CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

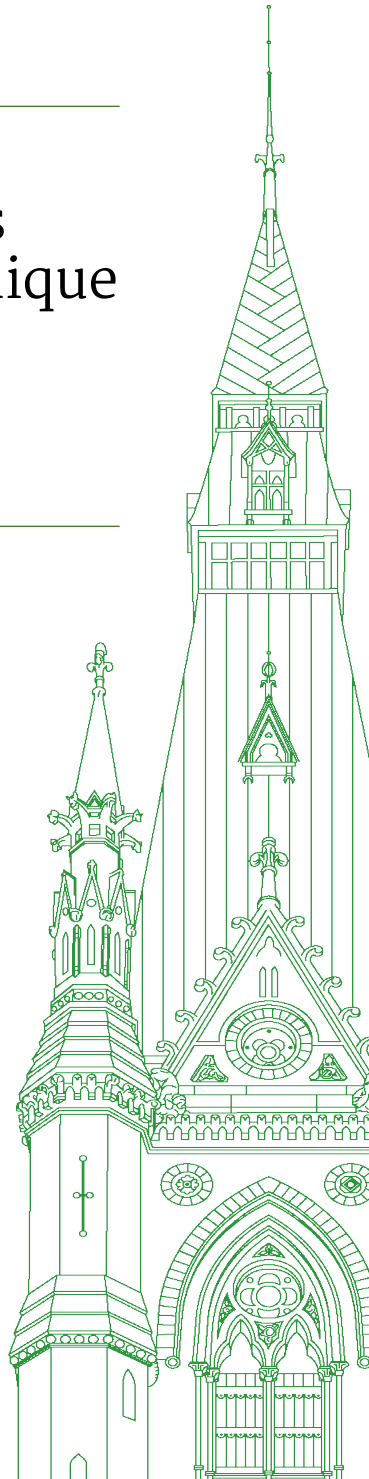
44e LÉGISLATURE, 1re SESSION

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

TÉMOIGNAGES

NUMÉRO 092

Le lundi 20 novembre 2023



Président : M. John Brassard

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

Le lundi 20 novembre 2023

● (1550)

[*Traduction*]

Le président (M. John Brassard (Barrie—Innisfil, PCC)): La séance est ouverte.

Bienvenue à tous et à toutes à la 92e 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.

[*Français*]

Conformément à l'alinéa 108(3)h) du Règlement et à la motion adoptée par le Comité le mardi 31 janvier 2023, le Comité reprend son étude de l'utilisation des plateformes de médias sociaux pour la collecte de données et le partage non éthique ou illicite de renseignements personnels avec des entités étrangères.

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

[*Traduction*]

Je voudrais rappeler à tous les membres et témoins qu'il faut faire attention aux oreillettes pour l'interprétation. Veuillez ne pas placer votre oreillette à proximité du microphone, car cela peut provoquer un choc acoustique, qui pourrait à son tour blesser les interprètes.

J'aimerais maintenant souhaiter la bienvenue à nos témoins de la première heure aujourd'hui.

Nous accueillons les représentants du Service canadien du renseignement de sécurité, le SCRS, M. Peter Madou, directeur général, Évaluation des renseignements — bienvenue, M. Madou — et Mme Cherie Henderson, directrice adjointe, Exigences.

Nous accueillons aussi M. Sami Khoury, dirigeant principal, Centre canadien pour la cybersécurité, du Centre de la sécurité des télécommunications.

Nous allons commencer par les représentants du SCRS. Vous avez au plus cinq minutes pour votre déclaration préliminaire.

Madame Henderson, allez-y, je vous prie. Merci.

Mme Cherie Henderson (directrice adjointe, Exigences, Service canadien du renseignement de sécurité): Merci.

Monsieur le président, mesdames et messieurs les membres du Comité, bonjour.

Je m'appelle Cherie Henderson, et je suis sous-ministre et directrice adjointe des Exigences au SCRS.

[*Français*]

C'est un honneur que de pouvoir me joindre à vous aujourd'hui pour contribuer à vos discussions importantes au sujet des médias sociaux et des entités étrangères. Je suis accompagnée de mon collègue Peter Madou, directeur général, Bureau stratégique.

[*Traduction*]

Nous espérons aujourd'hui pouvoir éclairer le Comité sur les préoccupations en matière de sécurité nationale associées aux échanges de données avec des entités étrangères telles que la République populaire de Chine, ou RPC, ainsi que le rôle que le SCRS joue pour protéger la prospérité du Canada, ses intérêts sur le plan de la sécurité nationale et la sécurité des Canadiens.

[*Français*]

Des acteurs étatiques étrangers mènent leurs activités d'ingérence en faisant appel à tous les moyens viables à leur disposition, dont les plateformes de médias sociaux, qui sont un outil idéal pour de telles opérations.

[*Traduction*]

Les auteurs de menace tels que la Fédération de Russie et la RPC exploitent les médias sociaux pour propager de la désinformation en faisant appel à des algorithmes subjectifs qui amplifient les chambres d'écho et manipulent le contenu affiché auprès du public sans susciter de suspicion. L'utilité de tels outils était notamment évidente lors de l'élection présidentielle de 2016 aux États-Unis et continue de susciter des préoccupations au Canada. Ces caractéristiques des médias sociaux sont également utilisées par des auteurs de menace extrémistes pour radicaliser et recruter des utilisateurs.

Les auteurs de menace s'intéressent aux plateformes de médias sociaux en raison des données qu'elles génèrent et recueillent. Ces plateformes tiennent des sondages, rassemblent des ensembles de données et demandent un accès aux données personnelles des utilisateurs dans leurs conditions d'utilisation, leur permettant ainsi d'accéder aux albums photos, aux messages et aux listes de contacts sur votre téléphone. Bien que certaines de ces données soient plutôt anodines lorsqu'elles sont examinées individuellement, elles peuvent permettre de cerner précisément des tendances et d'en apprendre plus sur diverses populations, sur l'opinion publique et sur des réseaux individuels lorsqu'elles sont recueillies et réunies en volumes importants. C'est pourquoi il est essentiel pour les Canadiens d'être au courant des facteurs à prendre en compte sur le plan de la vie privée lorsqu'ils choisissent de transmettre leurs informations personnelles en ligne, en particulier lorsqu'il est question d'entreprises étrangères qui se trouvent en dehors du Canada et de pays alliés.

Les États autoritaires tels que la RPC se servent des mégadonnées, y compris celles du secteur privé, pour mener leurs activités d'ingérence étrangère. Même si l'utilisation des données par le gouvernement est rigoureusement encadrée, au Canada, selon des obligations sur le plan de l'éthique, de la loi et du respect de la vie privée, les États autoritaires ne se soumettent pas à de telles restrictions. La RPC se sert de ce libre accès pour amasser des volumes de données supérieurs aux collections combinées de tous les autres pays, et ce, tout en protégeant ses propres informations.

Les nouvelles technologies, telles que l'intelligence artificielle, ne feront que l'aider encore plus dans ses activités malfaisantes. La loi de 2017 sur le renseignement national de la RPC oblige par ailleurs les particuliers, les organisations et les institutions, y compris les plateformes de médias sociaux qui offrent des services en Chine, à fournir des informations de masse au gouvernement de la Chine. Ces informations aident ensuite les services de sécurité et de renseignement de la RPC à mener toute une gamme d'activités dans le domaine du renseignement. Les organisations établies dans la RPC et les citoyens de la RPC sont également tenus de garder dans le secret tous les travaux de l'État liés au renseignement. Cette politique appuie et reflète les tentatives audacieuses et continues de la Chine visant à mener des activités d'ingérence étrangère au Canada.

Il est essentiel que le Canada devienne plus résilient face à l'ingérence étrangère. Cela comprend notamment de sensibiliser davantage la population au sujet de l'aptitude de la RPC à recueillir et à utiliser les informations des Canadiens obtenues à partir des médias sociaux pour mener des activités d'ingérence étrangère.

Par exemple, le compte X du SCRS a récemment publié un fil de messages sur la façon dont les services de renseignement de la RPC utilisent Linkedln pour cibler les Canadiens en prétendant être des contacts d'affaires à la recherche d'experts-conseils au Canada, de sorte à les pousser à fournir à leur insu des informations confidentielles d'intérêt pour la RPC à des agents de renseignement spécialement formés.

● (1555)

[*Français*]

Pour protéger la sécurité nationale du Canada, il est plus que jamais nécessaire d'adopter une approche englobant toute la société, qui prévoirait pour commencer des discussions éclairées et franches entre les communautés, les universitaires et tous les ordres de gouvernement. Il est important que les utilisateurs de médias sociaux soient au courant des risques associés à la transmission de données personnelles sur certaines plateformes. Le SCRS demeure un partenaire engagé dans ces efforts, et son équipe de professionnels talentueux et dévoués travaille d'arrache-pied à assurer la sécurité et la prospérité de tous les Canadiens.

[*Traduction*]

Je me ferai un plaisir de répondre à vos questions.

Merci.

Le président: Merci, madame Henderson, de nous avoir présenté votre déclaration.

C'est maintenant au tour de M. Khoury, dirigeant principal du Centre canadien pour la cybersécurité.

Vous aurez cinq minutes pour présenter votre déclaration au Comité, monsieur. Allez-y, je vous prie.

M. Sami Khoury (dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Bonjour, monsieur le président et chers membres du Parlement.

Je suis heureux de participer à la réunion d'aujourd'hui, et j'aimerais d'abord reconnaître que nous nous trouvons sur un territoire non cédé de la nation algonquine Anishinaabe.

Je m'appelle Sami Khoury, et je suis le dirigeant principal du Centre canadien pour la cybersécurité, ou Centre pour la cybersécurité. Le Centre pour la cybersécurité fait partie du Centre de la sécurité des télécommunications.

[*Français*]

En tant qu'autorité technique du Canada en matière de cybersécurité, nous mettons à profit notre expertise afin de protéger l'information et les systèmes auxquels se fient quotidiennement les Canadiennes et les Canadiens.

[*Traduction*]

Nous protégeons et défendons les biens électroniques précieux du Canada, nous menons les interventions fédérales du Canada lorsque se produisent des événements de cybersécurité et nous rehaussons la barre en matière de cybersécurité au Canada afin que les Canadiens et les Canadiennes puissent mener leurs activités professionnelles et personnelles en ligne en toute confiance et en toute sécurité.

Le Centre pour la cybersécurité publie des avis et des conseils à l'intention des Canadiennes et des Canadiens sur les dangers qui les guettent en ligne ainsi que sur les mesures à prendre pour assurer leur protection et celle de leurs organisations contre la menace que peuvent poser les applications de réseaux sociaux.

[*Français*]

Nous aidons aussi le gouvernement du Canada à prendre des décisions stratégiques en matière de cybersécurité, y compris sur l'utilisation des applications de réseaux sociaux, qui constituent un important outil de communication avec la population.

[*Traduction*]

En février dernier, le Secrétariat du Conseil du Trésor, le SCT, a publié une déclaration annonçant l'interdiction d'utiliser l'application TikTok sur les appareils mobiles fournis par le gouvernement. Pas plus tard que la semaine dernière, une annonce similaire a été faite concernant l'utilisation de WeChat. Les deux décisions ont été prises par la dirigeante principale de l'information du Canada, qui a évalué que les applications en question présentaient un niveau de risque inacceptable. Bien que ces interdictions s'appliquent uniquement aux appareils émis par le gouvernement, les deux déclarations du SCT ont mené les Canadiennes et Canadiens à des lignes directrices publiées par le Centre pour la cybersécurité.

Dans notre Évaluation non classifiée des cybermenaces nationales de 2023-2024, nous avons évalué que les États étrangers utilisent les médias sociaux pour cibler des Canadiennes et Canadiens en particulier. Selon un rapport du Citizen Lab de l'Université de Toronto, des cybermenaces ciblent des activistes au Canada en ayant recours à la désinformation ou à l'intimidation sur les médias sociaux, à des attaques par déni de service contre des organisations et à la compromission de leurs dispositifs personnels.

Au-delà du recours à des activités de cybermenace contre des citoyennes et citoyens, il est fort probable que des pays utilisent des applications de messagerie et de médias sociaux étrangers populaires auprès de la diaspora au Canada et à travers le monde pour surveiller les communications. Des pays peuvent profiter de conditions d'utilisation permissives et de leurs propres pouvoirs législatifs pour forcer le partage de données. Cette façon de faire menace la vie privée des communautés qui emploient ces applications.

● (1600)

[*Français*]

Les Canadiennes et les Canadiens qui ont des renseignements commerciaux confidentiels sur leurs appareils devraient faire particulièrement attention lorsqu'ils donnent accès à ces appareils.

[*Traduction*]

Les applications de messagerie instantanée et les plateformes de médias sociaux ne sont pas toutes équivalentes. Certaines plateformes sont plus responsables, et vous n'avez potentiellement pas à craindre que les données tombent entre les mains d'un État-nation. Cependant, d'autres plateformes sont trop près de cette ligne.

Le Centre pour la cybersécurité recommande fortement aux Canadiens et Canadiennes de prendre des décisions éclairées quant aux services en ligne qu'ils et elles sont prêts à utiliser.

[*Français*]

Effectuer ces évaluations et prendre ces décisions peut se faire facilement, et le Centre canadien pour la cybersécurité a publié des ressources en ligne afin de rendre le tout encore plus facile.

[*Traduction*]

Le Centre pour la cybersécurité recommande de faire des recherches sur toute application ou plateforme que vous comptez utiliser afin de déterminer si elle provient d'une source de confiance. On recommande en outre de lire les conditions générales d'utilisation. Mettez-vous au courant de ce que l'on dit d'une application en particulier dans les médias et d'autres sources fiables, et surtout, sachez ce à quoi vous consentez. Demandez-vous si une application a vraiment besoin d'accéder à vos renseignements personnels, comme votre liste de contacts. Il peut sembler inutile de consulter les fonctions de sécurité et de protection des renseignements personnels d'une plateforme, toutefois, c'est ainsi que vous éviterez d'utiliser des applications qui n'ont pas de mesures rigoureuses de protection des justificatifs d'identité, ce qui vaut amplement la peine.

[*Français*]

Enfin, ne sacrifiez jamais la sécurité pour la facilité. Découvrez où sont stockées vos données et quel impact cela pourrait avoir sur la protection de vos renseignements personnels.

[*Traduction*]

En conclusion, les médias sociaux ont changé la façon dont les Canadiennes et Canadiens communiquent, gardent contact et tissent de nouvelles relations.

[*Français*]

Alors que les menaces liées aux médias sociaux continuent d'évoluer, il faut s'assurer de prendre des décisions responsables et éclairées sur la meilleure façon de se protéger et de protéger ses renseignements en ligne.

[*Traduction*]

Renseignez-vous afin d'adopter de meilleurs moyens de protection de vos renseignements personnels et de votre sécurité, et sensibilisez les membres de votre famille et vos amis à ce sujet.

Je vous remercie encore de m'avoir invité à comparaître devant vous. Je répondrai à vos questions avec plaisir.

Le président: Merci, monsieur Khoury, de ces excellents conseils.

J'aimerais rappeler aux témoins de s'assurer de sélectionner la langue de leur choix, parce que nous allons poser des questions dans les deux langues.

Nous allons commencer par M. Barrett. Vous avez six minutes.

Allez-y, monsieur Barrett, s'il vous plaît.

M. Michael Barrett (Leeds—Grenville—Thousand Islands et Rideau Lakes, PCC): Merci beaucoup.

Combien y a-t-il de postes de police illégaux, au Canada?

Je pose ma question au SCRS, s'il vous plaît.

Mme Cherie Henderson: Pardon. J'ai dû chercher loin dans mes souvenirs.

Tout d'abord, je ne sais pas si je les appellerais vraiment des « postes de police ». Je pense que ce que nous avons vu, ces derniers mois, ce sont des personnes qui ont des liens avec la RPC ou qui appuient certaines des activités de la RPC. Souvent, il s'agit de personnes qui ont été récupérées. À un moment donné, il y en avait trois dans notre mire — les médias en ont parlé —, et la Gendarmerie royale du Canada, la GRC, a accordé toute son attention à ces postes de police.

Mais je ne voudrais pas commenter davantage les activités de la GRC.

M. Michael Barrett: D'après ce que vous savez, ces postes sont-ils toujours ouverts, ou les a-t-on fermés?

Mme Pam Damoff (Oakville-Nord—Burlington, Lib.): J'invoque le Règlement, monsieur le président.

Le président: Allez-y.

Mme Pam Damoff: Merci.

Notre étude porte sur les plateformes de médias sociaux. Je ne vois pas le lien entre notre étude et la question qui a été posée aux témoins.

Le président: Je suis certain que M. Barrett finira par faire le lien. Je comprends ce que vous voulez dire, mais il s'agit de son temps à lui, et je vais le laisser faire.

Poursuivez, monsieur Barrett.

M. Michael Barrett: Par rapport au rappel au Règlement, monsieur le président, ma question porte sur la répression transnationale. Je pense qu'il est important d'établir que des agents appartenant à des États étrangers travaillent dans ce but et de savoir quelles sont leurs activités. L'exemple dont je voulais parler avec les témoins concerne ces mêmes agents de l'État qui se livrent à la répression transnationale en utilisant les technologies des médias sociaux, dont certains ont justement été mentionnés dans les déclarations initiales.

Je ne sais pas dans quelle mesure je dois justifier mes questions. Je me ferai un plaisir d'en discuter davantage durant le temps du Comité, si vous le désirez, mais pas durant mes questions.

● (1605)

Le président: Merci.

Je tiens à dire aux membres du Comité que j'essaie généralement de donner à chacun et à chacune une bonne latitude, dans les cinq ou six minutes qui leur sont accordées ou peu importe le temps. Je m'attends à ce que M. Barrett fasse un lien, et son argument m'a convaincu. Vous pouvez poursuivre, monsieur Barrett.

J'avais arrêté le chronomètre. Il vous reste quatre minutes et 51 secondes. Poursuivez.

M. Michael Barrett: Pékin mène des activités de répression transnationale ici, en sol canadien — ces soi-disant postes de police, si vous voulez, en sont la preuve —, et cela veut dire que des Canadiens d'origine chinoise sont la cible d'intimidation et de pressions. C'est le but de ces soi-disant postes de police.

Mme Cherie Henderson: Je ne mettrais pas spécifiquement l'accent sur les soi-disant postes de police. Ce que je vous dirais, c'est qu'il y a indubitablement des activités d'ingérence étrangère ici, dans notre pays, mais ces activités prennent toutes sortes de formes et de visages. Si on met l'accent uniquement sur les postes de police, je crains que les gens perdent de vue tout ce qui arrive d'autre dans ce contexte.

M. Michael Barrett: Merci, je comprends.

Est-ce qu'on s'entend pour dire qu'une technique de la dictature de Pékin consiste à passer les médias sociaux au crible afin de repérer et de cibler les gens visés par des actes de répression? Est-ce que les médias sociaux sont un outil que ces agents, à ces endroits, utilisent pour recueillir du renseignement et ensuite cibler ces personnes?

Mme Cherie Henderson: Je trouve que c'est une question très intéressante, dont nous devons discuter.

Cela tient en grande partie à la manière dont les Canadiens — ou tout citoyen du monde, disons —, protègent leurs renseignements personnels. Si vous publiez ouvertement sur les réseaux sociaux de nombreux renseignements personnels, alors, absolument, les États hostiles pourront récolter ces données, de toute façon. Ce n'est pas seulement la Chine qui le fait. Il peut s'agir d'autres États hostiles. Je crois que c'est aussi très important. Vous perdez de vue toutes les activités hostiles menées contre les Canadiens si vous mettez l'accent seulement sur un seul acteur. Il est très important de protéger totalement l'accès à vos médias sociaux et aux données que vous y publiez.

Vous aviez absolument raison lorsque vous avez fait ce commentaire. Les États hostiles vont récupérer ces informations. Ils peuvent recueillir ces informations, traiter des données volumineuses et faire une surveillance très ciblée, s'ils le veulent.

M. Michael Barrett: Les acteurs des États étrangers ne prennent pas seulement pour cible les communautés de la diaspora de notre pays. Ils prennent également pour cible des représentants élus. Il y a eu des reportages dans les médias à ce sujet. Ces derniers mois, nous avons entendu des reportages concernant une campagne de « spamouflage » qui visait certains politiciens sur leurs réseaux sociaux.

A-t-on désigné la dictature de Pékin comme étant à l'origine de cette campagne?

Mme Cherie Henderson: Monsieur Khoury, pourriez-vous répondre à cette question-là?

M. Sami Khoury: Non, je ne peux pas, malheureusement.

Mme Cherie Henderson: Je ne suis pas certaine de pouvoir dire que l'on a remonté la piste jusqu'à la Chine. Il faudrait que je vérifie ce que nous savons à ce sujet.

Ce que je peux dire, c'est que, une fois de plus, vous avez tout à fait raison. Des gens obtiennent des données et prennent pour cible toute personne qu'ils croient devoir opprimer, sur laquelle ils veulent plus d'informations ou sur laquelle ils veulent faire pression en lien avec certaines activités.

Absolument, on peut utiliser les médias sociaux pour recueillir de l'information à ces fins.

M. Michael Barrett: Il s'agit d'activités d'ingérence étrangère. Même si on ne sait pas quel acteur d'un État étranger en est responsable, c'est de ces activités qu'il s'agit.

Mme Cherie Henderson: Je qualifierais cela d'activités d'ingérence étrangère, oui.

M. Michael Barrett: Pouvez-vous me dire combien de politiciens canadiens ont été pris pour cible par des acteurs d'États étrangers qui mènent ces activités d'ingérence, juste un chiffre, si possible?

Mme Cherie Henderson: Je ne pourrais vous donner un chiffre précis.

Une fois de plus, je dirais que tous les politiciens, tous les députés, devraient toujours protéger leurs renseignements personnels et leur vie privée et chercher à savoir si une personne ou une entité tente de les solliciter afin de mener une quelconque activité d'ingérence étrangère. Cela peut se faire de diverses manières.

M. Michael Barrett: Pouvez-vous me dire comment le mécanisme de réponse rapide a servi dans le cas du « spamouflage » visant des représentants élus?

Mme Cherie Henderson: Non, cela relève d'AMC. C'est Affaires mondiales qui gère le mécanisme de réponse rapide.

M. Michael Barrett: À quel moment comprenez-vous que le gouvernement est informé des tentatives d'acteurs d'États étrangers de prendre pour cible des Canadiens, y compris des politiciens canadiens? Est-ce que cela relève spécifiquement d'AMC ou bien notre organisme de sécurité nationale, le SCRS, intervient à un moment donné, étant évidemment au courant de ce qui se passe?

● (1610)

Mme Cherie Henderson: Oui, absolument.

Il y a quelques mois, le ministre de la Sécurité publique a émis une directive indiquant que, si le service apprend que des États étrangers hostiles mènent des activités nuisibles contre des politiciens, il doit examiner l'information, déterminer la gravité de la menace qu'elle représente, puis communiquer avec les différents acteurs politiques concernés et les conseillers.

Le président: Merci, monsieur Barrett et madame Henderson.

Madame Damoff, vous disposez de six minutes.

Allez-y, s'il vous plaît.

Mme Pam Damoff: Merci, monsieur le président.

Je remercie les deux organisations du travail qu'elles font pour assurer la sécurité des Canadiens. On ne reconnaît pas suffisamment le travail qu'elles font dans l'ombre, alors je tiens à remercier les deux organisations de tout ce qu'elles font.

Nous leur avons demandé de venir témoigner précisément au sujet de TikTok. Leurs représentants nous ont dit que les seules informations recueillies sont l'adresse électronique et l'âge. Je vais poser des questions au sujet de l'âge dans un instant. D'après vous, est-il exact de dire que ce sont bien là les informations recueillies en ligne au sujet des gens? Selon ce que je comprends, il est possible de recueillir beaucoup plus d'information en s'intéressant simplement à ce que les gens cherchent, et je les ai questionnés à ce sujet. On peut savoir qu'une personne a un problème cardiaque grâce aux recherches qu'elle a effectuées.

Je ne sais pas qui est le mieux préparé pour répondre à cette question. Monsieur Khoury, vous semblez prêt à y répondre.

M. Sami Khoury: Merci d'avoir posé la question.

Je crois qu'il est important de faire un peu la distinction entre l'information qu'il faut fournir pour ouvrir un compte sur TikTok et l'information qui est demandée pour améliorer l'expérience des utilisateurs. Il pourrait y avoir un plus grand accès, comme je l'ai souligné dans ma déclaration préliminaire, à votre liste de contacts, à votre calendrier ou à d'autres paramètres de confidentialité de votre téléphone, afin d'améliorer votre expérience d'utilisateur. C'est peut-être l'autre catégorie d'information partagée qui est recueillie par l'intermédiaire de TikTok.

Mme Pam Damoff: Ils ont affirmé catégoriquement qu'aucune information n'était transmise à la Chine et que les serveurs en question se trouvaient aux États-Unis, en Indonésie et en Malaisie, je crois.

Qu'est-ce qui a amené le gouvernement à interdire l'utilisation de TikTok sur ses appareils? Ce n'est pas une décision que vous auriez pu prendre à la légère.

M. Sami Khoury: La décision d'interdire TikTok sur les appareils du gouvernement a été prise par la dirigeante principale de l'information du Conseil du Trésor en raison du risque global, qui était jugé trop élevé. Du point de vue du gouvernement, le regroupement de toutes ces informations pouvait révéler nos contacts ainsi que nos activités au sein du gouvernement. Je soupçonne que, du point de vue de la protection de la vie privée, c'est ce qui a amené la DPI à adopter une politique pour interdire l'application dans les systèmes du gouvernement.

Mme Pam Damoff: J'aimerais parler des jeunes, parce que cela ne concerne pas seulement TikTok.

Ils ont dit qu'il existe toute sorte de mesures de protection pour empêcher les jeunes d'utiliser TikTok. Selon moi, il importe peu qu'il s'agisse de TikTok, d'Instagram ou des autres plateformes de médias sociaux; les jeunes partagent énormément de données sur leurs comptes de médias sociaux, et cela peut mener à l'exploitation.

J'aimerais tout d'abord avoir vos commentaires au sujet de l'exposition des jeunes aux réseaux sociaux et de la question de savoir si les plateformes en font suffisamment pour limiter leur exposition. De plus, que pouvons-nous faire, en tant que gouvernement, pour aider les jeunes à savoir ce qui se passe, étant donné qu'ils ne le savent pas, actuellement?

M. Sami Khoury: Une de nos préoccupations, au Centre pour la cybersécurité, est de mieux sensibiliser les utilisateurs aux menaces que représentent les réseaux sociaux et de les informer sur les paramètres de confidentialité et sur les meilleures façons d'utiliser ces applications; les utilisateurs ne doivent pas fournir volontairement trop de renseignements personnels et doivent s'assurer que les paramètres de confidentialité des applications leur sont adaptés autant que possible. Ils doivent savoir que l'endroit où les données sont hébergées et les personnes qui peuvent avoir accès aux données présentent un risque supplémentaire pour eux. En l'occurrence, les données hébergées dans certains pays pourraient présenter moins de risque que celles hébergées dans un pays comme la Chine ou ailleurs.

Notre rôle consiste essentiellement à éduquer et à mieux sensibiliser la population au sujet des menaces que présentent ces applications.

● (1615)

Mme Pam Damoff: Appuieriez-vous l'idée que les plateformes de réseaux sociaux présentent de manière plus conviviale pour les utilisateurs les conditions concernant la protection de la vie privée? Les conditions pourraient être rédigées dans un jargon juridique, mais les conditions que les gens acceptent pourraient être mises en évidence. Je parierais que 95 % des Canadiens ne lisent pas vraiment les conditions d'utilisation lorsqu'ils les passent en revue.

Pensez-vous que les plateformes devraient davantage avoir la responsabilité de simplifier ces conditions et de demander aux utilisateurs de consentir à la version courte et à la version longue?

M. Sami Khoury: Informer les Canadiens des conditions d'utilisation auxquelles ils consentent est absolument important. Nous pouvons expliquer ces conditions dans nos avis et conseils en matière de cybersécurité, mais, si elles sont également expliquées sur les applications individuelles dans une langue que les utilisateurs comprennent, afin qu'ils sachent exactement ce qu'ils acceptent de partager et avec qui, cela aiderait certainement tout le monde à savoir ce qui se passe en coulisses.

Mme Pam Damoff: Il me reste seulement 30 secondes environ.

Est-ce que l'un de vous deux aurait d'autres recommandations à nous faire que vous n'avez pas déjà faites, tout particulièrement en ce qui concerne les jeunes?

Mme Cherie Henderson: Je n'ai pas vraiment de recommandations à faire, mais j'aimerais revenir sur une chose que vous avez soulignée, c'est-à-dire la vulnérabilité de nos jeunes. Ce qui m'inquiète beaucoup, c'est que certains jeunes vont sur ces réseaux sociaux, se retrouvent parfois dans un milieu extrémiste et se font influencer de manière négative. C'est quelque chose qui devrait vraiment nous préoccuper et dont nous devrions être conscients. Ils créent des liens et entrent pour ainsi dire dans une chambre d'écho. C'est quelque chose dont nous devons être conscients.

Le président: Merci, madame Damoff, madame Henderson et monsieur Khoury.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

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

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

Madame Henderson, j'aimerais que vous nous donniez plus de détails sur les liens que vous avez faits entre l'ingérence étrangère, TikTok et les risques sur les plateformes.

Mme Cherie Henderson: Merci de la question. Je vais y répondre en anglais.

[*Traduction*]

J'aimerais donner des explications plus détaillées sur le fait que bien des personnes vont sur les plateformes de réseaux sociaux et partagent beaucoup d'information. Comme mon collègue, M. Khoury, l'a souligné, il s'agit parfois des choses que cette personne aime, et parfois, des pages auxquelles elle est abonnée. Toutes ses vidéos ou ses photos pourraient se retrouver sur les réseaux sociaux. Les acteurs étrangers qui ont des intentions hostiles peuvent rassembler toutes ces informations et avoir une très bonne idée de qui vous êtes et de la manière dont ils peuvent vous influencer.

Par ailleurs, nous constatons que les réseaux sociaux semblent être un bon endroit pour remarquer et observer les tendances. Si un acteur étranger veut savoir quelle tendance suit une région donnée, il n'a qu'à surveiller ce qui se passe sur les réseaux sociaux: Pour qui les gens votent-ils? De quoi les gens s'inquiètent-ils ou se préoccupent-ils? Quelles informations trompeuses ou erronées consultent-ils? C'est pourquoi je dis qu'il s'agit d'outils puissants qui peuvent réellement servir à faire du tort et à mener des activités d'ingérence étrangère.

[*Français*]

M. René Villemure: Si je comprends bien, afin de ne pas partager ces renseignements, il faut avoir lu les conditions et avoir consenti à ne pas partager ses renseignements personnels.

Une fois que les gens ont commencé à utiliser une plateforme de média social, est-il trop tard pour faire marche arrière?

[*Traduction*]

Mme Cherie Henderson: Je crois qu'il n'est jamais trop tard pour faire marche arrière, mais je dirais que, dans certains cas, le mal est déjà fait. Il faut s'en inquiéter, quand même, mais les gens changent avec le temps. Si vous arrêtez de partager des renseignements personnels ou que vous faites plus attention à ce que vous partagez, même à partir d'aujourd'hui, je crois que vous commencerez à protéger votre présence sur les médias sociaux.

[*Français*]

M. René Villemure: Vous mentionnez que la Chine n'est pas le seul acteur qui mène des activités d'ingérence étrangère. De quels réseaux faudrait-il particulièrement se méfier, autres que TikTok? Auxquels faudrait-il faire très attention, et à quels pays sont-ils reliés?

[*Traduction*]

Mme Cherie Henderson: Je déteste devoir tout ramener à une seule chose, parce que je crains que les gens ne se concentrent que sur les auteurs de menace.

Je crois que tout le monde ici sait déjà que l'autre acteur qui nous inquiète est la Russie. Nous sommes également préoccupés par l'Iran et la Corée du Nord. Ces pays se trouvent en tête de liste à l'heure actuelle, mais je dirais que vous devez envisager les choses de façon encore plus générale et toujours protéger ce qui se trouve sur vos comptes de médias sociaux. On ne sait jamais qui regarde et qui tente de recueillir plus de renseignements à votre sujet.

● (1620)

[*Français*]

M. René Villemure: Merci beaucoup de votre réponse.

Quand on pense à TikTok, on pense à la Chine. Quand on pense à la Russie, à l'Iran et à la Corée du Nord, à quoi doit-on les associer? Quels sont les réseaux auxquels on pourrait associer ces trois acteurs étrangers?

[*Traduction*]

Mme Cherie Henderson: Je ne connais pas moi-même tous les réseaux de ces pays précis.

Une fois de plus, en tant que citoyen innocent qui crée des comptes sur des réseaux sociaux, vous devez tenter d'en connaître la provenance. Plus les Canadiens se tiennent informés, plus ils se protègent. Vous pourriez penser qu'un compte ne vient pas d'un État qui pourrait nous préoccuper, mais, si vous creusez un peu plus, il se peut que ce soit le cas.

Je vous conseillerais de toujours vérifier deux fois pour être certain de savoir exactement à quoi vous consentez et avec qui vous le faites, du mieux que vous pouvez.

[*Français*]

M. René Villemure: J'imagine que les adolescents de 14 ou 15 ans n'ont pas le souci de vérifier l'usage final ou la destination de leurs données. Comme on le sait, le formulaire de consentement n'est pas lu et il est complexe. On ne connaît pas la destination des données.

Comment peut-on les protéger? Comment peut-on aider les jeunes et les plus jeunes à mieux comprendre ce qui est en jeu, afin qu'ils ne partagent pas leurs données avec imprudence?

[*Traduction*]

Mme Cherie Henderson: Je pense que c'est une très bonne question, et c'est difficile d'y répondre.

Je pense que cela revient beaucoup à ce que mon collègue, M. Khoury, a dit, c'est une question d'éducation — d'éducation continue. Il ne faut pas seulement éduquer les adultes, mais il faut éduquer les personnes de tout âge. Je ne m'occupe pas des politiques; je préfère agir, mais je crois qu'il serait très important de trouver des façons d'éduquer les jeunes et de s'investir dans ce dossier. Je pense que d'autres ministères peuvent appuyer ce genre de travail.

[*Français*]

M. René Villemure: Monsieur Khoury, je vous pose la même question.

M. Sami Khoury: Merci.

Comme vient de le mentionner ma collègue, l'éducation est super importante pour informer les jeunes. En réalité, il est sûr que le cas de la Chine soulève des soucis un peu plus complexes.

Toute l'information que nous mettons dans le domaine public pourrait ultimement être source d'inquiétude. Il est important d'informer les jeunes et les moins jeunes des risques qu'une publication de ce genre d'information peut avoir dans les années à venir. Il ne s'agit peut-être pas d'un risque immédiat, mais cela peut présenter un risque plus tard, une fois qu'une image un peu plus complète de l'individu ou du profil aura été formulée.

Le président: Merci, messieurs Khoury et Villemure.

[*Traduction*]

Monsieur Green, vous avez six minutes; allez-y.

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

Je vais vous poser une série de questions.

Tout d'abord, merci d'être ici. C'est toujours un plaisir pour moi, qui vient de la classe ouvrière de Hamilton, de pouvoir poser des questions au CST et au SCRS. C'est vraiment génial.

Je vais vous poser directement des questions, et j'aimerais que vos réponses soient les plus directes possible.

Le 27 février 2023, le gouvernement du Canada a annoncé qu'il interdisait l'utilisation de l'application TikTok sur les appareils mobiles gouvernementaux. Le Centre de la sécurité des télécommunications a-t-il été consulté lorsque la décision a été prise?

Je m'adresse à vous, monsieur Khoury.

M. Sami Khoury: Oui.

M. Matthew Green: Le SCRS a-t-il été consulté lorsque la décision a été prise?

Mme Cherie Henderson: Je ne sais pas.

M. Matthew Green: D'accord.

Pendant les consultations, qu'avez-vous dit au gouvernement sur le fait qu'il voulait interdire précisément TikTok?

M. Sami Khoury: Nous ne sommes pas un organisme de réglementation et nous n'évaluons pas toutes les applications existantes. Nos conseils concernent la façon d'évaluer les risques pour la vie privée des réglages permissifs demandés par l'application.

En plus de discuter de l'interdiction de TikTok, nous avons aussi donné des avis et des conseils sur les applications de médias sociaux aux Canadiens et aux entreprises canadiennes en général.

M. Matthew Green: En ce qui concerne l'interdiction et le gouvernement, il me semble que votre justification est solide. Vous avez parlé d'un niveau de risque acceptable, or toute l'attention semble être portée sur le fait qu'il s'agit d'un acteur appartenant à l'État par l'intermédiaire de ByteDance.

Je voudrais vous poser une question au sujet du capitalisme de surveillance et de données ou du capitalisme d'algorithmes. En d'autres termes, qu'est-ce qui empêche Facebook, X ou Twitter ou d'autres plateformes de tout simplement recueillir les mêmes données et de les vendre par l'intermédiaire d'une tierce partie à ces mêmes acteurs hostiles que vous avez identifiés?

● (1625)

M. Sami Khoury: Juste au cas où je n'ai pas été clair, TikTok présente un niveau de risque inacceptable. C'est pour cette raison que l'application a été interdite.

M. Matthew Green: Qu'est-ce qui est acceptable?

M. Sami Khoury: Le niveau de risque de nombreuses applications qui se trouvent sur nos téléphones gouvernementaux est jugé acceptable. Pour donner des avis et des conseils sur ce que nous téléchargeons nos téléphones gouvernementaux, nous étudions un certain nombre de choses, comme le contrôle de sécurité et le créateur de l'application.

M. Matthew Green: Depuis que vous travaillez pour le CST... Vous travaillez pour eux depuis combien d'années?

M. Sami Khoury: Cela fait 32 ans.

M. Matthew Green: Vous étiez là en 2016, et en 2019, en particulier, lorsque l'enquête conjointe du commissaire à la protection de la vie privée a mis en lumière le scandale Facebook-Cambridge Analytica.

M. Sami Khoury: Je travaillais pour le CST. Je n'occupais pas le rôle que j'occupe actuellement, mais je travaillais bien pour le CST.

M. Matthew Green: Donniez-vous aussi des conseils à ce sujet? Étiez-vous aussi au courant de la situation?

M. Sami Khoury: Cela ne faisait pas partie de mes fonctions.

M. Matthew Green: Vous vous rappelez, n'est-ce pas, que ce cabinet d'experts-conseils anglais, Cambridge Analytica, a accédé à 87 millions de profils et a recueilli leur information. Il est intervenu dans le Brexit, tout comme dans la campagne de Trump.

Savez-vous s'il est intervenu dans la politique canadienne?

M. Sami Khoury: Je ne sais pas.

M. Matthew Green: D'accord.

Vous ne devez donc pas savoir que, en 2016, le bureau de recherche du Parti libéral a retenu les services d'Eunoia Technologies, et de Christopher Wylie, l'un des fondateurs de Cambridge-Analytica, pour un projet pilote. C'est lui qui a sonné l'alarme.

Étiez-vous au courant?

M. Sami Khoury: Non, pas du tout.

M. Matthew Green: Ne seriez-vous pas préoccupé par le fait que le fondateur de Cambridge Analytica, entreprise qui a été impliquée plus tard dans un scandale important en lien avec la campagne de Trump et le Brexit, a fourni des services contractuels à un parti politique canadien, alors que, dans les analyses des menaces, Facebook n'est jamais mentionné? Comment cela se fait-il?

M. Sami Khoury: Notre rôle, au Centre pour la cybersécurité, est de nous assurer d'exposer les menaces et d'éduquer les Canadiens et les organisations canadiennes à propos des menaces. Nous les invitons à se poser des questions sur la façon de protéger...

M. Matthew Green: Respectueusement, je ne suis qu'une personne de la classe ouvrière de Hamilton, et il ne m'a fallu que 10 minutes de recherches sur Google pour trouver cette information. Vous travaillez pour le CST. Comment se fait-il que, quand vous faites une analyse des menaces des médias sociaux, vous ne relevez pas la menace de ce que j'appellerais le capitalisme des algorithmes, la collecte et la vente d'informations à des fins politiques, qui saperaient les processus démocratiques? Je trouve cela stupéfiant, pour être tout à fait franc avec vous, parce que, lorsque vous parlez d'un niveau de risque acceptable, nous avons vu les conséquences du Brexit et de M. Trump.

Cambridge Analytica et Facebook, l'entreprise de Mark Zuckerberg, ont dû comparaître devant le Congrès des États-Unis et payer des amendes en Europe pour avoir interféré dans les processus politiques. Pourtant, les seules menaces dont nous parlons sont liées à des acteurs appartenant à l'État, non pas à des entreprises, lesquelles sont souvent hostiles et, franchement, beaucoup plus dangereuses lorsqu'il est question de surveiller les différentes diasporas. J'ai parlé des façons dont les régimes dictatoriaux ciblent leurs populations civiles ici.

Je vais vous poser une question. Quand vous faites vos analyses des menaces, tenez-vous compte de toutes les autres plateformes et de tous les autres moyens par lesquels le capitalisme des algorithmes peut acheter et vendre nos informations et saper les institutions démocratiques?

M. Sami Khoury: Nous tenons bien sûr compte de tout cela dans notre évaluation des menaces, mais lorsque nous publions nos avis et nos conseils, nous posons une série de questions et encourageons chaque Canadien et chaque organisation canadienne à...

M. Matthew Green: Je parle de l'interdiction d'une application sur les appareils gouvernementaux. Je ne parle pas de vos relations publiques. Cela ne m'intéresse pas.

Nous sommes ici pour discuter d'un sujet très précis; pour ma part, j'aimerais savoir pourquoi nous interdisons un seul média social et pas tous les médias sociaux. Ne seriez-vous pas d'accord pour dire que Facebook, Twitter et Instagram ont eux aussi amplement les moyens de recueillir nos données, contrôler ce que nous aimons, nous diriger vers certaines sources de nouvelles, créer des chambres d'écho et, en fin de compte, créer des profils sur nous?

N'ai-je pas raison?

● (1630)

Le président: Répondez rapidement.

M. Sami Khoury: Monsieur le président, quand vous partagez de l'information, elle peut être extraite, peu importe à qui profite cette fuite de données.

Le président: Merci, monsieur Green.

Merci, monsieur Khoury.

Cela conclut la première série de questions.

[*Français*]

Monsieur Gourde, vous avez cinq minutes.

M. Jacques Gourde (Lévis—Lotbinière, PCC): Merci, monsieur le président.

Je remercie les témoins d'être ici. Il est rare d'avoir la chance d'accueillir des témoins avec des niveaux élevés de responsabilité comme eux. Merci de travailler pour la sécurité du Canada.

Je reviens sur l'ingérence étrangère au cours des élections de 2019 et de 2021. Est-ce que vos services avaient la capacité de déceler cette ingérence pendant ces élections?

M. Sami Khoury: Je vais commencer à répondre et j'inviterai ensuite ma collègue à poursuivre.

Le rôle du Centre canadien pour la cybersécurité est de collaborer avec Élections Canada pour s'assurer que les infrastructures électorales sont bien protégées. C'est ce que nous avons fait durant les élections de 2021.

M. Jacques Gourde: Je cherchais à savoir si vous aviez décelé de l'ingérence étrangère, soit des messages envoyés sur les médias sociaux qui ne venaient pas d'un parti politique ou d'une entité politique, mais qui venaient carrément de l'étranger.

M. Sami Khoury: Notre rôle ne consiste pas à examiner le contenu des messages échangés. Notre rôle principal est de protéger les infrastructures.

M. Jacques Gourde: Si je comprends bien, vous n'avez pas pu déceler l'ingérence étrangère. Si vous aviez pu le faire, auriez-vous été capables de bloquer cette information? Auriez-vous pu dire que cette information était de l'ingérence étrangère et de ne pas la consulter? Avez-vous la capacité de faire ça?

Pendant l'élection, des candidats ont vu qu'il y avait des messages venant de nulle part. Ils pouvaient les lire. Si, pendant une période électorale, les Canadiens peuvent voir ces messages, mais que vous me dites que vous ne pouvez pas les voir, j'ai un problème avec ça. En principe, vous êtes là pour faire de la surveillance. Expliquez-moi pourquoi vous ne voyez pas ces messages, mais les Canadiens moyens les voient.

M. Sami Khoury: Je vais clarifier quelque chose. Nous ne voyons pas les contenus parce que nous n'avons pas le mandat de les voir. Le rôle du Centre canadien pour la cybersécurité, son mandat, est de protéger les infrastructures et non d'aller voir les contenus. De toute évidence, nous nous préoccupons de la sécurité des infrastructures, mais aussi des indices d'ingérence. Notre objectif est d'apprendre aux Canadiens comment s'informer le mieux possible et où aller chercher l'information des sources les plus crédibles. En général, nous nous concentrons là-dessus.

M. Jacques Gourde: Merci.

À quelle date avez-vous été mis au courant, après les élections de 2019 et de 2021, qu'il y avait eu de l'ingérence étrangère pendant la campagne électorale?

M. Sami Khoury: Malheureusement, je n'ai pas de date en tête. Excusez-moi.

M. Jacques Gourde: Madame Henderson le saurait-elle?

[*Traduction*]

Mme Cherie Henderson: Je peux peut-être répondre. Merci.

Tout d'abord, je vais commencer par dire que l'ingérence étrangère ne se produit pas seulement lors d'une élection. Il y en a tout le temps, tous les jours, et je pense qu'il faut garder cela à l'esprit, parce que, quand vous décidez de vous pencher sur une période électorale, qui est bien définie dans le temps, vous n'allez pas toujours repérer l'ingérence étrangère sur le fait. Nous surveillons ce qui se passe tous les jours, avant une élection, et nous surveillons constamment la situation pour déceler une quelconque forme d'ingérence étrangère par un acteur hostile relevant de l'État.

Lorsque vous étudiez une période précise et que vous avez affaire avec une possible attaque sur les médias sociaux, trouver le point d'origine de l'attaque prend beaucoup de temps. Pour trouver le pays d'origine de l'attaque ou son auteur, il ne suffit pas d'appuyer sur un bouton. Cela prend beaucoup de temps aux services du renseignement pour faire le nécessaire et retracer l'origine de l'attaque.

Aussi, je dois dire que nous ne surveillons pas les médias sociaux. Vous ne voulez pas que votre service national de renseignements surveille tous les médias sociaux. Nous devons d'abord nous assurer que la menace sur les médias sociaux est réelle avant d'agir en vertu de notre mandat.

[*Français*]

M. Jacques Gourde: Merci.

J'ai une dernière question. Savoir d'où vient l'attaque, c'est une chose, mais c'en est une autre de savoir que l'attaque peut influencer les Canadiens et qu'elle est illégale parce que le message ne vient pas d'Élections Canada ou qu'il n'est pas conforme à la Loi électorale du Canada. Les Canadiens sont habitués à participer au processus électoral. Quand une telle attaque survient, elle devrait être décelée et condamnée, et il devrait y avoir moyen de dire qu'il s'agit d'une attaque et qu'il ne faut pas tenir compte de ce genre de messages venant de l'étranger. Est-il possible de le faire?

● (1635)

Le président: Je demanderais aux témoins de répondre brièvement.

[*Traduction*]

Mme Cherie Henderson: Nous devons aussi préserver la liberté d'expression. Nous devons éduquer tout le monde et nous assurer de préserver la liberté d'expression, mais il faut aussi, en même temps, éduquer les gens à propos de l'ingérence étrangère. C'est une situation très complexe. Il ne s'agit pas seulement de déterminer que, oui, cela provenait de l'étranger; nous devons aussi nous assurer que cela a une incidence sur notre souveraineté et notre sécurité nationale. Puis, nous commençons à éduquer les gens à ce sujet, partout.

Le président: Merci, madame Henderson.

[*Français*]

Merci, monsieur Gourde.

[*Traduction*]

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

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

Merci aux témoins de s'être joints à nous aujourd'hui. J'aimerais moi aussi vous remercier pour le travail que vous faites pour protéger les Canadiens et les Canadiennes.

Madame Henderson, pour en revenir à ce dont vous avez brièvement parlé, je suis père d'un adolescent et d'un préadolescent. Nous nous préoccupons tous des jeunes de notre pays. Nous avons appris avec le temps que des pays étrangers comme la Russie travailleront longtemps pour tenter d'influencer toute une génération. Vous avez aussi mentionné que des gens déploient des efforts pour influencer toute une génération.

Est-ce que d'autres pays hostiles suivent maintenant cette pratique dont vous avez parlé, la Chine, la Russie, l'Iran ou la Corée du Nord? Font-ils des imitations? Croyez-vous que d'autres applications sont en cours de développement et qu'elles auront autant d'influence que TikTok? Le siège social de TikTok et de tous ces autres médias sociaux sont situés à l'extérieur de l'Amérique du Nord, mais les applications sont utilisées mondialement. Surveillez-vous le développement d'autres applications que nous ne connaîtrions pas encore?

Mme Cherie Henderson: Nous ne surveillons pas nécessairement le développement de plateformes de médias sociaux. Cela revient un peu à ce que j'ai dit plus tôt, que je craigne de mettre l'accent sur une ou deux plateformes précises seulement. Je pense qu'il est vraiment important de commencer à éduquer tout le monde à propos de la bonne hygiène sur les médias sociaux. Je ne sais pas si cela se dit vraiment, mais je vais appeler cela ainsi. Je pense qu'il est primordial que chaque personne soit responsable de ce qu'elle partage et qu'elle soit bien au courant du coût et des conséquences de ses choix.

Par conséquent, si les gens sont renseignés et prudents, ils savent à quoi s'attendre, même s'il y a d'autres plateformes de médias sociaux. Ils se protègent. Cela n'a pas d'importance si une autre plateforme est créée, parce que, encore une fois, ils ont de bonnes pratiques d'hygiène sur les médias sociaux.

M. Parm Bains: Merci.

Monsieur Khoury, le CST signale aussi au gouvernement les activités étrangères qui menacent la prospérité et la sécurité, y compris les cybermenaces, l'espionnage, le terrorisme et les enlèvements. Est-ce que des renseignements sur ces sujets sont aussi recueillis sur les plateformes de médias sociaux?

M. Sami Khoury: En tant que dirigeant principal du Centre pour la cybersécurité, je suis ici pour vous parler du contexte des menaces telles que nous le percevons. Ces menaces sont éclairées par différentes sources. Certaines sources sont publiques, d'autres sont classifiées. D'une certaine façon, lorsque nous repérons quelque chose, nous allons au fond de l'affaire et communiquons l'information, peu importe la source.

M. Parm Bains: D'accord.

Avez-vous pu regarder la réunion du Comité du 18 octobre, lorsque des représentants de TikTok ont comparu? Si oui, qu'avez-vous pensé de leur témoignage? Ils avaient l'impression d'être ciblés injustement. Avez-vous été convaincu par leur témoignage sur les préoccupations liées à la sécurité, à la vie privée et aux données? Aviez-vous des préoccupations quant à leur utilisation de l'information partagée à des tierces parties?

M. Sami Khoury: Malheureusement, je n'ai pas regardé les témoignages de cette date-là.

● (1640)

M. Parm Bains: D'accord. Nous leur avons posé plusieurs questions concernant le fait que des tierces parties avaient accès à de l'information. Les représentants de TikTok avaient l'impression d'être ciblés injustement. Trouvez-vous préoccupant qu'une entité comme TikTok précisément soit en mesure de donner à des tierces parties accès à de l'information partagée?

M. Sami Khoury: Nos préoccupations sont les suivantes: Qui a accès aux données? Où les données sont-elles conservées? À quel point est-il facile pour le pays d'accueil d'obtenir l'accès aux données? C'est ce que nous demandons à savoir. Tous ceux qui utilisent une application de médias sociaux devraient se poser ces questions afin d'être des utilisateurs mieux renseignés au sujet des médias sociaux. Dans le cas de TikTok, si les données sont hébergées en Chine, ce serait une préoccupation, compte tenu de certaines lois permissives de la Chine concernant l'obtention de l'accès aux données des utilisateurs.

Nous voulons que les Canadiens se posent ces questions difficiles au sujet des paramètres de sécurité afin d'être des consommateurs mieux renseignés.

Le président: Merci, monsieur Bains et monsieur Khoury.

[*Français*]

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

M. René Villemure: Merci, monsieur le président.

Madame Henderson, tantôt, vous avez dit qu'il fallait s'éduquer sur tous les dangers potentiels relatifs aux médias sociaux. Or, M. et Mme Tout-le-Monde ne savent pas où se trouvent les serveurs où vont nos données et quels sont les risques. Au Comité, nous sommes un peu plus informés, mais il reste que, dans la population générale, personne ne connaît cela. Alors, où doit-on faire cette éducation?

Mme Cherie Henderson: Merci de cette question très importante.

[*Traduction*]

Je pense que l'éducation doit se faire à tous les niveaux.

Encore une fois, je ne suis pas une spécialiste des politiques. Je suis une mère, et j'aimerais m'assurer que mes enfants reçoivent une éducation à l'école, dans les centres communautaires et de manière générale. Il faut commencer à avoir une plus grande participation, mais je parle en tant que mère, et non pas en tant qu'agente de sécurité.

Je pense que nous devons absolument avoir ce volet d'éducation. C'est d'une importance capitale.

[*Français*]

M. René Villemure: Vous avez beaucoup parlé d'ingérence étrangère. Tantôt, vous avez dit que vous n'aimiez pas cibler qui que ce soit en particulier, mais, dans la minute et demie qu'il nous reste, pouvez-vous nous dire ce que nous, en tant que comité, devrions savoir au sujet de l'ingérence étrangère, mais que nous ne savons pas?

Le président: À qui posez-vous la question, monsieur Villemure?

M. René Villemure: Je m'adresse toujours à Mme Henderson.

[*Traduction*]

Mme Cherie Henderson: L'ingérence étrangère est une chose sur laquelle nous nous sommes penchés au Service. J'y travaille depuis 32 ans. Dès mon premier jour, nous avons enquêté sur l'ingérence étrangère. C'est quelque chose que l'on voit dans notre pays depuis des dizaines d'années.

Les Canadiens sont devenus très complaisants et à l'aise dans leur environnement. Je pense que nous devons être beaucoup plus au courant de ce qui se passe autour de nous. C'est quelque chose que l'on voit beaucoup plus avec l'avènement des médias sociaux et la technologie avec laquelle nous devons composer. Nous sommes exposés à un risque en raison des activités d'États hostiles. Ils veulent saper notre souveraineté et nos institutions démocratiques. Il est fondamentalement important de protéger la sécurité nationale et l'avenir de notre pays. Nous devons prendre les précautions nécessaires, en conscientisant et en éduquant les gens, afin de nous protéger et de protéger nos systèmes dans l'avenir.

[*Français*]

M. René Villemure: Merci.

[*Traduction*]

Le président: Monsieur Green — d'un ouvrier de Barrie à un ouvrier de Hamilton —, vous avez deux minutes et demie.

M. Matthew Green: Je vous suis reconnaissant. Merci beaucoup.

J'aimerais revenir sur vos avis publics, monsieur Khoury. Vous avez mentionné que vous fournissez des avis généraux au sujet des médias sociaux. Je note qu'un article de janvier 2023 de CBC annonçait ceci: « Le CST n'a pas publié d'avis contre l'utilisation de TikTok ».

Avez-vous, à ce jour, publié un avis contre l'utilisation de TikTok?

M. Sami Khoury: Dans le cadre de notre rôle, nous ne publions pas d'avis concernant des applications particulières. Nous communiquons des avis et des orientations au sujet des médias sociaux en général.

M. Matthew Green: Avez-vous conseillé au Conseil du Trésor d'interdire l'utilisation de TikTok lorsqu'il enquêtait sur cette question?

M. Sami Khoury: C'est une décision qui appartient à la dirigeante principale de l'information du Canada.

M. Matthew Green: Vous ne lui avez pas conseillé de l'interdire.

● (1645)

M. Sami Khoury: Nous intervenons dans la décision. Nous faisons partie de la table ronde avec le Conseil du Trésor.

M. Matthew Green: Lui avez-vous, à tout moment, conseillé d'interdire l'utilisation de TikTok?

M. Sami Khoury: Non.

M. Matthew Green: Je vous remercie.

Monsieur Madou, j'ai remarqué que Mme Henderson n'avait pas la réponse à ma question.

Le SCRS a-t-il été consulté lorsque le gouvernement a décidé d'interdire l'utilisation de TikTok?

M. Peter Madou (directeur général, Évaluation des renseignements, Service canadien du renseignement de sécurité): Pas à ma connaissance.

M. Matthew Green: Avez-vous, à un moment donné, conseillé au gouvernement d'interdire l'utilisation de TikTok sur les téléphones du gouvernement?

M. Peter Madou: Nous fournissons au gouvernement des conseils sur l'ingérence étrangère de manière générale. Je ne suis pas au courant du fait que nous ayons émis des conseils expressément au sujet de cette plateforme de médias sociaux.

M. Matthew Green: Je suis toujours frappé par le fait que cette plateforme de médias sociaux, compte tenu de toutes les controverses entourant toutes les autres, ait été ciblée. J'ai l'impression qu'il s'agit d'une décision politique, et non pas d'une décision fondée sur des données probantes. C'est mon opinion. Ce n'est pas la vôtre.

En ce qui concerne les menaces, vous avez le mandat d'enquêter sur les menaces à la sécurité nationale. À quelle fréquence le SCRS enquête-t-il sur les activités des plateformes de médias sociaux en ce qui concerne les menaces à la sécurité nationale, monsieur Madou?

M. Peter Madou: Nous enquêtons sur les auteurs de menace; nous n'enquêtons pas sur les plateformes de médias sociaux. En fonction de l'évolution des auteurs de menace, nous pouvons avoir une idée de ce qui se passe sur une plateforme, mais sinon, nous enquêtons sur les auteurs de menace.

M. Matthew Green: À quelle fréquence détectez-vous la présence de services d'ingérence étrangère sur les plateformes de médias sociaux?

Le président: Je suis désolé, monsieur Madou. Si vous pouviez vous rapprocher un peu du microphone pour parler, cela aiderait les interprètes.

Je vous remercie, veuillez poursuivre.

M. Peter Madou: Merci.

Pouvez-vous simplement répéter la question?

M. Matthew Green: À quelle fréquence le SCRS détecte-t-il la présence de services ou d'acteurs participant à l'ingérence étrangère sur les plateformes de médias sociaux?

M. Peter Madou: Je pense que la détection de contre-discours sur les plateformes de médias sociaux est un phénomène courant, mais qu'il est un peu plus complexe de les relier précisément à un auteur de menace hostile. Je ne sais pas à quelle fréquence cela se produit. Nous savons que les auteurs de menace le font — comme la RPC, la Russie ou d'autres auteurs de menace hostiles, comme mon collègue l'a mentionné — mais je n'ai pas de chiffre précis à vous donner.

M. Matthew Green: Merci.

Le président: Merci, monsieur Green.

Monsieur Kurek, vous avez trois minutes, s'il vous plaît. La parole est à vous.

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

Merci à nos témoins d'être ici.

Dans la foulée de l'attaque du 7 octobre contre des citoyens israéliens, une organisation terroriste a diffusé une information que le premier ministre, la ministre des Affaires étrangères, d'autres membres du gouvernement et d'autres partis politiques ont communiquée: les Forces de défense israéliennes avaient bombardé un hôpital. Cette information s'est répandue comme une traînée de poudre sur tous les médias sociaux, mais a très vite été considérée comme catégoriquement fausse. Nos alliés du Groupe des cinq savaient qu'il s'agissait de désinformation, mais notre gouvernement a refusé de se rétracter. C'est un exemple.

Madame Henderson, pouvez-vous nous expliquer comment ce type d'action du gouvernement contribuerait à l'érosion de la confiance et nous faire part de certains des défis associés aux médias sociaux et à l'influence que les États étrangers pourraient avoir sur la population canadienne?

Mme Cherie Henderson: Je ne suis pas sûre de savoir ce que vous me demandez. Je suis désolée.

M. Damien Kurek: Lorsque le premier ministre et la ministre des Affaires étrangères ont refusé de démentir les informations erronées, ils ont contribué à la diffusion rapide de ces fausses informations en ligne. Je sais qu'elles sont apparues dans mon fil d'actualité et qu'elles m'ont été transmises par des électeurs.

Lorsque les gouvernements tardent à réagir pour lutter contre la désinformation, cela contribue-t-il à favoriser des acteurs étatiques étrangers et à renforcer l'influence qu'ils peuvent avoir sur les Canadiens?

Mme Cherie Henderson: Pour répondre à cette question, je dirais que, dans toute situation, tout auteur de menace étranger surveille toujours tout ce qui se passe dans un pays d'intérêt. Il captera le moindre élément d'information et l'amplifiera pour en faire de la désinformation ou de la fausse information afin d'atteindre son objectif. Il continuera d'amplifier cette information jusqu'à ce qu'il estime que le mal est fait.

M. Damien Kurek: Je vous remercie. Certes, il est essentiel de lutter contre la désinformation.

Il y a un décalage entre ce que TikTok a communiqué au Comité pour ce qui est des paramètres de confidentialité qui peuvent être présents sur un téléphone et la zone grise des médias sociaux, où des renseignements inconnus peuvent être recueillis.

Dans les 45 secondes qu'il me reste, je me demande, madame Henderson, si vous pouvez nous dire comment nous pouvons concilier le décalage qui existe entre ce que les entreprises de médias sociaux disent, ce que nous entendons dire aujourd'hui et ce qui a été rapporté dans les médias.

Mme Cherie Henderson: Je vais répondre en disant qu'il y aura toujours, comme vous l'avez signalé, une zone grise. Il y a la politique et il y a ce que les médias sociaux recueillent et mobilisent intentionnellement, notamment — comme ils l'ont indiqué — les adresses de courriel. Cependant, comme M. Khoury l'a mentionné plus tôt, il ne s'agit pas seulement de l'adresse de courriel avec laquelle vous vous êtes inscrit; tout ce que vous faites en tant qu'individu sur ce site constitue également des données qui peuvent être recueillies. C'est ce que nous appelons, dans de nombreux cas, les mégadonnées. Ils recueillent toutes ces mégadonnées et peuvent faire du traitement de données.

C'est là une partie du danger, et c'est là qu'ils peuvent commencer à dégager des tendances quant à la façon dont ils peuvent s'ingérer et influencer.

● (1650)

Le président: Merci, madame Henderson.

Monsieur, monsieur Kurek.

Monsieur Kelloway, vous avez trois minutes pour terminer.

M. Mike Kelloway (Cape Breton—Canso, Lib.): Merci, monsieur le président.

Puis-je partager mon temps avec Pam Damoff, s'il vous plaît, pour les 30 premières secondes?

Mme Pam Damoff: Je n'ai besoin que de quelques secondes. Je voulais clarifier quelque chose que M. Kurek a dit.

Le gouvernement canadien a examiné lui-même l'information sur l'attentat à la bombe à l'hôpital. Le premier ministre, de façon très catégorique, à la Chambre des communes et ailleurs, a confirmé que ce n'est pas Israël qui a bombardé l'hôpital. En fait, je me rappelle que les collègues conservateurs se sont levés et ont applaudi lorsqu'il a dit cela à la Chambre.

Je veux m'assurer que le compte rendu reflète bien que nous avons mené notre propre enquête, monsieur le président. Nous avons effectivement dénoncé la désinformation.

Je vais céder la parole à M. Kelloway.

M. Damien Kurek: J'invoque le Règlement.

Monsieur le président, je note que c'était cinq jours après que l'information a été communiquée.

Le président: Allez-y, monsieur Kelloway. Merci.

M. Mike Kelloway: Merci, monsieur le président, d'un ouvrier à un autre, il faut que cette tendance se poursuive.

Je suis vraiment reconnaissant du travail que vous faites. Je ne peux pas imaginer le travail que vous faites. J'ai tellement de questions à vous poser, mais dans le temps qui m'est imparti, je ne pourrais pas vous rendre justice.

L'éducation est un élément en particulier qui revient toujours. En tant qu'éducateur, j'aimerais expliquer ce que cela signifie vraiment. Comme vous l'avez mentionné, le dentifrice n'est peut-être plus dans le tube, mais que faisons-nous?

Je vais essayer de ramener tout cela à une chose fondamentale. Pour ce qui est de la radicalisation des jeunes sur TikTok ou d'autres plateformes par des entités étrangères, pouvez-vous nous donner des précisions? Pouvez-vous essayer de quantifier la gravité de ce phénomène, au mieux de vos capacités?

Cette question s'adresse à l'un d'entre vous ou aux trois.

Mme Cherie Henderson: Je pense qu'il s'agit d'un problème très grave.

Ce ne seront pas des États hostiles; ce sont des organisations terroristes hostiles. Ces personnes seront assises dans un autre pays. Elles sont là en train de surveiller les médias sociaux, de créer leurs propres sites Web et de rechercher des jeunes. Elles recherchent les personnes qui sont peut-être seules, assises dans leur chambre devant leur ordinateur, en train d'explorer et d'essayer de répondre à des questions. Elles sont très vulnérables. Puis, ces personnes répondent, et elles établissent une relation.

Traditionnellement, dans le monde de l'espionnage, nous appelions cela créer un pot de miel. Vous attirez ces personnes afin qu'elles viennent à vous. C'est ce qu'ils font. Une fois qu'ils les ont attirées, ils continuent de travailler sur elles. Ils continuent de leur fournir des images des médias. Ils bâtissent cette idéologie extrémiste et ils façonnent ces jeunes esprits.

C'est ce qui m'inquiète beaucoup, parce que je pense qu'il y a en ce moment beaucoup de jeunes vulnérables et beaucoup d'acteurs très hostiles qui sont prêts à profiter de ces enfants.

M. Mike Kelloway: Me reste-t-il beaucoup de temps?

Le président: Je pense que nous pouvons terminer sur ce point, si cela vous va, monsieur Kelloway. Je pense que c'était un bon point à soulever.

M. Mike Kelloway: Très bien.

Merci, monsieur le président, je vous en suis reconnaissant.

Le président: Je ne sais pas à qui adresser ma question. Je vais probablement l'adresser à M. Khoury.

Une chose que nous n'avons pas encore abordée, c'est l'incidence de l'intelligence artificielle et des fermes de robots dans l'ensemble des médias sociaux et les conséquences qu'elles pourraient avoir dans l'avenir. Dans quelle mesure devrions-nous être préoccupés par la possibilité que l'intelligence artificielle et les fermes de robots influencent non seulement les jeunes, mais aussi tous les Canadiens à l'avenir?

M. Sami Khoury: Nous sommes assurément préoccupés par la mauvaise utilisation de l'intelligence artificielle. L'intelligence artificielle s'accompagne d'occasions, mais également de défis. Nous savons que l'intelligence artificielle est souvent utilisée pour amplifier la désinformation. Par sa nature même, une partie de l'algorithme de certains de ces outils est d'amplifier la désinformation.

Nous sommes également préoccupés par les fuites d'information au moyen de l'intelligence artificielle dans le cadre des interactions en ligne. Nous avons émis quelques conseils et orientations à l'intention des Canadiens sur la façon d'utiliser certains des outils publics existants en ce qui concerne l'intelligence artificielle, sur le fait d'être au courant de la menace inhérente à l'utilisation de l'intelligence artificielle et sur la manière dont certains pays ou États tentent d'exploiter les algorithmes de l'intelligence artificielle à leur profit.

● (1655)

Le président: Cela change rapidement. Que fait le Centre pour rester à la pointe du progrès? Comment faites-vous pour rester au fait de l'évolution de l'intelligence artificielle? Elle évolue rapidement et a une incidence énorme sur l'avenir. Que faites-vous à ce sujet?

M. Sami Khoury: Nous faisons un certain nombre de choses. L'une d'entre elles est notre propre recherche à la fine pointe de la technologie en matière d'intelligence artificielle. Du point de vue du gouvernement, nous travaillons également en étroite collaboration avec le Conseil du Trésor pour veiller à ce que celui-ci fournisse des directives aux autres ministères sur la manière d'utiliser ces outils grâce à des avis éclairés. Mis à part le gouvernement, nous avons publié quelques articles. Nous en parlons. Nous faisons des présentations sur la menace que constitue l'intelligence artificielle.

Tout à fait, il y a des possibilités, mais nous savons aussi que le revers de la médaille, c'est potentiellement un problème ou une menace.

Le président: Merci, monsieur Khoury, madame Henderson et monsieur Madou, d'avoir comparu devant le Comité. Au nom du Comité, je tiens à vous remercier pour les services que vous rendez aux Canadiens.

Nous allons suspendre la séance pendant une minute, puis nous reviendrons avec le témoin suivant. Nous aurons besoin d'un peu de temps pour les travaux du Comité, probablement environ cinq minutes. Je sais que nous avons prévu 15 minutes, alors nous devrions avoir assez de temps pour poser des questions et obtenir des réponses.

Nous allons suspendre pour une minute.

Merci à tous.

● (1655)

_____(Pause)_____

● (1700)

Le président: Bon retour à tous.

Nous allons amorcer la seconde partie de notre séance d'aujourd'hui.

Je souhaite la bienvenue à Mme Sharon Polsky, présidente du Conseil du Canada de l'accès et la vie privée.

Madame Polsky, vous avez cinq minutes pour vous adresser au Comité. Allez-y, s'il vous plaît.

Mme Sharon Polsky (présidente, Conseil du Canada de l'accès et la vie privée): Je vous remercie.

Je vous remercie de m'avoir invitée à présenter quelques observations sur la question de savoir si, et comment, les médias sociaux peuvent compromettre la vie privée, la sûreté, la sécurité et la démocratie.

Je suis Sharon Polsky, présidente du Conseil du Canada de l'accès et la vie privée, un organisme indépendant, à but non lucratif et non partisan qui n'est pas financé par le gouvernement ou le secteur. L'organisme est composé de membres provenant des secteurs public et privé, qui utilisent régulièrement les médias sociaux dans leur vie personnelle et professionnelle.

Plusieurs personnes se souviennent de la présentation de Google Mail. Il s'agissait d'une brillante manœuvre de marketing qui s'attaquait à la nature humaine. Seules quelques personnes triées sur le volet pouvaient posséder un compte. L'invitation conférait à ces rares personnes un statut spécial parmi leurs pairs. Cette tactique et l'attention des médias ont créé la demande. On ne parlait pas des inconvénients, des risques ou de la protection de la vie privée. Les gens voulaient simplement avoir ce compte Google. C'était de la simple psychologie qui montrait à quel point les gens peuvent être facilement manipulés.

Depuis lors, nous avons vu d'innombrables exemples de grandes entreprises technologiques qui nous manipulent pour partager en ligne les détails les plus intimes de notre existence. Les médias sociaux continuent de tirer parti de la nature humaine, et l'industrie lucrative des courtiers en données en est le principal bénéficiaire, à l'exception de ceux qui voudraient nous manipuler à leur profit, qu'il s'agisse d'entreprises, de partis politiques ou de gouvernements. Avec les récents événements géopolitiques, il est facile de penser que ce que les gens publient sur des médias sociaux pourrait être utilisé pour contraindre, extorquer de l'argent ou manipuler, mais imputer cela uniquement aux médias sociaux ou aux médias sociaux d'un autre pays est une vision à court terme.

Les risques en ligne sont le reflet de la société et proviennent de nombreuses sources, y compris des outils de communication et de collaboration familiers que de nombreuses personnes présentes dans cette salle utilisent probablement tous les jours. Chacun d'entre eux constitue une menace réelle et constante. Les applications Zoom, Teams, Slack, Facebook et les autres sont toutes étrangères.

Ce n'est un secret pour personne que de nombreuses entreprises récupèrent des données et justifient leurs actions en disant qu'elles considèrent les informations comme publiques parce que leurs systèmes d'intelligence artificielle ont été capables de les trouver sur le Web. Peut-être que le site sécurisé où vous avez publié des informations personnelles ou confidentielles, ou que le système de sécurité informatique de l'hôpital de l'Ontario que vous avez visité récemment ont été compromis et que votre état de santé ou vos conversations de nature délicate sont maintenant vendus sur le Web clandestin.

Si nous craignons que les personnes qui utilisent les médias sociaux divulguent des informations susceptibles de les rendre controversées sur le plan politique et plus susceptibles d'être influencées, j'attire votre attention sur l'enregistrement que nous entendons chaque fois que nous appelons notre fournisseur de téléphonie mobile ou la plupart des autres entreprises, qui dit: « Cet appel sera enregistré à des fins de formation ». Cela signifie généralement la formation des systèmes d'intelligence artificielle grâce à l'apprentissage automatique. L'aspect humain de cette formation est réalisé dans des pays du monde entier par des personnes qui ont accès à vos informations sensibles.

Une entreprise technologique finlandaise a récemment commencé à utiliser la main-d'œuvre des prisons pour l'étiquetage des données. Et ce n'est pas fini. Nous ne choisissons pas que l'étiquetage soit effectué par quelqu'un en Alberta ou en Albanie. Il n'y a aucun contrôle, et rien n'empêche une entreprise ou un gouvernement d'acheter les informations, parce qu'elles sont disponibles en grande partie par l'intermédiaire du réseau de courtiers de données. Elles sont facilement accessibles à l'échelle internationale. Je pourrais continuer ainsi longtemps.

Oui, l'éducation est certainement importante. Les ordinateurs sont présents dans les bureaux depuis près d'un demi-siècle. L'éducation n'est pas encore là, puisque nous voyons les grandes entreprises technologiques investir des dizaines de milliards de dollars par an pour contrecarrer et miner les efforts de réglementation du secteur, sous prétexte que cela nuirait à l'innovation. Il s'agit d'un faux-fuyant qui a été réfuté à maintes reprises au fil de l'histoire.

Nous voyons des sites de rencontre que les gens utilisent couramment et qui sont merveilleux pour une vie sociale, mais lorsque les sites comme le site de rencontre canadien Ashley Madison sont compromis, j'ose dire que beaucoup de leurs clients deviennent controversés sur le plan politique.

● (1705)

Lorsque des enfants ou des adultes se rendent sur un site Internet, avant même de voir le résultat, le fait qu'ils sont allés consulter le site — qu'il s'agisse de santé mentale, de toxicomanie ou de conseils médicaux — est déjà secrètement transmis à des entreprises telles que Facebook et les courtiers de données.

Ce n'est pas quelque chose que le projet de loi C-27, ni aucun autre texte législatif, va régler. En fait, la plupart des lois introduites ici et à l'étranger ne feront qu'aggraver la situation pour tout le monde, y compris pour les enfants, et surtout pour les enfants.

Je serai heureuse de répondre à vos questions. Il s'agit d'une tâche colossale, et je vous félicite tous.

Le président: Merci, madame Polsky. Je suis sûr que nos membres ont beaucoup de questions à vous poser. Vous serez la seule à y répondre, alors c'est parti.

Monsieur Kurek, vous disposez de six minutes. Allez-y, s'il vous plaît.

M. Damien Kurek: Merci, monsieur le président.

Merci beaucoup et bienvenue au sein du Comité.

L'un des grands défis que nous devons relever est le suivant. Lorsque quelqu'un télécharge une application, il coche la case des conditions générales. Il y a de plus en plus d'éducation sur ce qui doit ou ne doit pas être publié sur des médias sociaux. Cependant, il y a une immense zone grise quant aux informations qui sont réellement recueillies ou consultées, qu'il s'agisse de l'emplacement ou d'autres éléments. En fait, c'est le Comité qui s'est penché sur le fait que les informations relatives à l'emplacement des téléphones portables ont été partagées avec le gouvernement pendant la pandémie de la COVID-19. Ces informations détaillaient les déplacements des personnes dans les magasins d'alcool, les épiceries et d'autres lieux publics.

Comment nous réconcilier avec ce monde de « mégadonnées », où quelqu'un télécharge une application et coche une case, et où tout d'un coup ces informations sont envoyées vers quelque chose que nous ne comprenons pas vraiment? Quelles sont les conséquences de la destination de ces données?

Mme Sharon Polsky: C'est une excellente question, surtout si l'on considère que les témoins précédents du Comité, du CST et du SCRS, ont répété à maintes reprises qu'il appartient au consommateur, y compris aux enfants, de lire la politique de protection de la vie privée et de comprendre ce qui se passe. Beaucoup de mes collègues et de membres du Conseil du Canada de l'accès et la vie privée ne comprennent pas. Ils ne comprennent juste pas. Comment peut-on raisonnablement s'attendre à ce qu'un enfant ou quiconque comprenne? Je vis avec ce genre de choses. Ce n'est pas le cas de la plupart des gens.

Comment cela se produit-il? En grande partie à cause des entreprises étrangères. Nos lois sont obsolètes, inefficaces et mal appliquées. Les entreprises étrangères le font parce qu'elles le peuvent.

● (1710)

M. Damien Kurek: Constate-t-on les lacunes que vous soulignez? Pouvez-vous citer des exemples au Canada où des acteurs étatiques étrangers ou d'autres entités qui tentent de nuire aux Canadiens tirent parti de cette situation? Pouvez-vous citer des exemples et dire: « C'est là que nous voyons les conséquences de cette situation en temps réel »?

Mme Sharon Polsky: Je pense que c'est un phénomène généralisé.

Par ailleurs, au cours de la dernière demi-heure, il m'a fallu quelques minutes pour trouver les anniversaires de tous les membres du Comité, à l'exception de trois. Je vous souhaite d'avance un « joyeux anniversaire » pour la semaine prochaine.

M. Damien Kurek: Merci.

Mme Sharon Polsky: C'est très facile. Nos informations circulent, même si nous diffusons de fausses informations. Vous pouvez imaginer ce que vivent mes enfants. Ils ont leur anniversaire en ligne. Le jour de leur véritable anniversaire, leurs amis leur disent « joyeux anniversaire », et les algorithmes s'en rendent compte. Les algorithmes détectent, par le volume de vœux à la date réelle, qu'il s'agit d'un véritable anniversaire, ainsi que d'autres informations recueillies par le réseau caché de courtier de données, où nos informations sont échangées, vendues et font l'objet d'enchères instantanées.

Les moindres détails de notre vie sont disponibles à la vente dans le monde entier.

M. Damien Kurek: Je comprends et je vous remercie pour vos vœux d'anniversaire. Je suis certainement beaucoup plus jeune que j'en ai l'air.

Ce qui a déclenché cette étude, c'est en grande partie la question de TikTok, qui a été banni par le gouvernement des appareils mobiles gouvernementaux. Il y a quelques semaines, le gouvernement a interdit WeChat, qui a certainement des liens beaucoup plus directs avec la dictature communiste de Pékin. Ce sont deux exemples qui ont fait les manchettes et pour lesquels le gouvernement a pris des mesures, mais nous avons vu qu'une application météorologique était l'une des applications qui vendaient des données, que le gouvernement a achetées au cours de la pandémie de la COVID-19.

Plus généralement, pouvez-vous donner votre avis au Comité — en une minute environ, si vous le pouvez — concernant la façon d'envisager les choses sous cet angle, dans leur ensemble, en regardant au-delà de TikTok, de WeChat ou des médias sociaux, pour examiner l'accès que nous donnons à diverses entités à une quantité incroyable d'information?

Mme Sharon Polsky: Je suis d'accord. Il ne s'agit pas seulement d'une plateforme de médias sociaux quelconque, une d'entreprise ou d'un gouvernement quelconque. Il s'agit d'un phénomène répandu, qui se développe depuis une génération.

Que devons-nous faire? Comment l'arrêter?

Oui, l'éducation commence dès le plus jeune âge. Est-il trop tard pour remettre le génie dans sa bouteille? Non. Il y a tellement d'information sur chacun d'entre nous que nous ne nous rendons même pas compte que nous sommes individuellement perdus. Dans les entreprises, les responsables des achats, qui en savent autant ou aussi peu que la plupart des gens, sont à la merci des fournisseurs. Ils ne s'intéressent pas à votre vie privée. Ce qui les intéresse, c'est leur commission, leur résultat net et le bénéfice de leurs actionnaires.

M. Damien Kurek: Je n'ai plus de temps, je vais donc vous demander un complément d'information. Pourriez-vous fournir au Comité des recommandations spécifiques — et nous parlons surtout des répercussions sur les enfants — que le Comité pourrait appliquer pour aborder ce problème, en particulier avec les enfants, mais aussi les répercussions plus larges sur la société que crée ce problème?

Je n'ai malheureusement pas le temps de vous laisser répondre à cette question, mais j'espère que vous pourrez fournir ces informations au Comité à une date ultérieure.

Mme Sharon Polsky: J'en serais ravie.

Le président: Merci. C'est une bonne demande.

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

M. Ali Ehsassi (Willowdale, Lib.): Merci, monsieur le président.

Merci, madame Polsky. C'était très instructif.

J'ai quelques questions à vous poser.

M. David Lieber, chef des politiques publiques en matière de vie privée pour les Amériques chez TikTok, a témoigné devant notre comité. Je me demandais si vous aviez eu l'occasion d'examiner ce témoignage.

● (1715)

Mme Sharon Polsky: J'ai lu certains extraits, oui.

M. Ali Ehsassi: Était-il trompeur, à votre avis?

Mme Sharon Polsky: Non. Était-ce une réponse complète, détaillée et exhaustive? Je ne sais pas, mais d'après mon expérience — en gardant à l'esprit que je suis la présidente du Conseil du Canada de l'accès et la vie privée, que je suis conseillère en matière de protection de la vie privée depuis environ 30 ans, que j'ai infiltré beaucoup d'organisations et que j'ai vu beaucoup de choses — très souvent, le langage utilisé dans les témoignages, dans les rapports des médias et dans les soi-disant politiques de protection de la vie privée ne donne pas l'heure juste. Nous recueillerons vos informations et les partagerons avec nos partenaires et nos affiliés, mais avec qui, quand, où et dans quel but?

M. Ali Ehsassi: L'une des choses qu'il a dites, qui m'a semblé un peu étrange, c'est que personne n'avait à s'inquiéter parce que nous sommes soumis au droit canadien. Est-ce que cela vous rassure? S'ils ont des données et, comme vous le laissiez entendre, qu'ils les envoient en Albanie ou ailleurs, même si vous êtes soumis au droit canadien, je ne crois pas que nous pouvons faire grand-chose, n'est-ce pas?

Mme Sharon Polsky: En tant que législateurs, une chose que nous pouvons faire est de ne pas adopter le projet de loi C-27, parce qu'il ne rendra pas les choses meilleures; il ne fera que les empirer.

Que pouvons-nous faire? La Loi sur la protection des renseignements personnels et les documents électroniques est-elle rassurante? Non, elle ne l'est pas, parce qu'elle n'est pas suffisante, comme l'a dit Jennifer Stoddart lors de ses derniers jours dans son rôle de commissaire. Elle pourrait avoir plus de mordant. C'était il y a combien d'années? La Loi a encore besoin d'un peu plus de mordant. Bien sûr, les organisations canadiennes sont responsables de la collecte, de l'utilisation, de la divulgation appropriées et de tout le reste en vertu de la LPRPDE, mais lorsque les renseignements sont transférés à l'étranger, elles en perdent le contrôle. Nous, en tant que Canadiens, n'avons aucun recours quand nos renseignements se retrouvent dans une nation étrangère et s'envolent, ou quand nous constatons des choses qui violent notre vie privée, que ce soit de la part d'Equifax, de Meta, de Google ou de toute autre organisation.

Une commissionnaire ou une autre quelque part dans le monde les frappe d'une amende de plusieurs millions de dollars ou de centaines de millions de dollars. Elles les mettent dans leur rapport financier comme un poste budgétaire, et cela réduit leur dette fiscale. Suivant. C'est tout. C'est de l'argent de poche pour elles. Il s'agit de l'entreprise, pas d'une personne.

M. Ali Ehsassi: Je vous remercie de votre réponse.

Une autre chose qui devrait vraiment nous préoccuper, ce sont les rançongiciels. Pouvez-vous nous parler de l'intersection entre ces applications sociales et les renseignements obtenus, puis mis à profit contre les consommateurs?

Mme Sharon Polsky: Je crois que les rançongiciels, comme bon nombre des problèmes que nous avons en ligne, sont un reflet de la société. Il s'agit du même type de crime que ceux qui étaient commis avant l'avènement d'Internet. Internet est un outil qui permet aux auteurs de crime de commettre ces crimes en plus grand nombre, avec une meilleure efficacité et rentabilité de leur côté, et des rendements plus élevés. C'est fantastique, mais ce n'est aucunement différent. Ce n'est vraiment pas différent.

Le problème une fois de plus est l'éducation. Vous pouvez avoir la meilleure technologie, la meilleure sécurité qui soit, mais si quelqu'un n'a pas le courage de poser des questions au patron ou d'appeler la présidente et de dire « Excusez-moi, madame, mais avez-vous réellement envoyé cela? » ou si personne n'a la curiosité ou le scepticisme, en particulier de nos jours, de remettre en question ce qui est présenté dans leur courriel — et je suis certaine que ces personnes agissent de bonne foi — et si elles cliquent sur la mauvaise chose, cela expose toute l'organisation à des rançongiciels et à des problèmes.

L'organisation peut s'en remettre, mais qu'en est-il de toutes les personnes dont les renseignements personnels ont été compromis? Dans le cas d'Equifax, on comptait 146 millions d'Américains, et le versement, le règlement négocié, l'amende... Je me souviens de Kevin Mitnick, quand il était toujours en vie, sur LinkedIn, qui montrait le chèque de 5,42 $ qu'il a reçu. Cela devait l'aider à se rétablir. Au Canada, les Canadiens qui ont été touchés ont bénéficié d'une année ou deux de surveillance de leur crédit, qui était administrée par l'organisation américaine d'Equifax.

● (1720)

M. Ali Ehsassi: Ma dernière question est la suivante: étant donné que vous avez sans doute eu l'occasion d'étudier les diverses administrations, selon vous, quelle administration fait le meilleur travail pour assurer la protection des droits à la vie privée?

Mme Sharon Polsky: En ce moment, je dirais que c'est l'Union européenne, en raison du Règlement général sur la protection des données, ou RGPD, et parce que, à la dernière minute, ils ont freiné une mesure législative qui aurait nécessité, essentiellement, de briser le chiffrement pour permettre à la police d'être en mesure de retrouver plus facilement les prédateurs. La police le fait maintenant sans passer par les portes arrières du chiffrement.

Le président: Je vous remercie, madame Polsky et monsieur Ehsassi.

[*Français*]

La prochaine personne à intervenir sera M. Villemure.

[*Traduction*]

Avez-vous mis votre écouteur, madame Polsky?

Mme Sharon Polsky: Oui.

Merci.

Le président: Merveilleux.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

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

Je tiens également à souhaiter un joyeux anniversaire à mon collègue M. Kurek.

Bonjour, madame Polsky. C'est un plaisir de vous revoir.

Comment qualifieriez-vous le comportement des plateformes sociales en matière de protection de la vie privée?

[*Traduction*]

Mme Sharon Polsky: Je dirais qu'elles sont très égoïstes, puisqu'elles sont des organisations à but lucratif. Elles font ce qu'elles doivent faire pour améliorer leurs résultats et fournir le meilleur rendement possible à leurs investisseurs et actionnaires.

[*Français*]

M. René Villemure: Se valent-elles toutes, ou y en a-t-il qui sont meilleures ou pires que d'autres?

[*Traduction*]

Mme Sharon Polsky: Je pense que certaines sont meilleures que d'autres. Elles s'intéressent davantage à la vie privée des personnes. Je pourrais nommer le Tor Project, Signal, et Proton. Voilà les trois qui me viennent à l'esprit. Elles ne constituent pas particulièrement des plateformes de médias sociaux, mais elles sont assurément des outils de communication qui ne prennent pas le moindre renseignement, la moindre métadonnée, ou autre. Elles ne les conservent pas. Cela offre bien plus de sécurité. De plus, leur technologie de chiffrement est beaucoup plus solide.

[*Français*]

M. René Villemure: En matière de protection de la vie privée, les plateformes sociales se valent, c'est-à-dire qu'elles ne sont pas très bien. Est-ce exact?

[*Traduction*]

Mme Sharon Polsky: C'est une question très difficile, puisqu'elles ont chacune leurs propres intérêts à cœur. Elles collectent les renseignements et offrent aux annonceurs l'occasion d'être dans notre champ de vision. Je ne sais pas si l'une d'entre elles s'intéresse vraiment à notre vie privée.

[*Français*]

M. René Villemure: À ce sujet, pouvez-vous nous fournir quelques commentaires sur le capitalisme de surveillance et nous dire ce qu'un comité comme le nôtre peut faire pour en atténuer les effets?

[*Traduction*]

Mme Sharon Polsky: Le terme « capitalisme de surveillance », inventé par Shoshana Zuboff, est un terme merveilleux. Nous pourrions aussi dire « économie de la surveillance », puisque de nos jours la majeure partie de notre économie est fondée sur la surveillance d'une manière ou d'une autre, que nous en soyons conscients ou non.

Que pouvons-nous faire? Avant qu'un médicament ne soit autorisé pour être vendu au Canada, avant qu'un véhicule ne soit autorisé à être vendu et immatriculé au Canada, et de nombreux autres produits, ils doivent être testés par une autorité canadienne indépendante qui puisse s'assurer qu'ils sont adaptés et sécuritaires. Je crois que la même chose s'applique à la technologie que nous utilisons tous les jours, qui est maintenant vendue par des entreprises n'ayant que leurs intérêts à cœur. Elles favorisent toutes l'économie de la surveillance.

La seule manière de ne pas laisser nos renseignements être utilisés en permanence pour alimenter la surveillance... Les manipulateurs de médias disent « Eh bien, tout le monde est d'accord avec cela parce qu'ils continuent à donner leurs renseignements », malgré le fait que nous n'ayons que très peu d'options voire aucun moyen de refuser. Il revient à notre gouvernement de réglementer cela, malgré les objections des grandes entreprises technologiques.

● (1725)

[*Français*]

M. René Villemure: Vous avez dit un peu plus tôt que, malgré les efforts que l'on a mis dans le projet de loi C-27, celui-ci était inutile pour nous prémunir contre de telles invasions de la vie privée, n'est-ce pas?

[*Traduction*]

Mme Sharon Polsky: Eh bien, je crois qu'il s'agit d'un pas de recul par rapport à ce que nous avons dans la LPRPDE. Tout d'abord, le premier mot est « consommateur » — la Loi sur la protection de la vie privée des consommateurs — nous désigne tous comme des consommateurs. Nous sommes des produits, et nos renseignements sont voués à être commercialisés.

Elle prévoit un droit privé d'action, une fois que nous nous sommes plaints auprès du commissaire qui — comme la plupart de ces instances — est chroniquement sous-financé. Une fois qu'ils auront enfin assigné le dossier, enquêté, décidé et tranché, le dossier sera envoyé à un nouveau tribunal qui, selon moi, devra au moins l'examiner, ou au moins procéder à une nouvelle enquête approfondie. Si le tribunal est d'accord avec le commissaire pour dire qu'une amende est justifiée, alors l'entreprise fautive a le droit de porter l'affaire devant les tribunaux.

Combien d'années cela prendra? Une fois qu'ils auront épuisé leurs recours juridiques, vous et moi pourrons faire valoir notre droit privé d'action. Nous devons alors payer un autre avocat et passer encore 7 à 10 ans.

[*Français*]

M. René Villemure: Donc, ce n'est pas très utile.

Vous mentionniez un peu plus tôt que la simple présence sur un site Web, avant même de cliquer sur le consentement, était une donnée en soi. Pouvez-vous nous en dire un peu plus à ce sujet?

[*Traduction*]

Mme Sharon Polsky: Oui, il s'agit d'une caractéristique qui... J'ai remarqué que dans beaucoup d'organisations, les gens qui créent les sites Web ne parlent pas aux personnes du Commissariat à la protection de la vie privée, si l'on peut dire. C'est une vieille histoire selon laquelle nous mettons en place tous ces outils merveilleux qui peuvent recueillir des renseignements, et c'est vraiment génial de dire « Hé, nous pourrons peut-être en faire quelque chose à l'avenir », sans savoir — en raison d'un manque d'éducation — qu'ils recueillent trop d'information. Le fonctionnement est similaire à celui d'un témoin. Avant même que vous ne voyiez le site Web auquel vous voulez accéder, le fait est que vous êtes déjà transmis à Facebook et aux courtiers en données.

[*Français*]

Le président: Merci, monsieur Villemure et madame Polsky.

[*Traduction*]

Ensuite, nous avons M. Green, pendant six minutes.

Allez-y, s'il vous plaît.

M. Matthew Green: Je vous remercie.

J'apprécie certainement votre analyse très juste selon laquelle le consommateur est le produit. Je pense que cela illustre parfaitement l'essentiel de ce dont nous parlons ici.

Étiez-vous présente pendant que le précédent groupe de témoins comparaissait? Si vous l'étiez, vous aurez remarqué que, dans mes questions, j'ai soulevé fréquemment la notion selon laquelle il n'y a pas un seul responsable dans ce scénario, mais qu'en fait, toutes les plateformes sont engagées dans ce type de capitalisme de surveillance. Peu importe qu'un acteur d'un État étranger ait un accès direct grâce à ByteDance ou qu'un autre régime dictatorial l'achète à un autre en étant le plus offrant, il n'y a essentiellement pas de différence. Ils détiennent les données.

Êtes-vous d'accord avec cette analyse?

Mme Sharon Polsky: Absolument. Nos renseignements sont vendus, échangés, et font l'objet d'enchères en temps réel. Nous ne le savons pas, et nous ne pouvons pas dire « Non, ne faites pas ça », car nous n'avons aucune idée qui enchérit sur nos renseignements. Nous n'avons aucune relation directe avec eux. Nous n'avons aucun recours. Nos renseignements sont partis.

M. Matthew Green: À cet égard, j'aimerais parler des recours. Vous avez mentionné le mordant que vous aimeriez voir dans la législation.

Plus précisément, pouvez-vous prendre un moment et réfléchir aux types de mesures ayant du mordant que vous aimeriez voir dans une loi proposée qui traiterait de la vie privée d'une manière plus approfondie?

Mme Sharon Polsky: Je pourrais vous fournir un exemple très rapide.

Le fait que les entreprises se voient désormais imposer des amendes, mais pas les personnes, n'a aucun sens. En revanche, après le scandale d'Enron, il y a de cela 20 à 25 ans, les États-Unis ont adopté la loi SOX. Le nom complet est la loi Sarbanes-Oxley de 2002. Elle dit très simplement que la personne à la tête de l'organisation est responsable de tout ce qui figure dans l'état financier. Si les choses vont de travers, ces responsables risquent personnellement des amendes de plusieurs millions de dollars et des peines de prison. Des entreprises du monde entier, notamment celles du Canada se sont précipitées de s'assurer qu'elles étaient conformes à la loi SOX. Nous devons faire de même.

● (1730)

M. Matthew Green: Affirmez-vous que lorsqu'une personne ne donne pas tous les renseignements et le plein consentement quand elle utilise une application ou une plateforme, il s'agit d'une sorte de fraude commise par l'entreprise et, par conséquent, qu'il devrait y avoir une responsabilité criminelle à cet égard?

Mme Sharon Polsky: Je n'irais pas jusqu'à dire qu'il s'agit d'une fraude, mais que c'est sans doute trompeur. C'est autorisé par la législation actuelle et par le projet de loi C-27, qui va maintenir le statu quo du même consentement vague. Cela n'améliorera pas la protection de la vie privée.

M. Matthew Green: Voilà une occasion pour vous d'aborder cette clause précise en matière de consentement.

Selon moi, si vous ne vous engagez pas avec une totale compréhension, vous ne pouvez pas consentir. Si vous téléchargez une application pour un certain usage et que votre utilisation de l'application est ensuite vendue à de tierces parties sans que vous le sachiez et sans que vous connaissiez l'objectif réel de l'application... Je fais référence à Cambridge Analytica. Cette entreprise détient votre vie en données. Je ne me souviens pas du nom exact de l'application où elle a obtenu tous ces renseignements. Je dirais qu'il s'agit d'une fraude. Vous n'avez pas à dire cela, mais je dirais qu'il s'agit d'un engagement frauduleux du consommateur.

Quant au consentement, pourriez-vous préciser les types de consentement explicite que vous souhaiteriez voir pour que les personnes qui utilisent ces plateformes aient une connaissance préalable complète de ce à quoi elles s'engagent?

Mme Sharon Polsky: D'accord. Je pense que vous parlez de deux choses ici.

La première est que les entreprises ou les organisations qui sont censées obtenir notre consentement éclairé au moment de collecter nos renseignements personnels ou préalablement reconnaissent — comme l'a fait Mark Zuckerberg devant le Congrès — que peu de gens lisent ces politiques de confidentialité. À mes yeux, ils recueillent nos données en sachant pertinemment que personne ne lit les politiques sur la protection des renseignements personnels. Par conséquent, il ne s'agit pas d'un consentement éclairé. Ils violent nos lois en matière de protection de la vie privée, le RGPD et bien d'autres règles.

Que faut-il faire? Remettre les choses en ordre. Cesser de permettre aux organisations d'avoir le contrôle. Changer les choses de sorte que chacun d'entre nous soit en mesure...

M. Matthew Green: De consentir ou de refuser.

Mme Sharon Polsky: Non, il s'agit bien plus de simplement consentir ou refuser; questionnez l'entreprise. Faites en sorte qu'il y ait un index d'entreprises que les consommateurs peuvent consulter pour voir quelles entreprises se conforment à la législation. Si une entreprise le fait d'une meilleure manière qu'une autre, le consommateur peut faire un choix. J'autorise mes renseignements à être utilisés par votre compagnie dans un certain objectif. J'obtiens un reçu. Il y a un document qui précise que c'est moi qui détiens le contrôle et non l'entreprise.

M. Matthew Green: C'est intéressant. Je comprends.

Je crois que la dernière étude à laquelle vous étiez présente, il y a quelque temps, portait sur la surveillance dans les téléphones, avec la GRC.

Mme Sharon Polsky: Les logiciels espions.

M. Matthew Green: Oui. Voilà. De nombreuses manières, qu'il s'agisse de l'utilisation de ces appareils par les gouvernements ou les entreprises qui utilisent ce type d'application, il s'agit de logiciels espions. Êtes-vous d'accord pour dire que les applications de médias sociaux sont une forme de logiciels espions?

Mme Sharon Polsky: Absolument.

M. Matthew Green: Pourriez-vous nous en dire davantage à ce sujet?

Le président: Veuillez répondre très rapidement.

Mme Sharon Polsky: Cela me pose parfois problème. Il y a beaucoup de choses, comme je l'ai dit, à discuter.

C'est le niveau de détail des renseignements qu'ils recueillent sur nous, généralement à notre insu, comme l'application de covoiturage que nous utilisons qui enregistre la géolocalisation précise et l'heure de la journée. Ils peuvent l'utiliser à leurs propres fins. À qui ces renseignements sont-ils remis, et quelles hypothèses peut-on tirer de ces renseignements ou de tout autre renseignement?

En réalité, on nous espionne. Je suis d'accord.

Le président: Merci, madame Polsky.

[*Français*]

Monsieur Gourde, vous avez la parole pour cinq minutes.

M. Jacques Gourde: Merci, monsieur le président.

Je remercie les témoins. Leurs déclarations et celles des témoins précédents m'inquiètent beaucoup.

Comme êtres humains, nous sommes devenus des produits. Ces grandes compagnies ont établi un profil pour chacun d'entre nous selon nos aspirations, ce que nous achetons et ce que nous regardons, et ce profil est revendu à des entreprises qui veulent nous vendre quelque chose.

J'ai l'impression qu'il est déjà trop tard pour notre génération et tous ceux qui utilisent les réseaux sociaux présentement. Je suis l'heureux grand-père de six petits-enfants — j'en aurai bientôt un septième —, qui sont trop jeunes pour utiliser cela. Devrait-on plutôt travailler pour protéger cette génération?

● (1735)

[*Traduction*]

Mme Sharon Polsky: Nous protégeons la prochaine génération, assurément, mais nous luttons tous contre les géants du Web bien financés qui insistent sur le fait que tout le monde veut cela. Personne ne comprend cela. Bon, quelques personnes le comprennent suffisamment bien pour s'opposer à ce qu'ils nous font.

Les choses ont changé très rapidement. Je pense que c'était en 2004 qu'un ministre du gouvernement canadien était sur la sellette parce que les médias avaient découvert que le gouvernement recueillait 2 000 éléments d'information sur chacun des 33,7 millions de Canadiens, alors qu'il y avait environ 31 millions de Canadiens. Les gens ont réagi rapidement, haut et fort. Le ministre a répondu que ce n'était pas grave, que les renseignements avaient été restitués — comment faire cela avec des données électroniques, je ne sais pas —, et ils les ont apparemment retirés.

Cela a très vite changé. Au lieu de traiter avec un ministère ou un autre, nous traitons désormais avec le gouvernement, et le gouvernement déclare qu'il est propriétaire de nos renseignements. Le concept même de politique publique a changé. J'ose dire que, s'il existe un véritable intérêt à préserver et à protéger les enfants, la vie privée et les générations futures, il faut y réfléchir sérieusement. Des études, c'est formidable, mais il faut agir très vite.

[*Français*]

M. Jacques Gourde: Est-ce que la quête d'information sur l'ensemble des individus, présentement, est une atteinte à nos libertés individuelles?

[*Traduction*]

Mme Sharon Polsky: Est-ce une menace pour notre liberté? Absolument. Il est trop facile pour une organisation d'utiliser les renseignements recueillis sur nous pour influencer nos opinions, pour influencer les opinions à propos des politiques publiques, du gouvernement, des législateurs, des enseignants, des institutions. Il s'agit fondamentalement d'une menace pour la démocratie, les libertés civiles et les droits de la personne. L'intelligence artificielle ne fera qu'aggraver la situation, à moins qu'une réglementation efficace et solide ne soit mise en place pour protéger les personnes, et pas seulement pour favoriser le commerce.

[*Français*]

M. Jacques Gourde: Merci beaucoup.

Le président: Merci, monsieur Gourde.

[*Traduction*]

Madame Damoff, vous disposez de cinq minutes. Allez-y, je vous prie.

Mme Pam Damoff: Merci, monsieur le président.

Merci beaucoup d'être des nôtres aujourd'hui et d'apporter vos vastes connaissances à notre comité.

Je veux revenir aux jeunes. Plus tôt, quand nous avons reçu le SCRS et le CST, j'ai dit que lorsque les représentants de TikTok ont comparu, ils ont déclaré que la seule chose qu'ils recueillaient était une adresse de courriel. Ils veillent à ce que les jeunes leur donnent leur date de naissance, et tout baigne dans l'huile! Il n'y a pas, sur la plateforme, un seul jeune qui ne devrait pas être là. J'ai remis en question leurs propos à l'époque.

Je me demande si vous pourriez simplement nous expliquer un peu. Les jeunes s'inscrivent. Ils donnent une adresse de courriel. Combien de renseignements supplémentaires TikTok et Instagram, qui sont les deux plateformes les plus populaires auprès des jeunes, recueillent-ils et comment les recueillent-ils? Est-ce que cela vous préoccupe?

Mme Sharon Polsky: Je n'ai pas enquêté suffisamment sur ces entreprises pour savoir ce qu'elles recueillent, mais de manière plus générale, les entreprises recueillent ces renseignements.

Normalement — et n'oubliez pas qu'on nous dit de respecter l'autorité et de répondre franchement lorsqu'on nous pose une question —, les gens fournissent leurs véritables renseignements. Il ne leur vient pas à l'esprit de donner un nom ou un anniversaire inventé ou d'utiliser une adresse de courriel à usage unique ou qui cache leur véritable adresse de courriel. Ils utilisent leur adresse de courriel, qui est connectée en arrière-plan par les courtiers en données. C'est extrêmement préoccupant.

Quant à savoir comment déterminer si une personne fournit son âge réel ou non, de nombreuses entreprises vendent ce service. Elles récupèrent votre pièce d'identité gouvernementale avec photo et la vérifient. Elles rassemblent ces renseignements, et c'est une autre menace. En ce qui concerne la loi, je sais que le Canada réfléchit à la même chose que le Royaume-Uni et l'Union européenne — ou, dans le cas du Royaume-Uni, elle a été adoptée —, c'est-à-dire exiger que les organisations recueillent ces renseignements. C'est une menace énorme.

● (1740)

Mme Pam Damoff: Pour revenir aux jeunes, nous n'avons pas du tout parlé des applications et des filtres. Je me souviens qu'il y a quelques années, il existait un système permettant de télécharger une application sur votre téléphone qui vous montrait à quoi vous ressembleriez dans 20 ans. Je me souviens que toutes sortes de personnes téléchargeaient cette application et téléversaient leurs photos — c'est amusant de partager ces photos —, puis il se trouve que l'entreprise était installée en Chine et que ces renseignements n'étaient en fait pas sécurisés.

Je vois souvent des jeunes qui ont téléchargé des filtres qui peuvent les transformer en personnage de Disney, entre autres, selon l'application de filtres. Je me demande simplement si vous êtes préoccupée par ce genre de choses qui semblent amusantes, mais qui sont en fait assez dangereuses quant aux renseignements que vous partagez.

Mme Sharon Polsky: Je pense que cela ressemble beaucoup aux questions qu'on vous pose: Quel est votre chien préféré, votre animal préféré ou votre couleur préférée, ou si vous étiez une voiture, laquelle seriez-vous? Ce sont autant de moyens subtils de recueillir des renseignements sur les gens, leur profil psychologique et leurs préférences. Vous ne savez pas qui les recueille et quel usage ils feront de ces renseignements. C'est une grande préoccupation, vraiment.

Mme Pam Damoff: Je n'y avais pas pensé, mais très souvent sur Facebook, on voit « répondez à ce questionnaire »: Dans quelle ville êtes-vous né et quelle école avez-vous fréquentée? Souvent, les gens ne vérifient pas leurs paramètres de sécurité pour voir avec qui ils partagent des renseignements, et cela finit par devenir public. Vous avez donné aux gens tous les renseignements dont ils ont besoin pour compromettre votre sécurité, car ce sont souvent les réponses aux questions que vous utilisez concernant vos cartes de crédit ou vos renseignements bancaires.

Mais comment éduquer le public? La responsabilité incombe aux entreprises, mais elle incombe également aux Canadiens — et partout dans le monde, mais nous nous concentrons sur le Canada. Comment pouvons-nous éduquer les Canadiens afin qu'ils soient plus conscients de ce qu'ils partagent en ligne?

Mme Sharon Polsky: Il existe des endroits, des organismes bien financés, qui font la promotion de l'éducation, mais ce n'est qu'une goutte d'eau dans l'océan. Je pense que c'est une question de politique publique d'exiger... Je comprends que ce n'est pas une question de compétence fédérale, mais je suis sûre que le gouvernement fédéral pourrait avoir une certaine influence, peut-être, auprès de ses collègues provinciaux et territoriaux, pour dire: « Incluez cela dans le programme obligatoire, dès la prématernelle. »

Mme Pam Damoff: Je sais que mon temps est écoulé.

J'ai siégé au comité de la sécurité publique, et nous avons réclamé à plusieurs reprises que la littératie numérique soit enseignée dans les écoles.

Merci d'avoir été généreux de votre temps, monsieur le président.

Le président: Je suis probablement l'homme le plus généreux que vous ayez jamais rencontré.

Des voix: Ha, ha!

Le président: De quoi riez-vous? Jetez simplement un coup d'œil à mon profil sur Facebook.

[*Français*]

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

M. René Villemure: Merci beaucoup, cher généreux président.

Madame Polsky, un peu plus tôt, mon collègue Matthew Green et vous discutiez des améliorations qui devraient être apportées afin que l'on ne soit pas coincé dans un cul-de-sac pour avoir déjà donné son consentement. À mon avis, plusieurs éléments de cette discussion étaient fort intéressants. Pouvez-vous continuer à nous en parler?

[*Traduction*]

Mme Sharon Polsky: J'ai perdu l'interprétation.

[*Français*]

Le président: Nous avons perdu le service d'interprétation, monsieur Villemure.

[*Traduction*]

Madame Polsky, assurez-vous d'être sur le bon canal. Vous voulez l'anglais.

Mme Sharon Polsky: Je suis sur le canal anglais, mais le son a diminué. Je n'ai pas pu entendre la traduction de toute la question.

Le président: D'accord.

[*Français*]

Monsieur Villemure, j'ai interrompu votre temps de parole. Vous pouvez poser votre question à nouveau. Nous allons veiller à ce que Mme Polsky soit capable de la comprendre. Veuillez recommencer.

● (1745)

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

Madame Polsky, vous étiez en discussion avec mon collègue M. Green, qui interviendra après moi. Vous étiez tous deux à énumérer des solutions pour éviter qu'on soit pris dans le piège, le cul-de-sac du consentement. J'aimerais que vous poursuiviez sur ces pistes de solution qui m'apparaissaient très intéressantes.

[*Traduction*]

Mme Sharon Polsky: L'une des choses que nous constatons dans les lois canadiennes et étrangères existantes, c'est un consentement qui n'a aucun niveau de détail. Vous devez consentir à ce que l'organisation recueille des renseignements auprès de vous et à votre sujet. Ils seront partagés avec ses partenaires commerciaux et affiliés. Vous ne savez pas qui sont ces gens, où ils se trouvent dans le monde ou ce qu'ils vont en faire.

Le projet de loi C-27 maintient le statu quo, sauf qu'il devra être rédigé dans un anglais simple et non juridique. Cela ne change rien. Ce n'est pas détaillé. Nous avons besoin d'un certain niveau de détail.

En fait, le gouvernement du Québec a adopté une nouvelle loi il y a environ un an. La partie sur le consentement est entrée en vigueur en septembre de cette année. C'est mieux, mais ce n'est pas ce que ça devrait être; on laisse encore libre cours aux organisations.

Nous devons renverser la situation afin que les organisations soient obligées de se conformer à la loi et que leur conformité soit évaluée par une organisation indépendante qui crée un répertoire accessible au public, si l'on peut dire. Nous pouvons alors tous consulter ce répertoire et déterminer si nous voulons ou non traiter avec une organisation en fonction de sa conformité avec la loi. C'est alors à nous de donner notre consentement.

[*Français*]

M. René Villemure: Je vais profiter des dix secondes qu'il me reste pour résumer en disant qu'à votre avis, on aurait besoin d'une loi Sarbanes-Oxley pour la vie privée, un genre de moteur pour ce genre d'activité. Je suis très intéressé par ce lien avec cette loi. Pourriez-vous préciser votre pensée sur le sujet ou nous envoyer des documents par écrit?

[*Traduction*]

Mme Sharon Polsky: Je serai heureuse de vous faire parvenir plus d'information. Je travaille avec des collègues qui élaborent une norme internationale et une fonctionnalité pour faire exactement ce que j'ai décrit. Cette norme renverse la situation, nous place aux commandes et oblige les organisations à se conformer à la loi.

C'est important, étant donné qu'il y en a encore beaucoup au Canada qui ne se conforment pas encore entièrement ou pas du tout à la LPRPDE, 20 ans plus tard.

[*Français*]

Le président: Merci, monsieur Villemure et Madame Polsky.

[*Traduction*]

Monsieur Green, vous disposez de deux minutes et 52 secondes. Vous avez la parole, monsieur.

M. Matthew Green: Je comprends le renversement du fardeau de la preuve. Je suis d'accord. Cependant, si la conformité pose problème, pourquoi avoir ce mécanisme de notation que vous avez imaginé, au lieu d'une simple réglementation stricte et d'une conformité rigoureuse qui auraient du mordant, avec des amendes qui auraient un effet dissuasif ou, pire, avec une culpabilité pénale?

Mme Sharon Polsky: Allez-y sur les deux fronts, pour que les organisations soient obligées de s'y conformer. Pensez à ce que Ralph Nader a fait il y a longtemps concernant l'industrie automobile. Certains ont qualifié cela d'humiliation publique.

Si vous ne savez pas comment une organisation se conforme, si elle se conforme ou dans quelle mesure elle se conforme, vous êtes dans le noir.

M. Matthew Green: Je serais d'accord.

Mme Sharon Polsky: Faites en sorte que l'organisation doive avouer publiquement.

M. Matthew Green: Vous avez mentionné que le projet de loi C-27 représente le statu quo, et je comprends. Il s'agit essentiellement de les obliger à utiliser un anglais simple, mais la responsabilité incombe toujours à la personne plutôt qu'à l'entreprise.

À votre avis, faudra-t-il davantage de dispositions législatives pour réglementer correctement les plateformes de médias sociaux?

Mme Sharon Polsky: Je pense qu'il existe déjà énormément de lois au pays qui traitent des problèmes de société et des problèmes liés à la nature humaine que nous constatons en ligne et dans les médias sociaux. Je ne sais pas si le fait d'avoir plus de lois — certainement pas plus de mauvaises lois — améliorera quoi que ce soit, donc la réponse est non.

Regardez les lois que nous avons déjà et appliquez-les.

M. Matthew Green: Vous pensez donc que ce que nous avons est suffisant.

Mme Sharon Polsky: Si les personnes en mesure de faire appliquer les lois avaient le pouvoir de les faire respecter, oui. Aujourd'hui, nous avons des gens qui ont la responsabilité, mais pas assez de pouvoir ou d'autorité ni de financement.

● (1750)

M. Matthew Green: Pour être clair, votre recommandation serait d'accroître le pouvoir de surveillance de ces plateformes, avec des mesures musclées qui incluent un renversement du fardeau de la preuve où la responsabilité incombe à l'entreprise, ainsi qu'une réglementation et/ou l'humiliation publique, pour assurer une meilleure surveillance des plateformes de médias sociaux.

Mme Sharon Polsky: Oui, mais je conteste ce que vous dites à propos du « renversement du fardeau de la preuve où la responsabilité incombe à l'entreprise ». Non, c'est une obligation qui lui échoit déjà selon la loi. Obligez-la à se conformer.

M. Matthew Green: Je devrais dire « renverser le fardeau de la preuve »...

Mme Sharon Polsky: Oui, renversez-le. Merci.

M. Matthew Green: ... parce qu'à l'heure actuelle, selon le statu quo, le fardeau incombe à la personne qui pourrait ne pas consentir ou être informée de la destination de ses données. Vous suggérez — à juste titre, j'ajouterais, à mon avis — que cette responsabilité soit imposée à ceux qui créent les algorithmes, communiquent l'information et, en fin de compte, en profitent.

Mme Sharon Polsky: C'est exact. Ils monétisent nos renseignements. Ce sont eux qui devraient prouver que ce qu'ils imposent à un public ignorant et peu méfiant est sûr et ne portera pas atteinte à la vie privée, à la sécurité et à la sécurité nationale.

M. Matthew Green: Merci.

Le président: Merci, monsieur Green.

Merci, madame Polsky, d'avoir comparu devant le Comité aujourd'hui. Cela met fin à notre deuxième série de questions. Au nom des Canadiens, j'aimerais vous remercier de l'information que vous avez fournie ainsi que de votre travail.

Nous allons suspendre la séance pendant quelques minutes. Nous allons revenir à huis clos. J'espère que ce sera rapide. Nous avons un problème de personnel dont nous devons discuter.

[*La séance se poursuit à huis clos.*]