une préoccupation pour l'Institut professionnel de la fonction publique du Canada. Nous représentons des professionnels, notamment des ingénieurs, des infirmières et des médecins... Ce sont tous des professionnels réglementés qui prennent leur travail au nom des Canadiens très au sérieux.

En voyant le travail qui est donné en sous-traitance... Cela entraîne une augmentation des coûts pour le gouvernement — 40 % selon le rapport — ainsi qu'une diminution de la transparence, de la reddition de comptes et de la qualité des services. Le plus important, pour moi, c'est la perte de connaissances institutionnelles parce que le travail se fait à l'externe. Cela signifie que nous devons toujours dépendre des entrepreneurs, ne serait-ce que pour corriger leurs erreurs.

Nous devons nous assurer d'investir dans la fonction publique, afin qu'elle puisse maintenir et fournir les services fiables sur lesquels les Canadiens comptent et auxquels ils s'attendent.

M. Larry Brock: Merci beaucoup.

Puisque le Comité élargira la portée de son travail, je suis certain que nous allons vous revoir, madame Carr. Merci.

J'aimerais maintenant poser la question à M. Prier et à Mme Shantz.

Voulez-vous commenter cette affaire?

M. Nathan Prier: Il s'agissait d'une violation flagrante des politiques d'approvisionnement et d'une violation flagrante de... C'est l'une des nombreuses façons dont la sous-traitance a enflé ce que les gens considèrent généralement comme le secteur public. En fait, les fonctionnaires ne constituent pas la totalité de la fonction publique. Il s'agit en grande partie de relations louches et d'entrepreneurs... Ils sont parfois nécessaires, bien sûr.

Je suis ici à titre d'analyste des politiques et de président d'un syndicat qui représente de nombreuses personnes qui ont la même profession que moi. Même dans le monde spécialisé de l'élaboration des politiques, la sous-traitance est chose commune. Il y a des bases de données auxquelles nous n'avons pas accès. Il y a des champs d'information auxquels nous n'avons tout simplement pas accès, mais le fait de ne pas être en mesure de bâtir la mémoire institutionnelle nécessaire pour pouvoir accomplir nos tâches de façon régulière est un problème persistant.

Lorsque les gens parlent du gonflement du secteur public, pour nos membres, il s'agit des vastes réseaux de relations avec les entrepreneurs pour un travail qui pourrait probablement se faire à bien meilleur marché, de façon beaucoup plus efficace et dans l'esprit de renforcer la mémoire institutionnelle et la capacité à l'interne.

Nous ne croyons pas que la taille du secteur public soit démesurée. Nous ne croyons pas qu'il soit nécessaire de couper dans le gras au cours des 5 à 10 prochaines années. Cependant, nous avons besoin que ces relations avec les entrepreneurs et ce vaste réseau soient fortement limités, car nous estimons que nos membres sont qualifiés et sont les mieux placés pour faire le travail, et qu'il faut assurer une surveillance stricte et appropriée.

M. Larry Brock: Merci.

Madame Shantz, qu'en pensez-vous?

Mme Laura Shantz (conseillère principale, Défense des droits et campagnes, Association canadienne des employés professionnels): J'aimerais ajouter une chose, rapidement. Nous sommes ici aujourd'hui pour parler de la protection des renseignements personnels. Dès que l'on ajoute des couches de sous-traitance, on se retrouve avec des possibilités infinies d'atteinte à la sécurité des données. Nous l'avons vu avec BGRS. Il y a eu un autre cas récemment; je ne me souviens plus du nom.

Ces situations commencent à se produire. Lorsque l'on donne de plus en plus de contrats en sous-traitance, on court de plus en plus de risques de défaillance ou d'atteinte à la sécurité. Il faut voir la situation de manière holistique et songer à la façon de maximiser la sécurité, parce qu'il s'agit des données personnelles des Canadiens et des fonctionnaires, et de données importantes pour le gouvernement sur le plan de la sécurité.

C'est un travail essentiel, pour lequel les fonctionnaires sont formés. Ils savent comment bien faire les choses. Lorsque nous donnons le travail en sous-traitance, nous perdons le contrôle. Il ne faut pas l'oublier.

M. Larry Brock: Merci beaucoup à vous tous.

Le président: Merci, monsieur Brock.

Monsieur Sorbara, vous disposez de cinq minutes. Allez-y.

● (1255)

M. Francesco Sorbara (Vaughan—Woodbridge, Lib.): Merci, monsieur le président.

C'est merveilleux d'être ici avec vous, monsieur le président, et tous mes honorables collègues. Cela fait déjà deux ou trois ans depuis la dernière fois où j'ai siégé au comité de l'éthique. J'ai siégé ici pendant un certain temps. J'ai toujours trouvé que ce comité était très important à bien des égards. Je dirais qu'il mène de nombreuses études sérieuses.

Je souhaite la bienvenue aux témoins ici aujourd'hui.

Tout d'abord, je tiens à remercier les témoins, tous vos syndiqués et tous les fonctionnaires fédéraux de tout le travail que vous faites. Je ne remercie pas seulement les employés de la Bibliothèque du Parlement qui aident les députés. Merci à vous pour tous les services et les prestations que vous fournissez à des millions de Canadiens tous les jours.

J'aimerais aussi dire que nous avons embauché bien des gens dans la fonction publique fédérale ces dernières années. Nous l'avons rebâtie après les compressions dévastatrices du gouvernement Harper; c'est ainsi que je pourrais les décrire. Ce gouvernement-là a fait des coupes jusqu'à l'os. Nous savons ce que c'était d'être fonctionnaire fédéral sous l'administration conservatrice, n'est-ce pas?

Il y a peu, le député de Brantford—Brant a dit ici au Comité que pour les fonctionnaires, il n'y a pas d'enjeux de vie privée dans leur cas.

Madame Carr et monsieur Prier, croyez-vous que les fonctionnaires ont droit à la protection de leurs renseignements personnels?

Mme Jennifer Carr: Ils ont tout à fait droit à leur vie privée. Je répète que nous sommes des citoyens canadiens. Nous ne prêtons pas allégeance à un gouvernement. Nous sommes autonomes et pouvons avoir des opinions politiques. Nous ne devrions pas craindre de perdre notre droit à la vie privée seulement parce que nous travaillons pour le gouvernement fédéral.

M. Francesco Sorbara: Qu'en dites-vous, monsieur Prier?

M. Nathan Prier: J'y crois et c'est un principe pour moi. Je crois qu'il y a des politiques qui protègent nos droits, comme Jennifer en a fait mention à quelques reprises ici.

M. Francesco Sorbara: D'accord.

Concernant la vie privée, j'ai le plaisir et l'honneur de siéger au comité de l'industrie. Le projet de loi C-27 et la LPRPDE contiennent des dispositions sur la protection de la vie privée, qui prend beaucoup d'importance de nos jours; c'est le moins qu'on puisse dire. Il faut trouver un équilibre. J'emploie des termes très courants, si je puis dire. Comme bien des députés, j'ai travaillé dans le secteur privé avant d'avoir le grand plaisir de servir les électeurs de ma circonscription. Lorsqu'on reçoit un appareil de son employeur, cet appareil lui appartient. Il faut l'utiliser avec discernement et diligence. Il faut trouver un équilibre; c'est ce que j'ai toujours considéré.

Dans ce contexte, dans les opérations du gouvernement et dans les ministères, il faut respecter des garde-fous et suivre les évaluations des facteurs relatifs à la vie privée. Je l'ai littéralement appris dans les dernières heures. Je siège à deux autres comités, donc ma semaine a été fort occupée. Ces évaluations prévoient qu'il peut y avoir des enquêtes au besoin. Quand il faut mener une enquête, il faut examiner tous les appareils et leur contenu.

Pour mettre les choses en perspective, si je travaillais pour l'organisation de M. Prier et que je signais une entente avec le gouvernement fédéral, on accepterait que j'utilise l'appareil qui m'est prêté, mais de façon responsable. Je le dis, car il faut trouver un équilibre. Quand les règles ne sont pas suivies comme il faut, il faut bien sûr corriger les processus internes et la gouvernance.

Êtes-vous d'accord que le consentement et l'équilibre sont importants, mais que l'utilisateur final détient aussi une responsabilité importante?

Mme Jennifer Carr: Oui, il s'agit d'une responsabilité partagée. Mais si vous ne me dites pas d'emblée ce que je peux et ce que je ne peux pas faire, si vous ne divulguez pas ce que vous allez examiner... Si j'accédais à un site pour consulter mes photos, vous pourriez ensuite franchir tous les pare-feux et les consulter aussi. Ce n'est pas arrivé jusqu'à maintenant.

M. Nathan Prier: Je crois que l'on est en train d'établir des limites à l'heure actuelle, et le droit à vie privée dans l'utilisation personnelle d'un cellulaire ou d'autres appareils est aussi plus ou moins bien établi. Nous découvrons des garde-fous avec le temps.

Je dirais que ce n'est pas ce dont il s'agit ici. Il est plutôt question de divulgation proactive d'une technologie qui aurait dû faire l'objet d'une communication aux employés qui utilisent ces appareils. Nous croyons que les intrusions dépassent de loin le consentement éclairé quand nous découvrons nous-mêmes les technologies qui se trouvent dans nos appareils grâce à une demande d'accès à l'information, et par divulgation proactive.

M. Francesco Sorbara: Combien de temps me reste-t-il, monsieur le président?

Le président: Vous avez 35 secondes.

M. Francesco Sorbara: Je veux seulement obtenir une précision. Actuellement, lorsqu'une personne est embauchée et se joint à la fonction publique, qu'elle répond aux exigences et que toutes les démarches ont été faites en bonne et due forme, à quoi doit-elle consentir ou quelle information lui est donnée?

J'aimerais entendre Mme Carr, puis M. Prier, assez rapidement.

Mme Jennifer Carr: Diverses règles s'appliquent, selon le ministère où la personne travaille. Évidemment, je crois qu'on l'informe des valeurs et de l'éthique à respecter. C'est une exigence qui requiert sa signature. Sinon, je ne pense pas qu'il y ait un même ensemble de mesures à observer dans tous les ministères.

Encore une fois, cela dépend du contexte. La décentralisation est telle que l'on permet aux ministères d'adopter leurs propres politiques.

● (1300)

M. Nathan Prier: J'ai travaillé pour bon nombre de ministères et je peux vous dire qu'il y a une grande variabilité dans la formation donnée à un nouvel employé ou à un employé qui reçoit un appareil, ainsi que dans sa capacité de donner son consentement.

Oui, il s'agit bien sûr d'une responsabilité partagée, mais dans certains cas, je sentais plus qu'on me parlait des modalités d'utilisation d'un nouveau cellulaire quand on me parlait de mes divers droits et responsabilités qui accompagnaient un appareil du gouvernement. Il serait peut-être nécessaire de donner de la formation, mais encore là, je ne pense pas que c'est ce dont il s'agit ici.

Le président: Merci.

Je vous remercie, monsieur Sorbara.

[*Français*]

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

M. René Villemure: On a parlé du Code de valeurs et d'éthique de la fonction publique, mais laissez-moi vous dire qu'il s'agit d'un guide qui n'éclaire pas beaucoup notre lanterne.

Je vais revenir à la question que j'ai posée lors de mon dernier tour de parole.

Autrefois, en matière d'éthique, les sous-ministres avaient des attentes signifiées lors de l'émission du Code. On devait mesurer leurs connaissances et l'implantation d'une telle chose. Je ne suis pas certain du succès.

Madame Carr, croyez-vous que de telles attentes en matière de vie privée devraient faire partie de l'évaluation des sous-ministres? Autrement dit, à la fin de l'année, on évaluerait les pratiques qu'ils ont mises en place ou leur conformité relative à la vie privée.

[*Traduction*]

Mme Jennifer Carr: C'est une grande question. Nous parlons de gestion du rendement. J'ai beaucoup à dire là-dessus aussi.

Oui, si vous aviez une liste de vérification des politiques que ne respectaient pas certains employés, il serait important de savoir qui d'entre eux ont signé la politique sur l'éthique et ce genre de choses.

Je pense que la question dépasse largement...

[*Français*]

M. René Villemure: Madame Carr, excusez-moi de vous interrompre, mais je n'ai pas beaucoup de temps de parole.

Monsieur Prier, voulez-vous répondre à ma question?

[*Traduction*]

M. Nathan Prier: Je crois que les outils de gestion du rendement peuvent effectivement être utilisés ici.

Je pense qu'il convient bel et bien d'imposer des conséquences en cas de violation de la vie privée.

[*Français*]

M. René Villemure: On nous a souvent dit que l'utilisation de cet outil était la seule manière d'obtenir les résultats recherchés. Croyez-vous que c'est le cas?

[*Traduction*]

M. Nathan Prier: Voulez-vous savoir si la demande d'accès à l'information était la seule façon...

[*Français*]

M. René Villemure: Je parle de l'utilisation de l'outil sur les appareils.

Souvent, le manque de supervision entraîne certains comportements. Si on faisait une meilleure supervision, certains comportements n'auraient pas lieu et, par conséquent, on n'aurait pas besoin de faire de la surveillance.

[*Traduction*]

Mme Jennifer Carr: Je pense que c'est bien l'objectif de l'évaluation des facteurs relatifs à la vie privée. Quelle information cherche-t-on à obtenir? Parlons du vol de temps et de la présence des employés sur les lieux de travail. Pourrions-nous obtenir ces informations par d'autres moyens que la recherche invasive dans un appareil?

C'est ce à quoi sert l'évaluation, qui devrait être la principale façon d'obtenir des données de manière moins intrusive.

[*Français*]

M. René Villemure: C'est parfait.

[*Traduction*]

M. Nathan Prier: Je n'ai pas grand-chose à ajouter, sauf que la divulgation proactive d'une nouvelle technologie qu'on utilise est au cœur du lien de confiance brisé ici; ne l'oubliez pas. Quels que soient les résultats que donne cette technologie, et bien qu'il soit encore important d'en parler, je pense que la divulgation proactive, pour ajouter à ce que Mme Carr a dit...

[*Français*]

M. René Villemure: Merci beaucoup.

Le président: Merci, monsieur Villemure.

[*Traduction*]

La parole va à M. Green pour deux minutes et demie.

M. Matthew Green: Je vous remercie beaucoup.

En préparation aux réunions de comités, on passe souvent en revue les questions qui pourraient être posées. On pense aussi aux points les plus importants qu'on veut faire valoir. Mais il arrive parfois que les questions attendues ne soient pas posées.

Y a-t-il des points intéressants que vous voulez présenter ou des réponses que vous voudriez donner au Comité, mis à part votre déclaration liminaire et les questions déjà posées?

Mme Jennifer Carr: Je vais justement parler de sous-traitance au comité de la défense dans deux semaines.

La reddition de comptes en général et la décentralisation des responsabilités que l'on confie aux ministères ont créé un contexte dans lequel il m'est difficile de dire à nos membres quels sont leurs droits, comment ceux-ci s'appliquent et quelles politiques ils doivent respecter. Il est difficile de les guider.

J'aimerais beaucoup dire que nous travaillons tous pour le gouvernement fédéral et que nous n'avons qu'un seul employeur. Cela dit, nous devons observer bien des règles et des règlements différents, selon le ministère où nous travaillons.

M. Nathan Prier: Je crois avoir mentionné la plupart des choses que je voulais dire aujourd'hui.

Merci.

M. Matthew Green: Si vous voulez ajouter quelque chose ou si vous entendez des informations auxquelles vous aimeriez réagir, nonobstant la prochaine séance avec le Conseil du Trésor, n'hésitez pas à nous en parler pour que nous examinions la question.

Nous vous sommes très reconnaissants de votre travail.

Mme Jennifer Carr: Je vais certainement vous fournir ces lignes directrices pour que tous les membres du Comité sachent ce qui est permis.

M. Matthew Green: Durant le temps qu'il me reste, je tiens aussi à dire que je ne suis pas surpris que des représentants syndicaux arrivent avec des solutions. Je sais qu'un ancien président d'une association de pompiers, notre président, n'est pas surpris lui non plus.

Merci d'être ici aujourd'hui. Je vous remercie de votre témoignage.

● (1305)

Le président: Merci, monsieur Green.

C'est ce qui met fin à cette partie de la réunion d'aujourd'hui.

Je vous remercie tous d'avoir témoigné devant notre comité pour cette étude importante. Je tiens aussi à relayer le message suivant du Comité à vos membres: nous vous sommes très reconnaissants du travail que vous accomplissez pour les Canadiens.

S'il n'y a pas d'autre chose, c'est ainsi que se conclue la réunion d'aujourd'hui.

Je vous souhaite tous une bonne semaine dans vos circonscriptions.

À notre prochaine séance du 27 février, nous entendrons le commissaire de la GRC en lien avec SNC-Lavalin.

Je remercie la greffière, les analystes et les techniciens de toute leur aide pour tenir cette réunion.

La séance est levée.