



CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

44^e LÉGISLATURE, 1^{re} SESSION

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

TÉMOIGNAGES

NUMÉRO 095

Le lundi 4 décembre 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 4 décembre 2023

• (1535)

[Traduction]

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

Bienvenue à la 95^e réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes.

Conformément à l'article 108(3)h) du Règlement et à la motion adoptée par le Comité le mardi 31 janvier 2023, le Comité reprend son étude sur 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.

[Français]

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

[Traduction]

Je tiens à tous les membres du Comité de ne pas placer leurs oreillettes près des microphones, car cela pourrait causer de graves blessures à nos interprètes.

Je vais maintenant vous présenter les témoins qui se joignent à nous pour la première heure de séance. Nous accueillons M. Brett Caraway, professeur agrégé d'économie des médias à l'Université de Toronto, et Mme Emily Laidlaw, professeure agrégée et titulaire de la Chaire de recherche du Canada en droit de la cybersécurité à l'Université de Calgary, qui témoignent à titre personnel.

Avant de commencer, la sonnerie se fait entendre. J'ai obtenu le consentement unanime du Comité pour commencer la réunion pour entendre les déclarations préliminaires avant les votes. Je remercie les membres du Comité de leur indulgence afin que nous puissions entendre nos témoins.

Monsieur Caraway, vous avez cinq minutes, puis ce sera au tour de Mme Laidlaw.

M. Brett Caraway (professeur agrégé de l'économie des médias, University of Toronto, à titre personnel): Je tiens à remercier les membres du Comité de me donner l'occasion de prendre la parole aujourd'hui.

Je suis professeur agrégé de l'économie des médias à l'Université de Toronto. Je comparais aujourd'hui à titre personnel; les points de vue que j'exprime sont donc strictement personnels.

Je veux parler des risques que pose la structure incitative sous-jacente des plateformes de médias sociaux. J'espère ainsi vous donner une idée des changements qui se sont produits dans notre pay-

sage médiatique et des raisons pour lesquelles il y a, trop souvent, des divergences entre intérêt public et intérêts privés.

Les plateformes numériques sont des éléments importants de l'économie de l'information en raison de leur capacité de réduire les frictions sur le marché et les coûts de transaction. Pour comprendre ce dont je parle, imaginez l'utilité d'une application de médias sociaux comme Instagram pour rendre accessible un groupe d'utilisateurs donné, par exemple les photographes amateurs ou les passionnés de voyage, à des annonceurs qui veulent leur envoyer de la publicité ciblée.

Dans ce scénario, il y a en fait trois acteurs du marché: les utilisateurs, les annonceurs et l'exploitant de la plateforme, qui ont chacun leur propre ensemble d'incitatifs. Instagram a pour incitatif financier de maximiser le nombre d'utilisateurs et leur niveau de participation, ce qui rend la plateforme plus attrayante pour les annonceurs. De leur côté, les annonceurs veulent le plus de renseignements possible sur les utilisateurs de la plateforme afin de minimiser l'incertitude, tandis que les utilisateurs veulent simplement profiter des fonctionnalités de la plateforme avec le moins de perturbations possible.

Les marchés multilatéraux de ce genre n'ont rien de nouveau. Il s'agit d'une caractéristique des systèmes de communication de masse depuis le début de la vente d'espaces publicitaires dans les premiers bulletins d'information, dans les années 1600. Cependant, des termes comme « marketing de créneaux » et « publicité ciblée » sont loin d'être représentatifs de ce qui se passe réellement chaque fois que vous faites une recherche sur Google, que vous regardez une vidéo sur TikTok, que vous aimez la publication de quelqu'un sur Facebook ou que vous partagez un gazouillis. L'information est collectée, il y a des enchères et des messages commerciaux sont livrés.

Mes préoccupations ne sont pas principalement liées à l'escalade des tensions géopolitiques ou aux auteurs étrangers de menaces, bien que l'ingérence étrangère, la désinformation, la désinformation et la radicalisation soient toutes de légitimes préoccupations. Ce qui me préoccupe, c'est que ces plateformes, même lorsqu'elles fonctionnent exactement comme prévu, ont des répercussions négatives sur la sphère publique. Ce qui me préoccupe, c'est que les aspects économiques des plateformes garantissent pratiquement la propagation de la désinformation, les efforts pour influencer les comportements et l'érosion de la vie privée de la personne.

Mes préoccupations découlent du constat suivant: dans l'économie des plateformes, il n'existe aucune réelle limite supérieure à l'exploitation de l'attention humaine. Le mot « attention » renvoie peut-être à la capacité de se concentrer sur quelque chose, mais d'un point de vue sociétal, il renvoie à notre capacité collective de reconnaître les problèmes et les possibilités; à l'horizon de notre imagination et de notre créativité; à notre capacité d'être à la hauteur pour nous attaquer aux problèmes les plus criants du monde. L'attention est une ressource renouvelable, mais n'est pas comme toute autre ressource, en ce sens qu'on ne peut la stocker comme un métal précieux. On peut seulement l'orienter vers quelque chose. En fait, c'est la fonction économique de la publicité: accaparer l'attention limitée au détriment d'intérêts concurrents. La façon dont nous choisissons d'accorder notre attention est importante, tant pour les particuliers que pour la société. Notre attention façonne notre identité, qui nous pourrions devenir et où nous pourrions aller.

Les économistes parlent souvent de « la tragédie des biens communs ». L'origine du concept pose problème, mais comme métaphore, cela peut être très utile. Cela met en lumière notre propension, lorsque nous permettons l'accès sans entrave aux ressources limitées, à la surutilisation et à l'exploitation de ces ressources. Les plateformes numériques ne cherchent pas uniquement à mesurer l'attention, mais aussi à la modifier pour qu'elle se plie aux impératifs commerciaux. De nos jours, l'économie de l'attention ressemble moins à *Mad Men*, du réseau AMC et davantage aux transactions à vitesse vertigineuse sur les marchés financiers. Les principes économiques fondamentaux de ce système sont incompatibles avec des mesures rigoureuses de protection de la vie privée.

L'impératif économique primordial est la maximisation de la collecte de données, pas seulement pour la République populaire de Chine ou la Russie, mais aussi pour des entreprises américaines comme Alphabet, Meta, Amazon et une multitude de courtiers en données dont vous n'avez jamais entendu parler. Par conséquent, notre attention est épuisée, et sa qualité est réduite.

Nous avons des mesures de protection pour protéger d'autres ressources, notamment l'eau, l'air et l'habitat. Nous devons également gérer cette ressource renouvelable de la même manière, de manière durable, comme nous le ferions pour l'air, l'habitat et l'eau.

Le Canada est à un point d'inflexion. J'espère que nous pourrions prendre des mesures concrètes pour habiliter les Canadiens grâce à la création d'un cadre de réglementation exhaustif pour l'ensemble des plateformes numériques.

Merci.

• (1540)

Le président: Merci, monsieur Caraway.

Madame Laidlaw, vous avez cinq minutes pour présenter vos observations préliminaires au Comité. Allez-y, s'il vous plaît.

Mme Emily Laidlaw (professeure agrégée et titulaire de la Chaire de recherche du Canada en droit de la cybersécurité, University of Calgary, à titre personnel): Monsieur le président, je vous remercie de m'avoir invitée à prendre la parole devant le Comité.

Je suis honorée de vous parler depuis Calgary et le territoire traditionnel des peuples du Traité n° 7 et de la nation métisse de l'Alberta.

J'ai eu l'occasion d'écouter certains témoins et les discussions précédant ma comparution. Pendant le temps qui m'est imparti, j'aimerais revenir en arrière pour examiner les questions juridiques plus générales qui sont en jeu.

Mon message fondamental, c'est que ce n'est pas seulement une question de protection de la vie privée. La protection de la vie privée est une partie de l'équation. Par exemple, Discord n'utilise pas d'outils pour détecter le contenu montrant l'exploitation sexuelle d'enfants, ne surveille pas le contenu diffusé en direct et n'offre pas d'outils pour faire des signalements. C'est courir au désastre. C'est un problème de conception de la sécurité et non seulement un problème de protection de la vie privée.

C'est une question de réglementation des plateformes. La santé de notre écosystème de l'information dépend de plateformes privées et des choix que font ces entreprises quant à la conception de leurs produits, à la gouvernance d'entreprise, à la culture et aux systèmes de modération de contenu. Bref, les plateformes ont un pouvoir énorme.

Le Canada est actuellement à la traîne sur le plan de la réglementation des plateformes. Une loi sur les méfaits en ligne, que nous n'avons pas encore au Canada, réglerait bon nombre des aspects dont le Comité a discuté. L'Europe, le Royaume-Uni et l'Australie ont tous des lois pour lutter contre ces problèmes. Dans certains cas, ces lois en sont à leur deuxième ou troisième version. Le Canada n'a aucune loi fédérale visant la réglementation des plateformes. Nous pouvons tirer des leçons des avantages et désavantages de ces autres lois, mais il est temps d'agir maintenant.

De quoi avons-nous besoin et quels aspects exigent la prudence?

Premièrement, la réglementation des plateformes comporte des similitudes avec la protection de l'environnement, en ce sens que de nombreux domaines du droit doivent se conjuguer pour protéger notre sécurité et nos droits. En particulier, les lois sur la protection des renseignements personnels et les lois sur les méfaits en ligne se renforcent mutuellement. Nous avons donc besoin des deux. Par exemple, les algorithmes qui poussent du contenu préjudiciable le font grâce à la collecte de renseignements permettant d'identifier une personne, ce qui relève du droit relatif au respect de la vie privée. Toutefois, l'algorithme peut aussi utiliser des données agrégées anonymisées, ce qui ne relève pas du droit relatif au respect de la vie privée.

Les lois sur les méfaits en ligne permettent de mieux cibler les choix des plateformes en matière de conception de produits et de systèmes de modération de contenu. Les médias sociaux exploitent les données pour déterminer les préférences et les intérêts. Or il s'agit d'un aspect auquel les lois sur les méfaits en ligne peuvent remédier. On pense au fait que Meta amplifie le contenu émotif et toxique sur Facebook en accordant cinq fois plus de valeur aux réactions « colère » et « j'adore » qu'aux « j'aime ». Cela a alimenté la propagation de la désinformation et de la mésinformation.

Deuxièmement, les plateformes font partie de la solution. Elles peuvent être d'importants collaborateurs et innovateurs dans la résolution de problèmes. Toutefois, il y a une friction lorsque leur rôle s'apparente à celui d'un État. Certaines ont leurs propres équipes de sécurité nationale qui, essentiellement, établissent des politiques en matière de sécurité nationale.

Nous dépendons également des plateformes pour aller au-delà de la loi dans la lutte contre le contenu haineux, la désinformation et l'extrémisme violent, qui ne sont pas nécessairement illégaux. Toutefois, cela ne remplace pas une loi pour établir les normes de l'industrie. Les normes sont nécessaires. J'ai donné comme exemples des plateformes qui ont des structures de gouvernance relativement perfectionnées, mais il existe de nombreuses plateformes populaires qui font le minimum pour gérer les risques associés à leurs produits.

Troisièmement, lorsqu'il est question des risques de préjudice, il convient de préciser que les risques ne sont pas tous les mêmes. La protection des enfants, la propagande haineuse et terroriste, la désinformation et la violence ont chacune leur propre dynamique et ne devraient pas être regroupées sous une seule règle de droit, sauf l'idée fondamentale de la diligence raisonnable des entreprises.

En outre, toujours pour ce qui est des risques de préjudice, il faut savoir que cela comprend les risques pour les droits fondamentaux: le droit à la liberté d'expression, le droit à la vie privée et le droit à l'égalité. Toute analyse de solutions sur les plans du droit ou de la gouvernance doit être axée sur la protection et la promotion des droits. C'est un exercice particulièrement difficile lorsqu'il s'agit de s'attaquer à la mésinformation et la désinformation, puisqu'il est légal — sauf dans des cas très précis — de croire et de diffuser de fausses informations.

Cela dit, j'aimerais vous laisser sur cette note: quels sont les éléments de base nécessaires à l'élaboration d'une loi sur les méfaits en ligne?

Les plateformes devraient avoir l'obligation de gérer les risques de préjudices de leurs produits et de protéger les droits fondamentaux. Il devrait y avoir des obligations en matière de transparence assorties d'un mécanisme d'évaluation de cette transparence au moyen de vérifications et d'un accès aux données par des chercheurs approuvés. Il faut créer un organisme de réglementation chargé d'enquêter sur les entreprises et d'éduquer le public. En outre, les victimes devraient avoir accès à des recours, car le préjudice est à la fois collectif et individuel.

Merci. Je suis prête à répondre à vos questions.

• (1545)

Le président: Merci, madame Laidlaw.

Nous allons vous demander d'être patients, car il nous reste environ 11 minutes avant le vote. Cela devrait prendre encore une dizaine de minutes. Nous devrions donc être de retour dans 25 minutes pour notre première série de questions, si cela vous convient, si vous pouvez rester.

Je vais suspendre la séance pour le vote. Nous serons de retour tout de suite après.

Merci.

• (1545)

(Pause)

• (1610)

Le président: Nous reprenons nos travaux. Je constate qu'il y a clôture du débat et qu'un vote est imminent. Il nous reste environ 45 à 50 minutes. Nous avons entendu les déclarations préliminaires des témoins, et nous les remercions de leur patience.

Nous allons commencer notre première série de questions de six minutes avec M. Kurek.

M. Damien Kurek (Battle River—Crowfoot, PCC): Merci beaucoup, monsieur le président, et merci à nos témoins.

Je vous suis également reconnaissant d'avoir formulé un certain nombre de suggestions pratiques dans vos déclarations. Comme toujours, si vous avez des choses à ajouter, n'hésitez pas à nous les transmettre.

Monsieur Caraway, j'ai trouvé fort intéressants certains de vos travaux, car l'économie des médias sociaux est sans aucun doute un sujet fascinant. C'est l'équilibre entre un service perçu comme gratuit et le coût associé à une chose dont les coûts d'exploitation sont très élevés, comme une plateforme de médias sociaux. Sur les plans de la réglementation et de la gestion, comment peut-on établir un équilibre entre le désir du consommateur, qui est d'avoir un service gratuit, et les exigences associées à l'exploitation d'une énorme plateforme Web?

• (1615)

M. Brett Caraway: C'est une excellente question.

Ce que je dis toujours à mes étudiants, c'est que rien n'est gratuit. Même si vous semblez obtenir ces services gratuitement, s'il s'agit d'un modèle financé par la publicité, vous payez pour ce service plus tard lorsque vous achetez des biens ou des services.

La plupart des plateformes du monde des médias sociaux dont nous parlons sont exploitées comme des marchés multilatéraux. Il est assez difficile de satisfaire tout le monde. Comme je l'ai évoqué, on tente de satisfaire les annonceurs, mais ils veulent le plus d'informations possible sur les utilisateurs. Les utilisateurs veulent simplement qu'on les laisse utiliser la plateforme librement sans vouloir nécessairement payer pour cela non plus. Ce n'est jamais populaire, sauf dans certains contextes, peut-être, notamment les services de diffusion en continu en ligne comme Spotify ou Netflix. Cependant, même dans les modèles par abonnement, une entreprise comme Netflix, qui ne collecte pas nécessairement le même genre de données que des entreprises comme Meta ou Alphabet, collecte aussi des données sur la façon dont les abonnés utilisent la plateforme et déploient l'intelligence artificielle pour les systèmes de recommandation, etc.

Du côté des annonceurs, il y a toujours un impératif économique pour demander plus de données et, par conséquent, les exploitants de plateformes collecteront plus de données. Je pense que cela témoigne de la nécessité d'une intervention du gouvernement pour dire: « Eh bien, voici les droits énumérés dont nous tenons compte, notamment la protection de la vie privée des citoyens ». Je ne parle pas uniquement de les inclure dans un préambule, mais de les inscrire dans des critères juridiques, donc...

M. Damien Kurek: Je suis désolé, mais notre temps est très limité.

J'aimerais que vous reveniez — en une trentaine de secondes, car j'aimerais poser d'autres questions — sur le contexte précis de la protection des enfants. Pourriez-vous en dire davantage sur le rôle que cela peut avoir pour assurer la protection des enfants contre les préjudices en ligne? À quoi cela ressemble-t-il dans le contexte des jeunes?

M. Brett Caraway: La protection des mineurs doit faire partie du libellé du projet de loi C-27. On entend les représentants de TikTok dire qu'ils ont un mécanisme d'autoréglementation et qu'ils sont à l'avant-garde à cet égard. Ils diront que les personnes de moins de 18 ans ne peuvent pas faire de diffusion en direct, que les paramètres de confidentialité sont établis par défaut à 16 ans et moins, ou encore que les 16 ans et moins sont limités à 60 minutes. Cependant, ces paramètres peuvent simplement être modifiés.

Il est important que le gouvernement intervienne et aide les parents, car ils sont littéralement submergés par toutes les différentes plateformes de médias sociaux et, évidemment, les adolescents utilisent ces plateformes, selon la personne à qui l'on pose la question, de quatre à cinq heures par jour.

M. Damien Kurek: Merci beaucoup. Je souligne simplement que la formulation « aider les parents » est très bien choisie.

Madame Laidlaw, nous parlons de la protection des jeunes. Les médias sociaux regorgent de préjudices: de l'intimidation aux types d'exploitation les plus odieux, comme les crimes associés à la traite de personnes, au matériel d'exploitation des enfants, par exemple.

Dans le contexte des médias sociaux et des jeunes, en quoi consiste le rôle du gouvernement pour l'élaboration de la réglementation? Quel est le rôle des plateformes de médias sociaux pour tenter de créer des cadres remédiant aux innombrables défis potentiels?

Il reste un peu plus d'une minute, et je sais que c'est une question complexe. J'espère que vous avez suffisamment de temps pour faire part de vos commentaires au Comité.

Mme Emily Laidlaw: Merci.

C'est une question énorme, mais c'est la question qui vaut cher.

Je serai concise et je dirai qu'il est essentiel que le gouvernement joue un rôle, parce que jusqu'à maintenant, nous nous sommes surtout fiés à l'autogouvernance des entreprises, qui ne fonctionne pas. Toutes sortes de méfaits sont commis en ligne.

Ce dont nous avons besoin, c'est d'un organisme de réglementation, qui pourrait intervenir avec plus d'agilité. Il est trop lourd de porter certaines de ces préoccupations devant les tribunaux. Nous avons besoin d'aide pour établir des pratiques. Chaque plateforme est différente, alors elles doivent vraiment trouver des solutions pour leurs sites. Or, il doit y avoir une procédure pour leur demander des comptes. Elles doivent démontrer à un organisme de réglementation les mesures qu'elles prennent pour protéger les enfants.

Je pense que nous devons départager les préjudices. Pensons aux mesures pour protéger les enfants. Le visionnement d'images d'exploitation sexuelle d'enfants et d'abus intimes ainsi que la traite de personnes constituent des crimes. Puis, il y a les principaux acteurs qui, dans la mesure où ils peuvent être trouvés et poursuivis, devraient être les cibles. Cependant, les plateformes devraient avoir une responsabilité distincte et des obligations uniques.

En ce qui concerne les enfants...

• (1620)

Le président: Merci, madame Laidlaw.

Je suis désolé. La pire partie de mon travail consiste à interrompre les intervenants.

Madame Khalid, vous avez six minutes. Allez-y, s'il vous plaît.

Mme Iqra Khalid (Mississauga—Erin Mills, Lib.): Merci beaucoup, monsieur le président.

Madame Laidlaw, vous avez parlé de solutions concernant les entreprises de médias sociaux. Vous pourriez peut-être terminer vos réflexions sur la question de M. Kurek et également formuler des commentaires sur ce que vous pensez être de bonnes solutions que les entreprises de médias sociaux peuvent examiner et pour lesquelles elles peuvent établir des pratiques exemplaires.

Mme Emily Laidlaw: À titre de précision, demandez-vous des solutions du point de vue de la gouvernance d'entreprise ou des lois que nous devrions adopter?

Mme Iqra Khalid: Je parlais des deux, en fait.

Mme Emily Laidlaw: D'accord.

Premièrement, il s'agit d'une question juridique, et le gouvernement doit adopter une loi sur les préjudices en ligne, parce qu'il doit établir les obligations des entreprises. Essentiellement, il doit établir des normes minimales. Les entreprises elles-mêmes, cependant, peuvent commencer à prendre plus au sérieux la protection des enfants.

Je pense que l'un des problèmes, c'est qu'une grande partie de la transparence que nous voyons actuellement a tendance à être davantage un exercice de marketing. Je pense que les compagnies ne sont pas aussi franches au sujet de certaines pratiques. C'est un aspect clé, bien sûr, dont M. Caraway a parlé: l'économie de l'attention.

En ce qui concerne les enfants en particulier, je pense que nous devons considérer ces pratiques comme de la manipulation des esprits. Par le passé, le milieu publicitaire recourait à des interventions pour protéger les enfants contre la manipulation de l'esprit. Certaines publicités n'étaient pas diffusées à certains moments de la journée ou pendant les émissions pour enfants. La même chose se passe sur les médias sociaux: on promeut le contenu suicidaire, le contenu sur les troubles de l'alimentation et ainsi de suite.

Il est essentiel que ces plateformes, par leur conception... Il faut se demander comment une plateforme est conçue. Comment les algorithmes promeuvent-ils le contenu? Comment encourage-t-on certains comportements? Les plateformes doivent se pencher sur ces réalités et rendre des comptes, alors je pense qu'on devrait leur imposer des responsabilités particulières entourant les enfants.

Mme Iqra Khalid: Merci beaucoup.

Monsieur Caraway, avez-vous quelque chose à dire au sujet des observations de Mme Laidlaw sur le type d'économie par rapport à la manipulation des esprits ou à la modification du comportement des consommateurs? Quel rôle le gouvernement doit-il jouer à cet égard sur le plan de la réglementation? Je comprends que nous ne pouvons pas simplement créer de la réglementation que les mauvais acteurs ne respectent pas toujours. Selon vous, quel rôle le gouvernement doit-il jouer dans cet équilibre entre l'économie, l'efficacité et la manipulation des esprits?

M. Brett Caraway: Un élément qui, selon moi, est vraiment important... en fait, il y en a deux, en quelque sorte.

Je pense que nous devons nous pencher très attentivement sur ce qui constitue un consentement éclairé. Ce qui me pose problème, c'est que non seulement les enfants, mais aussi les utilisateurs moyens doivent composer avec des contrats de licence d'utilisateur final tellement alambiqués que quelqu'un comme Mme Laidlaw doit les débroussailler. Ils nécessitent énormément d'expertise et peuvent changer presque quotidiennement. Je pense qu'il importe de revoir ce qui représente vraiment du consentement dans ce contexte.

Puis, il y a la transparence et la façon dont les données sont utilisées. C'est un enjeu pour lequel il faut pouvoir compter sur un intervenant comme un commissaire à la protection de la vie privée, qui peut envoyer un vérificateur indépendant pour voir ce qui se passe réellement en coulisses.

Enfin, je dirais que les pénalités doivent avoir un effet. Oui, 25 millions de dollars semblent représenter une grande somme, mais ce n'est peut-être pas extraordinaire pour Meta ou Alphabet, alors que 5 % des revenus mondiaux sembleraient plus sérieux. J'appuie aussi ce genre d'approche.

• (1625)

Mme Iqra Khalid: Merci.

Depuis les dernières années, les médias sociaux sont utilisés comme plateforme de promotion, de prise de parole et d'expression, non seulement au Canada, mais aussi dans le monde entier. Il y a quelques années, sur TikTok, nous avons vu une jeune femme se maquiller et parler d'enjeux de façon à contourner les algorithmes sur ce qui était dit ou affiché.

Où est le lien entre les médias sociaux et la liberté d'expression, et comment veille-t-on à ce que les enfants au Canada puissent également naviguer en sécurité dans cet espace?

M. Brett Caraway: Qui aimerait répondre à cette question?

Mme Iqra Khalid: J'aimerais d'abord entendre vos commentaires, monsieur Caraway, puis je passerai à Mme Laidlaw.

Le président: Il nous reste environ une minute. Allez-y, monsieur Caraway.

M. Brett Caraway: Puisque la question porte sur la liberté d'expression, Mme Laidlaw voudrait peut-être répondre à cette question, au lieu de moi.

Mme Emily Laidlaw: Merci, monsieur Caraway.

Je dirais que la liberté d'expression est fondamentale. Si vous adoptez une loi qui ne fait que mettre l'accent sur les préjudices, vous incitez les entreprises à mettre en place des solutions rudimentaires qui, en fait, entraîneront des conséquences fortuites. Beaucoup de preuves démontrent que l'effet inverse peut se produire: ce sont les voix racisées et d'autres voix marginalisées qui finissent par être réduites au silence.

En ce qui concerne les exigences imposées aux entreprises, si nous nous soucions des préjudices, nous nous soucions des préjudices brimant les droits. Il faut donc que les entreprises de médias sociaux aient deux priorités. Elles doivent se concentrer sur la protection et la promotion de la liberté d'expression et elles doivent démontrer les mesures prises à un organisme de réglementation. Elles doivent démontrer que les mesures qu'elles prennent sont adaptées à leurs contextes et à leurs services.

Mme Iqra Khalid: Merci beaucoup.

Je suis désolée, madame Laidlaw. Je ne me suis pas adressée à vous comme je l'aurais dû. C'est une erreur de ma part.

Mme Emily Laidlaw: Je ne l'avais même pas remarqué, mais je vous remercie.

Le président: Merci, madame Khalid.

[Français]

C'est maintenant au tour de M. Villemure.

[Traduction]

Avant de poursuivre avec M. Villemure, je veux m'assurer que nos invités ont activé l'interprétation, s'ils en ont besoin.

[Français]

Monsieur Villemure, vous avez la parole pour six minutes.

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

Je remercie nos deux témoins de se joindre à nous aujourd'hui. Leur réputation les précède.

Je vais d'abord m'adresser à Mme Laidlaw.

Je pense que vous n'êtes pas une adepte de l'autoréglementation, n'est-ce pas?

[Traduction]

Mme Emily Laidlaw: Non, effectivement, mais je crois au fait de laisser les entreprises trouver elles-mêmes les solutions.

[Français]

M. René Villemure: Si on vous demandait, aujourd'hui, de créer un régulateur, en espérant que ce ne soit pas le CRTC, que suggériez-vous?

[Traduction]

Mme Emily Laidlaw: Je recommande de créer un organisme de réglementation de la sécurité en ligne qui aurait le devoir d'enquêter sur les entreprises et de vérifier si elles se conforment à des obligations précises. Je pense que l'obligation devrait être d'agir de façon responsable avec, peut-être, un devoir particulier de diligence à l'égard des enfants.

Je pense que l'organisme de réglementation devrait également jouer un rôle d'éducation très important auprès du public. Nous nous sommes rendu compte qu'une grande partie de la solution consiste à améliorer la capacité et la compréhension du public et aussi à demander des comptes aux entreprises.

[Français]

M. René Villemure: Cet organisme de réglementation serait-il comme le commissaire aux conflits d'intérêts et à l'éthique ou le commissaire au lobbying, c'est-à-dire une personne nommée par le Parlement? Serait-il plutôt le fonctionnaire d'un ministère?

[Traduction]

Mme Emily Laidlaw: Je pense qu'il est absolument essentiel que cet organisme de réglementation soit indépendant du gouvernement. Il s'apparenterait davantage au commissariat à la protection de la vie privée, parce qu'on créerait un organisme de réglementation des droits de la personne numériques. Un tel commissariat doit se dissocier de toute pression pour trouver le juste équilibre entre les droits. Son travail doit se faire dans une perspective juridique et de la responsabilité des entreprises. De plus, il doit avoir le pouvoir d'imposer des sanctions pécuniaires assez salées, comme M. Caraway l'a mentionné.

• (1630)

[Français]

M. René Villemure: Justement, les pénalités dont on parlait un peu plus tôt devraient être un pourcentage des revenus plutôt qu'une amende de 25 000 \$, qui est insignifiante dans les circonstances.

Vous avez beaucoup parlé d'éducation également. Tous les témoins que nous avons entendus, y compris les représentants de la police, ont parlé d'éducation. Cependant, au bout du compte, personne ne nous dit qui devrait éduquer qui. Peut-être ce nouvel organisme de réglementation pourrait-il avoir pour mission cette éducation, qui pourrait être faite à l'école même, puisqu'on parle de jeunes.

Comment voyez-vous cette éducation, que tout le monde favorise, sans toutefois trouver de solution, pour l'instant?

[Traduction]

Mme Emily Laidlaw: Je pense qu'il est essentiel que l'éducation se fasse par l'entremise de l'organisme de réglementation, comme nous le voyons en Australie avec le commissaire à la sécurité électronique. Je pense que ce serait le modèle à suivre ici pour un organisme de réglementation chargé de l'éducation.

Je prône cette approche en partie parce que l'éducation à l'échelle du pays et dans les différentes écoles et collectivités varie beaucoup, et encore faut-il que les gens demandent de l'information. Il faut que les écoles fassent appel aux bonnes personnes. À l'heure actuelle, beaucoup d'interventions font simplement peur aux enfants ou aux parents, et la plupart des études démontrent que c'est inefficace. J'ai essayé de transmettre ce message à l'école de mes enfants, et la direction s'est montrée très réceptive.

Je pense que l'éducation est à ce point essentiel dans ce dossier qu'elle doit s'inscrire dans le mandat de l'organisme de réglementation.

[Français]

M. René Villemure: L'organisme de réglementation pourrait avoir le pouvoir d'aller jusque dans les écoles afin d'implanter ce genre d'éducation, n'est-ce pas?

[Traduction]

Mme Emily Laidlaw: C'est une question intéressante au sujet des pouvoirs du gouvernement fédéral et des provinces: on pourrait certainement établir le programme à enseigner et fournir les ressources qui, espérons-le, influenceraient les programmes des différentes écoles et même des municipalités. Je suppose que l'objectif est que l'intérêt devienne contagieux. En fin de compte, ce dossier comporte un volet provincial, alors si des organismes de réglementation provinciaux commencent à voir le jour, ils pourraient peut-

être travailler ensemble, un peu comme les commissaires à la protection de la vie privée.

[Français]

M. René Villemure: Moi, je suis un apôtre friand du respect des compétences provinciales.

Vous avez dit plus tôt que le Canada était en retard sur le plan de la législation des lois numériques.

Est-il trop tard?

Je connais bien la loi européenne. On peut faire du rattrapage, mais est-il trop tard?

[Traduction]

Mme Emily Laidlaw: Nous ne sommes pas en retard pour l'instant, mais nous le serons bientôt si nous n'adoptons pas de lois. L'Europe et le Royaume-Uni viennent d'adopter leur loi sur la sécurité en ligne — la législation sur les services numériques — plus tôt cette année ou au cours de la dernière année, et ils sont en train de la mettre en œuvre.

Dans cinq ans, je pense que nous verrons des enquêtes mondiales plus coordonnées sur les entreprises, ce qui réglerait certains des problèmes transfrontaliers. Si le Canada ne fait rien en ce sens au cours de la prochaine année, je pense qu'il accusera un sérieux retard. Cependant, à l'heure actuelle, nous avons l'avantage de ne pas avoir été les premiers à agir.

[Français]

M. René Villemure: Dites-moi, 30 secondes, êtes-vous en faveur du projet de loi C-27 dans son état actuel?

[Traduction]

Mme Emily Laidlaw: J'appuie entièrement les recommandations d'amendements du commissaire Dufresne au projet de loi C-27. Je pense qu'il faut l'amender: le projet de loi ne résout qu'une partie du problème, car il s'appuie toujours sur un paradigme de consentement. De plus, tant qu'il s'appuiera sur le consentement, il n'abordera pas certains des aspects les plus problématiques des médias sociaux et de leur influence, auxquels, en réalité, personne ne peut consentir.

Par conséquent, à moins de revoir complètement le projet de loi C-27 — ce qui, à mon avis, n'arrivera pas —, nous aurons besoin d'une loi sur les préjudices en ligne. Je suis d'avis que la Loi sur l'intelligence artificielle et les données pose problème et doit être retirée du projet de loi C-27 et retravaillée. Il ne devrait absolument pas y avoir de commissariat relevant d'Innovation, Sciences et Développement économique Canada.

[Français]

M. René Villemure: Merci beaucoup.

Le président: Merci, monsieur Villemure.

[Traduction]

Étant donné l'heure et les votes, je propose — et je veux que vous y réfléchissiez également — que nous accordions six minutes à M. Green. Nous allons avoir besoin d'un peu de temps pour passer au prochain groupe de témoins. Nous pourrions entendre les déclarations liminaires. Je m'attends à ce qu'il y en ait deux dans le prochain groupe de témoins.

Cela nous amènerait à peu près à l'heure des votes, mais cette série de questions se terminerait après l'intervention de M. Green. J'invite nos témoins à nous envoyer toute réflexion supplémentaire qu'ils pourraient avoir.

Monsieur Green, vous avez six minutes.

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

J'aimerais revenir sur certains points, surtout à propos du projet de loi C-27. Personnellement, je pense qu'il aurait mieux valu aborder cette partie du projet de loi dans un cadre éthique plutôt que dans un cadre de l'industrie.

Madame Laidlaw, pouvez-vous nous parler de l'aspect éthique entourant l'intelligence artificielle, ou IA? Pour quelle raison, du point de vue juridique, les considérations sur la légitimité de la démocratie et sur les façons dont l'IA mine la société devraient-elles probablement être abordées dans un texte distinct, comme vous venez de le suggérer?

• (1635)

Mme Emily Laidlaw: C'est une excellente question. Merci.

Je pense que nous avons vu, au cours de la dernière année, les transformations sociales que peut entraîner l'IA, et ce n'est que le début. Le problème avec la Loi sur l'intelligence artificielle et les données, dans sa forme actuelle, c'est qu'elle n'est pas suffisamment étoffée pour nous permettre de faire face aux différents problèmes qui nous attendent. Elle doit être séparée du reste afin que nous puissions avoir une discussion réfléchie sur les façons d'utiliser l'IA qui peuvent perturber fondamentalement la démocratie, miner notre capacité de prendre des décisions et créer des risques physiques pour nous, individuellement ou collectivement.

Nous devons dresser la liste de ces divers risques et possibilités et rédiger un projet de loi en conséquence. Je pense que le modèle européen peut nous aider. Toutefois, dans sa forme actuelle, la Loi sur l'intelligence artificielle et les données doit être modifiée.

M. Matthew Green: Je veux entrer dans les détails.

Vous avez parlé de l'affaiblissement de la démocratie. Je vais parler du cas de Cambridge Analytica, dans lequel nous savons que Facebook n'a pas effectué une surveillance suffisante pour s'assurer que l'utilisation des données était conforme à ses propres conditions de service.

Je crois vous avoir entendu dire dans votre témoignage que l'autoréglementation de l'industrie est un problème, mais qu'elle pourrait être en mesure de présenter certaines solutions.

Dans quelle mesure avons-nous la certitude que les entreprises de médias sociaux comprennent parfaitement comment leurs données sont utilisées et qu'elles sont adéquatement protégées? De plus, pensez-vous qu'elles savent que les données sont détournées et qu'elles permettent cette mauvaise utilisation, tout simplement?

Mme Emily Laidlaw: Je pense que c'est un peu des deux. Selon moi, elles ne donnent pas un portrait complet de la situation. Elles ne savent pas tout ce qui se passe.

Par exemple, un de mes collègues, Joel Reardon, a fait l'ingénierie inverse de diverses applications qui sont censées être dotées de toutes les mesures de protection de l'enfance. La conclusion est que de nombreuses applications n'offrent pas de telles mesures.

Essentiellement, nous attendons que les problèmes soient révélés au grand jour, puis qu'un scandale éclate. C'est tout simplement nettement insuffisant. La transparence à elle seule ne change absolument rien. Nous avons besoin d'un mécanisme pour enquêter et vérifier ces entreprises, pour lever le voile sur elles. Autrement, nous nous retrouvons avec une crise comme celle de Cambridge Analytica.

M. Matthew Green: Revenons à cela.

À votre avis, le gouvernement fédéral pourrait-il, par l'entremise de lois et de règlements, mieux protéger les renseignements personnels recueillis et utilisés par ces plateformes?

Mme Emily Laidlaw: Je pense qu'une chose que nous devons examiner de plus près est la définition des zones interdites. Certaines formes de collecte de données devraient être considérées comme totalement inappropriées. Je pense que nous nous en remettons encore tellement sur le consentement qu'il a...

M. Matthew Green: Pouvez-vous nous donner quelques exemples, dans le cadre de votre témoignage?

Mme Emily Laidlaw: Les conditions d'utilisation des médias sociaux en sont un exemple. Nous acceptons la collecte de toutes sortes de données à n'importe quelle fin parce que nous voulons utiliser cette application. La plupart des études révèlent que ce que nous subissons tous est une fatigue concernant la vie privée, où nous savons essentiellement que c'est mauvais pour nous, mais nous l'acceptons quand même. C'est vraiment paternaliste et c'est là le problème. Ce que nous disons essentiellement, c'est que les gens ne devraient pas donner leur accord parce qu'ils ne comprennent pas vraiment ce qu'ils acceptent. Les données sont ensuite vendues à des courtiers en données, dont a parlé M. Caraway, et nous perdons alors le contrôle. Nous ne savons pas vraiment ce qu'il advient des données.

La Californie fait un meilleur travail, avec sa loi, en disant essentiellement qu'il faut être en mesure de suivre ces données et à qui elles sont destinées. Si vous vous appuyez sur le consentement, vous pouvez le retirer et savoir où vont ces données. Ce sont là autant de pistes pour les lois sur la protection des données et des renseignements personnels.

M. Matthew Green: C'est très utile et cela me permet de passer à M. Caraway.

Vous avez mentionné que certaines applications de médias sociaux adoptent une approche de collecte de données bancale. Pouvez-vous nous dire quelles applications adoptent cette approche et si notre loi actuelle offre une protection suffisante?

M. Brett Caraway: De nombreuses données sont recueillies par les entreprises sociales les plus importantes. C'est tout le monde, de Facebook... J'inclus Google, Instagram et TikTok. Elles recueillent tout ce que vous publiez — c'est-à-dire toutes vos données personnelles — et suivent également toutes vos données dites transactionnelles et vos données relatives aux interactions.

Facebook a du succès parce qu'il est capable d'exploiter vos liens sociaux à grande échelle. Google a du succès car il peut exploiter votre intention d'achat à grande échelle.

M. Matthew Green: Quand vous dites « à grande échelle », pour la gouverne du public et pour les témoignages, que voulez-vous dire?

• (1640)

M. Brett Caraway: Elles peuvent prendre ces renseignements, les utiliser dans un contexte numérique, les conditionner à un coût marginal presque nul et les vendre ensuite à des courtiers en données.

Cambridge Analytica est un excellent exemple, car la collecte initiale de données n'a pas violé les conditions de Facebook à l'époque. Un accord d'échange réciproque de données était en place. Ce n'est que lorsque l'application « This is Your Digital Life » a divulgué ces données à Cambridge Analytica que le véritable scandale a eu lieu, car c'est ainsi qu'elles...

M. Matthew Green: Il me reste 20 secondes.

Connaissez-vous des restrictions sur l'utilisation des données? Pouvons-nous, en tant que personnes, limiter ou savoir comment nos données sont utilisées?

M. Brett Caraway: La plupart des dispositions actuelles sont les mêmes que celles qui figurent dans la LPRPDE depuis l'an 2000, je suppose, et c'est la raison pour laquelle nous la réexaminons aujourd'hui.

Ce dont nous avons besoin actuellement, c'est d'un droit à la vie privée énuméré qui fasse partie d'un critère juridique lorsque l'on envisage une injonction ou une amende.

M. Matthew Green: C'est très utile.

Merci.

Le président: Merci, monsieur Green. Je suis ravi que vous ayez surveillé le temps, car nous avons appuyé sur le mauvais bouton sur le téléphone et nous avons perdu le compte. Vous auriez pu avoir deux minutes de plus si vous l'aviez voulu.

Tout d'abord, je tiens à remercier nos invités d'être venus aujourd'hui. Comme je l'ai mentionné plus tôt, si vous souhaitez soumettre d'autres renseignements au Comité dans le cadre de l'étude du rapport, veuillez les faire parvenir à la greffière.

Je tiens avant tout à m'excuser pour les perturbations d'aujourd'hui et de la semaine dernière. Je ne me sentais pas très bien. Je vous suis reconnaissant de la patience dont vous avez fait preuve en revenant au Comité cette semaine et en nous communiquant les renseignements que vous avez fournis.

Merci, madame Laidlaw et monsieur Caraway.

Nous allons suspendre la séance quelques minutes. Nous reviendrons avec le nouveau groupe de témoins pour entendre leurs déclarations liminaires. Nous avons un peu de temps pour cela, alors suspendons nos travaux une minute ou deux.

Merci.

• (1640)

(Pause)

• (1645)

Le président: Nous allons reprendre la séance. J'aimerais souhaiter un bon retour à tout le monde.

J'aimerais maintenant souhaiter la bienvenue aux témoins pour la deuxième partie de notre réunion d'aujourd'hui.

À titre personnel, nous recevons M. Matt Malone, professeur adjoint à la Thompson Rivers University. Bienvenue, monsieur Ma-

lone. De l'organisation The Dais, nous accueillons Sam Andrey, directeur général, et Joe Masoodi, analyste principal des politiques.

Je vous informe que des votes auront lieu. Nous disposons d'environ 27 minutes, alors nous allons commencer avec les déclarations liminaires. Nous suspendrons la séance, puis nous reviendrons pour les questions et réponses. Je vous remercie de votre patience à cet égard.

Monsieur Malone, vous avez au plus cinq minutes pour faire votre exposé au Comité.

Allez-y, monsieur, s'il vous plaît.

M. Matt Malone (professeur adjoint, Thompson Rivers University, à titre personnel): Merci, monsieur le président.

Je suis Matt Malone, et je suis un professeur adjoint à la faculté de droit de la Thompson Rivers University à Kamloops. J'assiste aujourd'hui à la réunion à titre personnel.

Je vais utiliser mes remarques liminaires pour vous faire part de mes réflexions à l'aide d'une étude de cas, qui concerne plus précisément l'interdiction sélective de TikTok sur les appareils émis par le gouvernement qui a été annoncée en février 2023. Comme le Comité s'en souvient peut-être, cette interdiction sélective était accompagnée d'une déclaration sur les préoccupations relatives à la protection de la vie privée et à la sécurité.

Ces préoccupations déclarées n'expliquent pas plusieurs choses. Tout d'abord, elles n'expliquent pas pourquoi le gouvernement a attendu cinq mois pour intervenir en ce qui concerne la note d'information sous-jacente qui mettait en garde contre les pratiques de TikTok. Ensuite, elles n'expliquent pas pourquoi le gouvernement continue d'acheter de la publicité sur TikTok. Enfin, elles n'expliquent pas pourquoi le gouvernement a ignoré que TikTok n'est pas la seule application qui conserve les données de ses utilisateurs dans les instances étrangères et les divulgue potentiellement à des régimes étrangers.

Comme le Secrétariat du Conseil du Trésor me l'a confirmé quelques jours avant cette audience, aucune des applications suivantes n'est interdite de téléchargement et d'utilisation sur les appareils émis par le gouvernement: l'application de médias sociaux VKontakte affiliée à la Russie, l'application Yandex associée à la Russie, l'application Mail.ru, ainsi que d'autres applications de médias sociaux comme Facebook, Instagram, Tinder, Snapchat, Bumble, Grindr, Truth Social, Gab et Discord, qui ont été impliquées dans les fuites du Pentagone de 2022-2023 et qui, selon Mme Laidlaw, ne disposent pas de mesures de protection de la sécurité des enfants.

Comme je l'ai recommandé dans un article publié récemment — et je vais profiter de l'occasion pour le recommander à nouveau au président du Conseil du Trésor —, je pense qu'une meilleure protection de la vie privée et de la sécurité consisterait à ce que le gouvernement interdise toutes les applications de médias sociaux sur les appareils fournis par le gouvernement, à moins qu'il n'y ait une justification commerciale solide. Je trouve incroyable que les applications que je viens d'énumérer ne soient pas interdites sur les appareils fournis par le gouvernement. Je pense également que le gouvernement devrait cesser d'acheter des publicités sur tous les services de médias sociaux.

Même avec de telles interdictions en place, il convient de noter que la loi fédérale en matière de protection de la vie privée n'impose aucune contrainte significative sur les transferts de données vers des pays tels que la Russie et la Chine. Une note interne du gouvernement que j'ai obtenue grâce à la Loi sur l'accès à l'information fait état que le projet de loi C-27 et la loi sur la protection des renseignements personnels dont le Parlement est actuellement saisi évitaient d'intégrer dans ce projet de loi de nouvelles restrictions ou des restrictions de type européen sur le transfert transfrontalier de renseignements personnels, surtout par respect pour les intérêts commerciaux. Il est très révélateur que le projet de loi sur la vie privée dont le Parlement est saisi soit géré par le portefeuille de l'industrie au sein du cabinet, et non par un portefeuille des droits de la personne, de la sécurité publique ou de la sécurité nationale.

Comme de nombreuses applications de médias sociaux, TikTok mérite l'opprobre pour ses violations de la vie privée, de ses pratiques de collecte de données et de contrôle du discours, et pour avoir donné l'accès à des données malgré avoir fourni des assurances. Comme d'autres applications de médias sociaux, TikTok est un vecteur de préjudice en ligne pour les jeunes. Son modèle économique est axé sur la publicité ciblée qui porte atteinte à la vie privée et exacerbe la crise de la santé mentale qui touche les jeunes. Les fonctions de sécurité de l'application pour les enfants sont toutes faciles à contourner.

Par l'entremise de diverses demandes d'accès à l'information, j'ai vu plusieurs séances d'information internes où les acteurs du gouvernement canadien ont relevé ces problèmes à maintes reprises. Je serais heureux d'en parler.

Toutefois, il est important de noter que le vrai coupable ici est la loi canadienne, car elle n'empêche pas ces pratiques pour TikTok ou tout autre service de médias sociaux. Comme l'ont souligné à plusieurs reprises les lobbyistes de TikTok qui ont comparu devant ce comité, le traitement par TikTok des données des utilisateurs canadiens est régi par le droit canadien. Et c'est là où le bât blesse. Les lois canadiennes sur la protection des renseignements personnels ne respectent pas les droits et les intérêts des individus et des collectivités à l'ère numérique. L'application de ces lois est pratiquement inexistante. Au niveau fédéral, le Commissariat à la protection de la vie privée est devenu habile à annoncer en fanfare ses enquêtes, mais il est très lent à enquêter, comme je l'ai appris dans ma propre plainte concernant l'application ArriveCAN, qui a finalement été retenue.

Les forces de l'ordre ont également eu du mal à s'adapter au nouveau paysage numérique. Le système national de signalement de la cybercriminalité et de la fraude de la GRC, dont ce comité a récemment entendu parler en termes élogieux dans le cadre de cette étude, a en fait deux ans de retard et est toujours à l'étape des essais bêta. Son site Web indique qu'il n'accepte que 25 plaintes par jour dans tout le pays.

Pour donner aux députés un autre exemple, comme je l'ai appris lors d'une récente demande d'accès à l'information, l'équipe d'enquête sur la cybercriminalité de la GRC ne compte que huit employés pour l'ensemble de l'Alberta. En Colombie-Britannique, où s'est déroulée récemment une tragique affaire d'extorsion sexuelle d'un jeune sur les médias sociaux, l'équipe d'enquête sur la cybercriminalité ne compte que quatre employés pour l'ensemble de la province. Il n'y en a aucun en Saskatchewan, au Manitoba ou dans les provinces maritimes.

Avec une loi sur la protection de la vie privée et des données qui prive les citoyens d'une protection significative, des priorités de financement du gouvernement en profond décalage avec les valeurs déclarées et les besoins réels, et des lacunes dans la loi et la politique que le gouvernement ne montre aucune urgence à combler, les politiques et les pratiques du gouvernement fédéral posent des défis importants pour répondre aux types réels de préjudices que nous voyons se perpétuer ces jours-ci sur les médias sociaux.

● (1650)

Pour conclure, je tiens à remercier le Comité de son invitation inattendue.

Je tiens également à remercier tout particulièrement la députée de Mississauga—Erin Mills du leadership dont elle a fait preuve dans ce dossier très important. J'ai été très impressionné par son travail dans ce dossier.

Je me ferai un plaisir de répondre, du mieux que je peux, à toutes les questions que les membres du Comité pourraient avoir.

Merci.

Le président: Merci, monsieur Malone. Nous vous sommes certainement reconnaissants des bonnes paroles que vous avez tenues à l'égard de notre honorable collègue.

Monsieur Andrey et monsieur Masoodi, je crois savoir que vous allez partager votre temps de parole. Vous disposez d'au plus cinq minutes. Peu importe qui veut commencer, allez-y, je vous prie.

M. Sam Andrey (directeur général, The Dais): Je vous remercie.

Merci de l'invitation à vous faire part de nos points de vue sur cette importante question.

Bonsoir. Je suis Sam Andrey, directeur général de l'organisation The Dais, un groupe de réflexion politique de la Toronto Metropolitan University. Nous travaillons à former les gens et à façonner les idées dont nous avons besoin pour faire progresser une économie, une démocratie et un système d'éducation inclusifs et novateurs pour le Canada.

Je suis accompagné de mon collègue, Joe Masoodi. Avec notre ancien collègue, Yuan Stevens, nous avons publié il y a trois ans un rapport intitulé « Home Ice Advantage », qui se penchait sur le sujet dont le Comité est saisi aujourd'hui, à savoir la sécurité transfrontalière des données des plateformes de médias sociaux. Bien que beaucoup ait changé au cours des trois dernières années, le problème fondamental de la protection inadéquate des Canadiens persiste.

M. Joe Masoodi (analyste principal des politiques, The Dais): Les plateformes de médias sociaux recueillent, transfèrent et stockent une grande variété de renseignements personnels et sensibles, y compris des renseignements d'identification personnelle, des messages privés, l'emplacement, des données financières et des données biométriques. Ces plateformes ont été conçues sciemment pour maintenir les personnes en ligne et les inciter à s'engager afin de recueillir le plus de données possible à leur sujet. Grâce au regroupement de ces données, il est possible de créer des profils détaillés et de faire des déductions sur les personnes, notamment sur leurs opinions politiques, leur orientation sexuelle, leur religion, leurs revenus, leur santé ou des détails sur leur famille. C'est le cas de TikTok, mais aussi de la plupart des grandes plateformes en ligne.

Malgré les risques importants que représente pour les Canadiens l'utilisation potentiellement abusive de ces données, il n'existe actuellement aucune protection adéquate sur la manière dont les données personnelles des Canadiens sont transférées et stockées, en particulier à l'étranger. Cette situation menace la souveraineté canadienne ainsi que la sécurité numérique et la vie privée des Canadiens. Les agences de sécurité nationale et d'application de la loi peuvent avoir accès aux données personnelles dans des pays qui ne disposent pas de protections juridiques suffisantes, comme la Chine. Je pense qu'il convient également d'ajouter que les entreprises technologiques peuvent faire l'objet de rachats, de fusions et de faillites qui peuvent modifier l'endroit et la manière dont les données personnelles sont stockées ainsi que la protection de la vie privée dont elles bénéficient. Enfin, les acteurs malveillants peuvent toujours tirer parti de données dont les garanties sont insuffisantes.

• (1655)

M. Sam Andrey: Dans notre enquête annuelle sur les préjudices en ligne, nous avons constaté que les Canadiens font très peu confiance aux plateformes de médias sociaux, tant pour assurer la sécurité de leurs données que pour agir dans l'intérêt du public, se classant bien en dessous d'autres entreprises technologiques et d'autres organisations de divers types. En fait, la confiance dans TikTok, plus particulièrement, a chuté considérablement l'année dernière, pour se classer au dernier rang. Seulement 7 % des Canadiens disent qu'ils ont très confiance dans la plateforme, malgré sa croissance rapide avec près de 30 % des Canadiens qui l'utilisent.

TikTok a fait l'objet d'un examen particulier, compte tenu de sa structure d'entreprises. Comme on l'a souligné plus tôt au Comité, avant 2019, la politique de confidentialité de TikTok était transparente en déclarant qu'elle communiquait les renseignements des gens « avec tout membre ou associé de [son] groupe » en Chine. Cette ligne a ensuite été mise à jour pour supprimer cette référence à un lieu précis, mais la disposition relative à la divulgation demeure. Cette même disposition figure aussi dans la politique de protection de la vie privée de l'application WeChat, qui est utilisée par 6 % des Canadiens. Comme l'a souligné notre collègue, M. Malone, c'est également le cas pour beaucoup d'autres.

La loi actuelle sur la protection des renseignements personnels du Canada n'interdit pas aux entreprises de transférer des données personnelles à des tierces parties ou à l'extérieur du Canada de cette manière. Nous estimons que les parlementaires ont la possibilité de répondre à ces risques par l'entremise du projet de loi C-27 proposé. Toutefois, dans sa forme actuelle, le projet de loi C-27 permettrait, d'une certaine manière, un échange encore plus facile des données entre les entreprises en érodant les dispositions limitées qui existent en matière de consentement. L'article 18 proposé de la Loi sur la protection de la vie privée des consommateurs crée de nouvelles exceptions importantes qui permettent aux entreprises de divulguer des données à l'insu de la personne ou sans son consentement, en incluant des expressions telles que « activités commerciales » et « intérêt légitime ».

Nous ne pensons pas qu'il incombe exclusivement aux Canadiens de s'éduquer et de se protéger en ligne. Nous proposons que des exigences plus précises soient ajoutées au projet de loi afin de garantir des niveaux de protection équivalents pour les données lorsqu'elles sont transférées à l'extérieur du Canada. Nous suggérons également des exigences qui sont comparables au RGPD de l'Union européenne, afin d'obtenir le consentement explicite et éclairé des Canadiens pour le transfert de leurs données personnelles vers des

pays qui n'offrent pas des niveaux de protection équivalents, en fournissant des renseignements à la fois sur les pays précis concernés et sur les données précises. Bien que de nombreuses personnes aient fait remarquer à ce comité qu'il y a une lassitude à l'égard du consentement, nous pensons à tout le moins qu'il est important de faire preuve de transparence en ce qui concerne les données qui sont transférées vers des pays étrangers.

Nous allons conclure en disant que les Canadiens appuient sans réserve un tel changement. Une enquête représentative que nous avons menée a révélé que 86 % des Canadiens sont favorables à l'obligation de conserver les données des Canadiens au pays, contre seulement 3 % qui n'y sont pas favorables.

Merci du temps que vous nous avez consacré. Nous serons heureux de répondre à vos questions.

Le président: Merci, messieurs Andrey et Masoodi.

[Français]

Monsieur Gourde, vous disposez de six minutes.

Nous devons ensuite faire une pause pour nous permettre d'aller voter.

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

Ma question s'adressera à l'ensemble des témoins.

Les Canadiens s'attendent à ce que leur gouvernement les protège des plateformes numériques. Plusieurs témoins ont dit au Comité que nous étions en retard par rapport aux pays d'Europe, par exemple, en ce qui concerne la législation en la matière.

Pensez-vous que le retard que notre législation accuse par rapport à celle d'autres pays est tel que nous devons agir relativement rapidement, du moins pour la mettre à jour?

[Traduction]

M. Matt Malone: Je me ferai un plaisir d'intervenir.

Je crois que l'un des problèmes auxquels le Canada est confronté est que nous ne sommes pas une grande puissance et que nous sommes coincés entre des approches diamétralement opposées en matière de protection des renseignements personnels et des données parmi les grandes puissances. Si nous n'agissons pas rapidement, nous nous enfermerons dans l'une de ces approches. Les Européens ont adopté une approche plus restrictive. Depuis l'élaboration, l'adoption et la mise en œuvre du RGPD, nous avons assisté à une série de mesures restrictives, qui mènent à des choses comme la localisation des données, des exigences plus strictes concernant les transferts de données et un test d'équivalence solide.

Les États-Unis adoptent une approche diamétralement opposée avec leur cadre de réglementation, dans lequel ils n'ont pas mis à jour leur loi en matière de protection de la vie privée, et il n'y a pas de loi uniforme sur la protection des renseignements personnels aux États-Unis. Parallèlement, les États-Unis exportent, par l'entremise de traités commerciaux et d'organismes de gouvernance dans le monde entier, une vision de la gouvernance des données et de la protection de la vie privée qui encadre ce que le Canada peut faire.

Les discussions sur les transferts de données doivent tenir compte du fait que l'accord Canada-États-Unis-Mexique interdit de restreindre les flux de données transfrontaliers et qu'il comporte d'autres restrictions pertinentes. Le PTPGP prévoit des restrictions semblables.

L'un des problèmes de l'inaction du Canada est que nous ne montrons aucune urgence d'agir. La Loi sur la protection des renseignements personnels, qui régit la conduite des gouvernements, n'a pas été mise à jour depuis plus de 40 ans. La LPRPDE a besoin d'une mise à jour importante, et non pas de simples ajustements. Personnellement, je ne crois pas que le projet de loi C-27 soit le moyen approprié pour y parvenir.

Je vais laisser les autres témoins intervenir.

● (1700)

M. Sam Andrey: Je voudrais ajouter que je souscris à la prémisses de votre question, à savoir que nous prenons du retard à certains égards, même si je pense que nous avons, comme l'a dit Mme Laidlaw, l'avantage d'être en second pour tirer certaines leçons et certaines lois ou approches bancales qui ont été adoptées dans des pays alliés.

En ce qui concerne la réglementation en matière d'intelligence artificielle plus particulièrement, je pense que le Canada avance rapidement par rapport au reste du monde, ce qui est une bonne chose, mais, oui, je dirais que nous devons agir plus rapidement, et le projet de loi C-27 fait partie de cette action.

[Français]

M. Jacques Gourde: Monsieur Malone, vous avez parlé de la capacité d'enquête insuffisante de la GRC. Nous avons reçu des représentants de la GRC, et ils semblaient dire qu'ils avaient la capacité de faire des enquêtes. Cependant, bien sûr, ils n'ont pas précisé s'ils avaient la capacité d'en faire plusieurs à la fois.

Vos inquiétudes sont-elles grandes pour ce qui est de la capacité d'enquête insuffisante de la GRC?

[Traduction]

M. Matt Malone: Quand on examine les ressources qui sont disponibles, elles ne répondent pas à la demande. En 2018, quand Sécurité publique a procédé à une mise à jour de la cybersécurité et a injecté beaucoup d'argent dans la GRC pour qu'elle s'attaque plus sérieusement à la cybercriminalité, c'est à ce moment-là qu'a été annoncée la création du GNC3, le centre national de coordination contre la cybercriminalité.

J'ai écrit à ce sujet il y a trois ans et j'ai dit que nous attendions déjà depuis longtemps ce déploiement, mais trois ans plus tard, ce système de signalement a deux ans de retard. Si vous visitez le site Web en ce moment, vous y apprendrez qu'il est encore à l'étape des essais bêta et qu'il n'accepte que 25 plaintes concernant la cybercriminalité par jour pour l'ensemble du pays, ce qui est vraiment très peu. Dans une série de demandes d'accès à l'information concernant le nombre de ressources consacrées pour le personnel, j'ai découvert que plusieurs provinces n'ont pas d'enquêteurs en cybercriminalité, ce qui est une statistique vraiment choquante. Ici, en Colombie-Britannique, la troisième plus grande province du pays, nous n'avons que quatre personnes à temps plein dans l'équipe de lutte contre la cybercriminalité.

Je crois que ces outils seront déployés plus rapidement. Il devrait y avoir une plus grande transparence en ce qui les concerne, et la

loi devrait être rédigée en fonction de ce que nous constatons, car ces outils nous permettent de comprendre quels types de préjudices sont perpétrés. Il y a toutes sortes d'analyses que vous pouvez mener à partir des données reçues, et le GNC3 révèle que plus de la moitié des signalements qui lui sont transmis concernent des rançongiciels. Il est très intéressant de constater que la loi canadienne ignore les rançongiciels, qui représentent la plus grande menace cybercriminelle à laquelle nous sommes confrontés.

Lorsque nous discutons du projet de loi C-27, il est intéressant de prendre en considération également le projet de loi C-26, qui réglemente les rançongiciels pour les industries essentielles.

[Français]

M. Jacques Gourde: Monsieur Malone, mon temps de parole est presque terminé.

À votre avis, les sommes versées par le gouvernement à la GRC pour assurer la sécurité des données échangées sur les plateformes sont-elles suffisantes ou insuffisantes compte tenu des résultats obtenus?

[Traduction]

Le président: Veuillez répondre très rapidement.

M. Matt Malone: Je crois que l'on ne donne pas suffisamment d'argent à la GRC dans ce domaine, bien franchement.

[Français]

Le président: Merci.

Merci, monsieur Gourde.

[Traduction]

Nous allons maintenant entendre Mme Khalid, qui dispose de six minutes.

Mme Iqra Khalid: Merci beaucoup, monsieur le président.

Je remercie les témoins de comparaître devant nous aujourd'hui et de faire la lumière sur cet enjeu très important.

Monsieur Malone, j'aimerais commencer avec vous. Nous avons reçu des représentants de TikTok, qui nous ont appris que la majorité des données canadiennes n'étaient pas stockées au Canada. Elles sont stockées ailleurs dans le monde, notamment en Malaisie, à Singapour, etc. Quelles sont les répercussions juridiques de cette réalité sur les droits des Canadiens en matière de vie privée?

● (1705)

M. Matt Malone: Je vous remercie pour votre question.

Je pense qu'il est vraiment important d'identifier les représentants de TikTok qui se sont exprimés en tant que lobbyistes. Ils sont enregistrés à ce titre et font du travail de lobbyisme. Je pense qu'il est important de souligner que bon nombre de leurs affirmations étaient trompeuses. Il est possible de contourner facilement bon nombre des contrôles de sécurité pour les enfants dont ils ont vanté les mérites.

Pour répondre de façon plus directe à votre question, TikTok s'est fait prendre à utiliser toutes sortes de méthodes inquiétantes en ce qui concerne les données des utilisateurs. On a rapporté publiquement que TikTok accédait à l'emplacement physique de journalistes qui utilisent l'application, afin de retrouver leurs sources. C'est du domaine public. On a aussi rapporté que TikTok transférait les données des utilisateurs des États-Unis vers la Chine, alors que la société garantissait qu'elle ne le faisait pas, et il y a une foule d'autres rapports en ce sens.

Certains rapports internes du gouvernement canadien émanant notamment du Secrétariat de l'évaluation du renseignement du Bureau du Conseil privé cernent toutes sortes d'autres problèmes liés au type de données et à la collecte persistante de données qui se fait au moyen de l'application. J'ai également vu des documents provenant de l'unité du renseignement sur les cybermenaces du Commandement du renseignement des Forces canadiennes, au ministère de la Défense nationale, qui ciblent une série de problèmes préoccupants liés à la censure et à d'autres enjeux.

Ce qui rend la situation difficile ici, c'est que la loi canadienne est très permissive en ce qui concerne le transfert de données. En effet, même dans le projet de loi C-27, qui porte sur la protection des renseignements personnels, il n'y a rien qui empêcherait les transferts de données à l'extérieur du Canada. Dans son avis de confidentialité, TikTok indique qu'en utilisant l'application, vous acceptez les conditions voulant que la filiale puisse partager ces données avec sa société mère, ByteDance, et la loi canadienne lui permet de le faire. Même la mesure législative proposée le permettrait. L'article 19 et le paragraphe 11(1) du projet de loi C-27 permettent précisément ce type de transfert de données.

La loi canadienne sur le transfert des données repose essentiellement sur l'idée que les organisations peuvent transmettre des données à d'autres administrations si elles jugent que les protections sont suffisantes ou adéquates, comme ce serait le cas au Canada. Cette approche est très différente de l'approche européenne, qui se fonde sur la compétence... D'un pays à l'autre. On ne peut pas transférer de données vers un autre pays à moins d'être convaincu que les protections y sont équivalentes. Il y a une très grande différence entre la loi canadienne et la loi européenne dans ce domaine. Une fois que les données sortent du Canada, on ne sait pas vraiment ce qu'il en advient. Les autres ne prennent pas les mêmes mesures de protection que vous.

Pour la réunion d'aujourd'hui, j'ai demandé au dirigeant principal de l'information de la Chambre des communes où les données de l'application Zoom, que j'utilise, étaient localisées et traitées. On m'a répondu — et j'en suis très heureux et impressionné — que les données étaient traitées au Canada. Vos séances à huis clos sont encore mieux sécurisées; c'est tant mieux pour vous. Ce n'est pas le cas pour les utilisateurs de TikTok.

Mme Iqra Khalid: Merci.

Lors d'entrevues précédentes, vous avez parlé du déséquilibre du pouvoir associé à la collecte de grandes quantités de données des utilisateurs. Que vouliez-vous dire par là? Pouvez-vous nous l'expliquer?

M. Matt Malone: Comme de nombreuses personnes qui ont comparu devant le Comité et d'autres comités qui traitent de sujets connexes, je me préoccupe grandement de la façon dont le déséquilibre du pouvoir affecte la capacité des utilisateurs à donner un consentement valable et éclairé. Lorsque vous cliquez sur « Accepter » sur un avis de confidentialité très long, vous le faites en tant

qu'utilisateur individuel, alors que la société qui recueille vos données peut avoir une valeur sur le marché qui dépasse la taille d'un pays du G7. Le déséquilibre des pouvoirs est très grand.

Mme Iqra Khalid: Merci beaucoup.

Monsieur Andrey et monsieur Masoodi, vous avez rédigé un rapport — ou vous y avez contribué — sur les préjudices en ligne associés aux plateformes de médias sociaux du domaine public au Canada. Pouvez-vous nous parler des principales constatations émanant de ce rapport et nous parler de la façon dont les communautés et groupes vulnérables et marginalisés sont ciblés en particulier?

M. Sam Andrey: Bien sûr, avec plaisir.

Mon collègue pourra intervenir à tout moment s'il le souhaite.

Nous effectuons un sondage annuel auprès d'un groupe représentatif de Canadiens pour faire le suivi des expériences en ligne des Canadiens avec du contenu préjudiciable illégal. Nous commençons par les discours haineux: 40 % des Canadiens disent qu'ils voient des discours haineux au moins une fois par mois, et environ 10 % des Canadiens disent qu'ils ont été personnellement ciblés par des discours haineux en ligne. C'est environ le double ou le triple de ce taux pour diverses communautés marginalisées et racisées. Ce serait environ le double pour les Canadiens 2SLGBTQ, et 30 %, disent qu'ils ont été la cible de discours haineux. Nous effectuons un suivi à cet égard.

Nous suivons également l'exposition à la désinformation et à la désinformation et les croyances à cet égard. Nous réalisons un questionnaire, qui présente une série de déclarations vraies et fausses. Environ 15 % des Canadiens qui y participent montrent une croyance importante à l'égard de la désinformation. Ces Canadiens sont plus susceptibles de dire qu'ils consomment leurs nouvelles sur les médias sociaux et qu'ils font moins confiance aux médias grand public.

• (1710)

Le président: Monsieur Andrey, je vais devoir vous arrêter là. Je suis désolé.

[Français]

Nous allons suspendre la séance pour aller voter. Au retour, M. Villemure aura la parole pour six minutes.

[Traduction]

Nous devrions revenir dans une quinzaine de minutes; je vous remercie pour votre patience.

Merci.

La séance est suspendue.

• (1710)

(Pause)

• (1730)

Le président: Nous reprenons les travaux.

[Français]

Nous allons commencer notre tour de questions.

Monsieur Villemure, vous avez six minutes. Vous pouvez commencer votre intervention.

M. René Villemure: Je remercie les invités de leur présence.

Monsieur Malone, c'est un plaisir de vous revoir ici.

Le consentement éclairé, selon vous, est-ce impossible? Est-ce inutile? Est-ce un mirage, aujourd'hui?

M. Matt Malone: Je pense que le mot « mirage » décrit bien l'état actuel des choses.

[Traduction]

Je pense que le consentement éclairé, sur lequel reposent actuellement toutes les lois canadiennes sur la protection de la vie privée, ne sert pas les fins pour lesquelles nous avons vraiment besoin de lois sur la protection des données et la protection de la vie privée au pays. Le projet de loi C-27 a perpétué l'idée que cet instrument continuera de fonctionner et de servir ses fins même avec les exceptions commerciales légitimes, même avec les règles concernant le consentement implicite, et cela ne nous permettra pas d'avoir une loi robuste sur la protection de la vie privée et des données au pays.

Je pense qu'il faut changer fondamentalement le paradigme pour que la possession, la conservation, l'utilisation et la divulgation de renseignements personnels deviennent une responsabilité, par opposition à une façon rentable de gérer une entreprise. C'est ce que nous avons permis à ces entreprises de publicité et de médias sociaux de faire.

[Français]

M. René Villemure: C'est une très bonne façon de le voir. Je me disais que le consentement « libre et éclairé », comme on le dit en termes médicaux, ne pourra jamais être libre si vous voulez accéder à la chose. Le consentement éclairé, on sait que c'est un peu une fiction, voire un mirage.

Vous avez également mentionné que le Canada est une puissance moyenne dans ce domaine. C'est vrai, notamment par rapport à l'Union européenne, aux États-Unis et à la Chine.

Dans quelle mesure peut-on espérer qu'une législation canadienne s'impose et occupe une place valable?

[Traduction]

M. Matt Malone: Je crois que le Canada a l'occasion de reprendre son rôle traditionnel de puissance moyenne auprès des États alliés.

On a exprimé plusieurs idées relatives à la création de zones sécuritaires pour le flux des données, qui misent sur les alliances existantes en matière de sécurité, comme l'OTAN. Nous avons déjà pris un engagement de défense mutuelle avec nos alliés de l'OTAN. Il serait logique d'échanger nos données et nos renseignements personnels avec ces alliés dans une zone permettant le libre mouvement transfrontalier des données. Le Canada pourrait assurer un rôle unique en matière de réglementation, et créer des cadres réglementaires pour le mouvement transfrontalier des données.

Ce qui me préoccupe le plus, c'est l'état de la loi actuelle. De nombreuses lois canadiennes — et c'est une priorité pour les législateurs à l'heure actuelle — visent la protection des renseignements personnels dans le secteur privé uniquement. Comme nous l'avons notamment vu pendant la pandémie, il nous faut des lois robustes en matière de protection de la vie privée et des données qui s'appliquent également au gouvernement. Je suis vraiment contrarié de voir que la Loi sur l'intelligence artificielle et les données ne s'applique pas aux mesures gouvernementales, ce qui est vraiment préoccupant lorsqu'on pense au déploiement des technologies misant sur l'intelligence artificielle comme l'application ArriveCAN.

Je suis également très préoccupé par le fait que les priorités du projet de loi C-27 ne sont pas axées sur le gouvernement. Il est troublant de constater que ces efforts sont menés par le portefeuille de l'Industrie et que le projet de loi C-27 créerait de nouveaux instruments de réglementation qui relèveraient du ministre de l'Industrie. Il est difficile d'affirmer que nous abordons la protection de la vie privée du point de vue des droits de la personne, de l'application de la loi ou de la sécurité nationale lorsque les organismes que nous créons ne sont pas vraiment indépendants. Non seulement ils ne sont pas vraiment indépendants, mais ils sont aussi subordonnés au portefeuille de l'industrie dont le mandat est de faire croître l'économie.

[Français]

M. René Villemure: Je partage vos craintes, à ce sujet, croyez-moi.

Monsieur Andrey, je vous pose la même question.

Le Canada est une puissance moyenne, entre l'Union européenne, l'Amérique ou la Chine.

Quelle proposition de notre part serait acceptable?

• (1735)

[Traduction]

M. Sam Andrey: J'abonde dans le même sens que mon collègue à bien des égards. Je crois que nous pouvons miser sur... Je pourrais vous parler de la loi sur les préjudices en ligne de façon particulière. L'Allemagne a été une pionnière dans ce domaine et a créé un régime de retrait dans les 24 heures. Pour s'y conformer, les grandes plateformes ont versé dans la censure excessive. Elles ne voulaient pas être tenues responsables, alors elles ont retiré beaucoup trop de contenu légal.

Nous avons l'occasion d'apprendre de ces erreurs.

[Français]

M. René Villemure: Puisque le temps file, je me permets de vous interrompre pour vous demander de nous envoyer quelques informations sur ce qui s'est passé en Allemagne, s'il vous plaît. Ce serait très bien.

J'aimerais vous poser une dernière question avant que le temps ne soit écoulé.

Voyez-vous un organisme de réglementation qui serait indépendant, comme le Commissariat aux conflits d'intérêts et à l'éthique, le Commissariat à la protection de la vie privée du Canada ou le Commissariat au lobbying du Canada? Ferait-il plutôt partie d'un certain ministère, comme le ministère de l'Innovation, des Sciences et de l'Industrie, dans le cas qui est proposé? Où voyez-vous cet organisme de réglementation? Quels seraient ses pouvoirs?

[Traduction]

M. Sam Andrey: À mon avis, un responsable de la réglementation du contenu numérique a un rôle à jouer en ce sens.

À l'heure actuelle, le projet de loi C-27 prévoit la création du poste de responsable de la réglementation des données de l'intelligence artificielle, mais il relèverait d'Innovation, Sciences et Développement économique Canada. À mon avis, c'est inacceptable, surtout parce que le ministre aura les rôles concurrents de promouvoir les avantages économiques de l'intelligence artificielle et de réglementer ses risques. Le titulaire de ce poste devrait à tout le moins être nommé par le gouverneur en conseil. Idéalement, il s'agirait d'une nomination parlementaire distincte.

Je pense que vous pourriez confier au titulaire de ce poste la responsabilité du portefeuille des méfaits en ligne. Il pourrait y avoir deux postes distincts, mais cela ferait beaucoup. Le titulaire de ce poste aurait le pouvoir de faire des vérifications et s'acquitterait de fonctions semblables à celles d'un ombudsman pour aider les particuliers. Il assurerait également une fonction en matière de transparence.

[Français]

M. René Villemure: Ce serait donc un organisme de réglementation indépendant.

Le président: D'accord.

Merci, monsieur Villemure.

[Traduction]

Merci, monsieur Andrey.

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

M. Matthew Green: Merci beaucoup.

Je sais qu'il y a eu des éloges au début la série de témoignages. C'est dans cet esprit que je tiens à féliciter Christelle Tessono. Je crois savoir qu'elle travaille maintenant dans le domaine des politiques et de la recherche pour The Dais. Je sais que son travail a été souligné dans le cadre d'autres réunions des comités, ainsi que dans certaines études approfondies dans ce domaine. La technologie est souvent bien en avance sur la portée de notre expertise en la matière, et il est donc extrêmement important de pouvoir miser sur des experts comme vous. Je vous remercie d'être ici aujourd'hui. Je vous remercie également pour toutes vos contributions.

J'aimerais commencer avec M. Malone.

Dans un article paru en septembre 2023, vous avez dit avoir examiné un document du gouvernement fédéral intitulé *Economic Security and Technology: TikTok Takeover*. Êtes-vous en mesure de nous parler des préoccupations soulevées dans ce rapport? Partagez-vous ces préoccupations?

M. Matt Malone: Je ne sais pas exactement à quel document vous faites référence.

Est-ce que vous parlez du document sur lequel se fonde ma recommandation visant à interdire toutes les applications de médias sociaux sur les appareils du gouvernement?

M. Matthew Green: Oui.

Si vous avez suivi l'étude, vous aurez remarqué que j'insiste beaucoup pour que nous élargissions la portée de la réglementation, de la surveillance et du contrôle de toutes les plateformes, et non seulement de TikTok.

Je crois que vos commentaires sur ce sujet pourraient nous être utiles.

M. Matt Malone: Ce document provient de l'unité du renseignement sur les cybermenaces de la Défense nationale. Il cerne une série de préoccupations liées à TikTok qui comprennent des opérations de surveillance et de renseignement, des violations de la vie privée, la collecte de données, l'ingérence politique, le contrôle du discours et la censure des exportations par le Parti communiste chinois. On évoque également plusieurs préoccupations relatives à de nombreuses autres entreprises de médias sociaux, comme Snapchat et LinkedIn.

Je serais très heureux de transmettre ce document au Comité, si vous le souhaitez.

M. Matthew Green: Oui, cela nous serait très utile.

À votre avis, est-ce que le risque associé aux applications de médias sociaux sur les téléphones du gouvernement fédéral diffère de celui associé à l'utilisation de ces applications par les employés sur leur téléphone personnel?

M. Matt Malone: En ce qui concerne le type de renseignements communiqués sur les appareils fournis par le gouvernement, il ne fait aucun doute que la sensibilité est plus importante, surtout lorsque ces renseignements... Même si l'utilisation individuelle est inoffensive, elle pourrait servir de façon regroupée. Il faut penser à certains éléments comme les données de localisation, qui peuvent révéler des renseignements comme l'emplacement des politiciens ou des membres des Forces armées canadiennes. Il y a quelques années, on a rapporté qu'une fuite des données de localisation provenant d'une application de type Fitbit avait permis de localiser une base militaire américaine dans la province de Helmand. Ces données sont, de toute évidence, très délicates lorsqu'elles sont regroupées.

Si vous me le permettez, j'irais plus loin et je dirais qu'il devrait y avoir une interdiction des applications de médias sociaux sur les appareils fournis par le gouvernement, à moins qu'il y ait une solide justification relative à leur utilisation.

Cependant, cela donne une très bonne indication de ce que sont les priorités du gouvernement. J'ai parlé plus tôt du manque de fonds pour l'équipe d'enquête sur la cybercriminalité de la GRC. Toutefois, le nombre de personnes qui travaillent pour les médias sociaux ou les communications du gouvernement est exponentiellement plus important que le nombre de ressources que nous consacrons à la lutte contre les préjudices en ligne, que subissent certains des Canadiens les plus vulnérables.

● (1740)

M. Matthew Green: Je crois que vous avez même dit qu'à votre avis, nous devrions cesser de faire de la publicité sur ces plateformes. C'est à cette conclusion que vous en venez lorsque vous tenez compte des risques et des avantages sur le plan du rayonnement et de la communication des renseignements. Est-ce que vous faites référence à toutes les plateformes?

M. Matt Malone: Oui. Je crois qu'il est contraire à l'éthique de faire de la publicité auprès des entreprises de médias sociaux si nous avons de réelles préoccupations au sujet de la collecte de données et de l'ingérence étrangère illicite.

L'année dernière, le gouvernement a dépensé un montant record de 141 millions de dollars en publicité, soit plus du double de ce qu'il a dépensé pour l'administration de la Loi sur l'accès à l'information, et cela comprenait près de 2 millions de dollars de publicité sur TikTok.

Il est vraiment difficile d'assister aux audiences des comités et d'entendre toutes ces préoccupations au sujet des pratiques de TikTok, pour ensuite voir le gouvernement donner de l'argent à la société, ce qui, à mon avis, représente un appui implicite à l'égard de ces pratiques que nous cherchons à critiquer. Pour que ce soit bien clair, je crois que cette préoccupation s'applique à toutes les entreprises de médias sociaux.

J'ai été très heureux d'apprendre que le gouvernement avait cessé de faire de la publicité sur Meta cet été, mais c'était en guise de représailles à la suite des réactions de Meta à la Loi sur les nouvelles en ligne. C'était donc une mesure un peu différente, mais même en guise de représailles, je l'appuie.

M. Matthew Green: C'est exact.

Je dois revenir à M. Andrey et à M. Masoodi.

Est-ce que votre organisation a fait un travail de recherche sur l'échange de données entre les plateformes de médias sociaux comme TikTok et les entités étrangères, où les acteurs étatiques, le secteur privé ou les tiers réutilisent les données à des fins de profilage de marketing ou de méfait?

M. Sam Andrey: Je vous remercie pour la question, et je salue Mme Tessono, qui est aussi une membre précieuse de notre équipe. J'espère qu'elle sera un jour invitée à comparaître devant le Comité ou devant le comité de l'industrie pour parler de l'intelligence artificielle.

Pour répondre à votre question, oui. M. Masoodi, un autre collègue et moi avons rédigé un article sur les pratiques de stockage de données dans le cadre des transferts transfrontaliers de données des plateformes de médias sociaux. L'article s'intitule *Home Ice Advantage*, et nous vous sommes reconnaissants de l'avoir mentionné dans le cadre de l'une de vos réunions précédentes.

Monsieur Masoodi, je ne sais pas si vous voulez intervenir.

Dans le cadre d'une question précédente, on a fait valoir que TikTok stockait ses données à Singapour et aux États-Unis. Oui, c'est vrai, mais c'est un portrait incomplet de la situation. Il est possible d'accéder à ces serveurs à distance, à partir de n'importe quel pays du monde.

M. Matthew Green: Comme je n'ai plus de temps, est-ce que vous pourriez nous faire parvenir les points saillants de l'article? On y a fait référence, mais tous les renseignements et les préoccupations dont vous faites part au Comité peuvent être utilisés à titre de témoignages.

Merci.

Le président: Merci, monsieur Green et monsieur Andrey.

Je demanderais aux témoins de nous fournir les renseignements qui ont été demandés d'ici vendredi, si possible. Cela aiderait nos analystes. Nous devons imposer un délai; ce sera donc vendredi, à 17 heures, si vous n'y voyez pas d'inconvénient.

Nous allons entendre M. Barrett, puis M. Kelloway, M. Bains, M. Villemure et enfin M. Green. Vous disposez chacun de deux minutes et demie.

Monsieur Barrett, vous avez la parole.

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

Nous ne disposons que de quelques minutes.

J'aimerais que chacun des témoins réponde à ma question, si possible. Croyez-vous qu'il soit utile d'obliger les magasins d'applications comme Google Play et App Store à exiger le consentement des parents pour le téléchargement des applications de médias sociaux pour les enfants? Ma question à l'intention des témoins précédents visait les enfants de moins de 16 ans.

M. Sam Andrey: Je peux commencer.

Je ne crois pas qu'une telle obligation puisse nuire, mais je crois que la logistique associée à la vérification de l'âge est complexe. Je n'ai probablement pas le temps d'entrer dans les détails de tout cela pour le moment, mais en principe, je répondrais oui.

Je proposerais même d'aller plus loin, puisque nous parlons du stockage transfrontalier des données: on pourrait interdire le transfert des données d'utilisation des mineurs vers des pays où les mesures de protection ne sont pas suffisantes, également.

Oui, je crois qu'il serait utile d'ajouter de telles obligations.

• (1745)

M. Michael Barrett: Merci.

Allez-y, monsieur Malone.

M. Matt Malone: Je ne crois pas que ce soit une bonne idée.

Je comprends l'objectif de la proposition. Je pense qu'elle repose sur de bonnes intentions, et j'y ai réfléchi sérieusement, mais je pense qu'elle entraînerait des effets négatifs qui ne correspondraient peut-être pas à son intention.

La réalité, c'est que nous avons besoin d'une loi sur la protection des renseignements personnels qui protège les enfants par défaut. Cette responsabilité ne devrait pas revenir aux parents. Ces technologies présentent des avantages et des inconvénients, et je ne crois pas que les parents ou les générations plus âgées soient toujours les meilleurs pour s'y retrouver. J'ai vu de nombreux sondages du Bureau du Conseil privé qui montrent que ce sont les jeunes qui utilisent ces technologies — 30 % des adolescents consomment les nouvelles sur TikTok —, tandis que bon nombre des générations plus âgées ne les utilisent pas du tout. Je ne me sentirais pas à l'aise de confier cette responsabilité à tous les parents, mais ce n'est que mon opinion.

Ce que je dirais, cependant, c'est que les enfants devraient être explicitement considérés à titre de population vulnérable dans le projet de loi C-27. Je pense qu'il est inacceptable que les enfants et les jeunes, en particulier, aient été retirés du projet de loi C-27 et en soient exclus. C'était l'intention délibérée du ministère de l'Industrie. J'ai un mémoire interne qui explique les raisons derrière cette décision, et je serais heureux de vous le faire parvenir.

Le président: Merci, monsieur Malone.

Je suis désolé, mais nous n'avons plus de temps. Si vous pouviez nous le faire parvenir d'ici vendredi, à 17 heures, nous vous en serions reconnaissants.

Monsieur Bains, vous avez deux minutes et demie. Allez-y.

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

Je remercie nos témoins de se joindre à nous aujourd'hui.

Il est clair qu'il y a un risque ou un danger générationnel de préjudices en ligne. Deux tragédies nous ont frappés de près en Colombie-Britannique. Vous vous souvenez peut-être du suicide d'Amanda Todd, en 2012, à cause du cyberharcèlement dont elle faisait l'objet, et du suicide récent d'un garçon de 12 ans victime d'extorsion sexuelle en ligne, qui a fait les manchettes.

Il se trouve que j'ai moi-même une fille de 15 ans et un garçon de 12 ans, alors c'est terrifiant d'entendre ce genre d'histoires.

Je vais m'adresser d'abord à M. Malone.

Vous avez souligné, dans une entrevue, que la collecte de vastes quantités de données crée un « déséquilibre des pouvoirs » avec les utilisateurs. Pourriez-vous nous expliquer ce que vous entendez par là?

M. Matt Malone: J'ai déjà fourni une réponse à cet égard à la députée de Mississauga, Erin Mills, mais je serai heureux d'extrapoler un peu à ce sujet, surtout dans le contexte de l'influence et du contrôle chinois.

Il y a eu des déclarations selon lesquelles... Je vais prendre l'exemple de TikTok, bien que mes commentaires s'appliquent aussi à d'autres entités. TikTok recueille des données sur les utilisateurs canadiens et les stocke aux États-Unis, à Singapour et en Malaisie. Selon la loi chinoise, particulièrement la Loi nationale sur le renseignement, les entreprises qui exercent des activités en Chine doivent coopérer avec la Chine. On parle ici en particulier de l'article 7 de cette loi. L'article 10 prévoit quant à lui l'application extraterritoriale de la loi. Peu importe que les données se trouvent dans un pays étranger. Toute entreprise qui a une base en Chine, comme c'est le cas ici... Étant donné que l'État chinois en est propriétaire à 1 %, il peut exercer son contrôle sur TikTok et ByteDance.

Cela signifie que ces problèmes ne sont pas près de disparaître.

M. Parm Bains: Vous avez mentionné plus tôt plusieurs autres plateformes, dont Bumble. Qu'en est-il des plateformes de messagerie comme Signal, Telegram ou WhatsApp?

Nous avons vu récemment la police d'Abbotsford émettre un avertissement au sujet d'appels téléphoniques faits de l'extérieur du Canada dans WhatsApp pour extorquer de l'argent à des entreprises locales...

Le président: Monsieur Bains, votre temps est écoulé, mais je veux entendre la réponse.

Je ne sais pas à qui vous vous adressez, mais pourriez-vous répondre rapidement, s'il vous plaît?

M. Parm Bains: Je pose la question à M. Malone à nouveau, s'il vous plaît.

M. Matt Malone: Je crois que les raisons pour lesquelles les gens utilisent Signal pour se soustraire à l'application de la loi sont les mêmes que celles pour lesquelles les ministres et les membres du personnel politique utilisent Signal pour se soustraire à l'application de la Loi sur l'accès à l'information.

Je pense que toutes les entreprises de médias sociaux devraient être interdites sur les appareils fournis par le gouvernement.

• (1750)

Le président: Eh bien, c'était toute une réponse.

Je vous remercie, monsieur Malone.

[Français]

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

M. René Villemure: Monsieur Malone, au fond, aujourd'hui, on tente de combattre le capitalisme de surveillance, qui fait son pain et son beurre des données.

Comment peut-on combattre ce capitalisme de surveillance?

[Traduction]

M. Matt Malone: Je dirais qu'il est important de prêcher par l'exemple. Nous avons besoin de lois sur la protection de la vie privée et des données qui montrent aux Canadiens que vous prenez la chose au sérieux. Cela signifie que la conduite du gouvernement lui-même doit être régie par une loi robuste et adaptée à la réalité actuelle. Cela signifie également que les partis politiques, qui sont souvent très prompts à dénoncer les atteintes à la vie privée perpétrées par les entreprises privées de médias sociaux, doivent également être visés par la législation canadienne de protection des renseignements personnels.

Beaucoup de jeunes, s'ils entendaient ces discussions passionnantes sur la protection de la vie privée et des données au Canada (la collecte de données, l'ingérence illicite et toutes ces choses) exprimeraient probablement des valeurs très différentes, parce que ce sont eux qui utilisent ces services. Une bonne partie des législateurs et des détenteurs du pouvoir exécutif ne les utilisent justement pas.

Je pense qu'il sera vraiment difficile de convaincre les jeunes que ces questions (le capitalisme de surveillance en particulier) sont prises au sérieux, à moins que vous n'appliquiez ces lois à la conduite du gouvernement et des partis politiques.

[Français]

M. René Villemure: Merci beaucoup.

Le président: Avez-vous terminé, monsieur Villemure? Il vous reste encore du temps.

M. René Villemure: Me reste-t-il un peu de temps? Je n'ai pas ma minuterie pour le vérifier.

Le président: D'accord.

[Traduction]

Monsieur Green, vous avez deux minutes et demie. Allez-y, s'il vous plaît.

M. Matthew Green: Merci beaucoup.

Messieurs Andrey et Masoodi, je vais vous donner l'occasion de nous dire, au cours de la prochaine minute...

[Français]

Le président: Monsieur Villemure, est-ce que tout va bien de votre côté? Voulez-vous continuer pendant 30 secondes?

M. René Villemure: J'éprouve des problèmes techniques.

Le président: D'accord.

M. Villemure éprouve des problèmes techniques. Je m'excuse.

[Traduction]

Monsieur Green, je suis désolé. Allez-y. Vous avez deux minutes et demie.

M. Matthew Green: Je veux donner à tous les témoins l'occasion de nous faire part, en 30, 45 secondes ou une minute chacun, de tout ce dont ils voudraient discuter ou qu'ils voudraient souligner qui n'a pas été mentionné en réponse aux questions. Évidemment, vous n'êtes pas contraints par l'objet de nos questions ici.

Je vais commencer par vous, monsieur Andrey ou monsieur Masoodi, si vous voulez prendre une minute pour nous dire sur quoi vous voudriez nous voir conclure aujourd'hui.

M. Joe Masoodi: Je vous remercie de cette question.

Une question a été posée sur le capitalisme de surveillance, un concept introduit par Shoshana Zuboff. Il a été mis de l'avant à quelques reprises au cours des audiences. La question précédente portait sur ce que nous pouvons faire pour au moins essayer d'atténuer les répercussions du capitalisme de surveillance, qui a vraiment été initié, si nous regardons en arrière, par Google. C'est Google, grâce à ses techniques d'apprentissage automatique, qui a favorisé l'apparition du phénomène, et des régimes réglementaires et législatifs déficients lui ont permis de se développer.

Si je devais formuler des recommandations sur les leçons à retenir de tout cela, je dirais que nous avons besoin de lois robustes en matière de protection de la vie privée. Nous l'avons entendu à répétition. Je tiens à le souligner encore une fois. Nous devons mettre en place de solides mesures de protection de la vie privée, surtout en ce qui concerne les transferts de données transfrontaliers. Je pense qu'on pourrait miser sur le projet de loi C-27, dans lequel les transferts de données transfrontaliers sont expressément mentionnés, pour créer des protections robustes.

M. Matthew Green: D'accord. Je vais maintenant donner la parole à M. Malone.

Monsieur Malone, vous avez le mot de la fin. Y a-t-il quoi que ce soit, pour le bien du Comité, qui, selon vous, aurait pu être oublié?

M. Matt Malone: Je crois comprendre que tout le monde s'inquiète beaucoup des moyens détournés que la Chine pourrait utiliser pour mettre la main sur le genre de données recueillies par TikTok et de la possibilité que la Chine fasse peser des menaces sur nous en conséquence.

Je dirais que le Canada doit surtout prêcher par l'exemple à cet égard. Je veux dire par là que nous devons exiger des comptes de notre propre gouvernement pour nous assurer de sa transparence et de sa responsabilité et qu'il protège les droits de la personne et la démocratie en ligne.

Le dirigeant principal du Centre canadien pour la cybersécurité, qui relève du Centre de la sécurité des télécommunications, a comparu devant le Comité dans le cadre de cette étude. Le CST ne peut ni confirmer ni nier qu'il utilise des logiciels espions contre des adversaires étrangers dans le cadre de son travail. Vous n'obtiendrez aucune réponse à savoir si la Chine le fait si les autorités canadiennes ne répondent pas non plus clairement à cette question.

J'ajouterais simplement que j'aimerais vraiment voir tous les renseignements que le CST a fournis au Bureau du Conseil privé ou au Secrétariat du Conseil du Trésor pour qu'il interdise l'utilisation de TikTok, parce qu'il est très étrange que cette application de médias sociaux ait été interdite de façon sélective. Le moment choisi est remarquable, car c'était évidemment 10 jours après la publication d'un rapport explosif.

• (1755)

M. Matthew Green: Selon vous, était-ce le fruit d'une décision politique?

M. Matt Malone: Je n'ai pas d'opinion à ce sujet.

[Français]

Le président: Monsieur Villemure, votre vidéo n'est plus gelée. Voulez-vous 30 secondes pour poser une autre question?

M. René Villemure: Oui, s'il vous plaît.

Monsieur Malone, vous pouvez continuer.

[Traduction]

M. Matt Malone: Je n'ai rien d'autre à dire.

[Français]

Le président: Merci, monsieur Villemure.

[Traduction]

Tout d'abord, je tiens à remercier tous nos témoins — M. Malone, M. Andrey et M. Masoodi — de leur présence ici aujourd'hui.

Si vous avez des documents écrits à transmettre à la greffière et au Comité, veuillez le faire d'ici vendredi, à 17 heures. Vous nous avez fourni des renseignements très utiles aujourd'hui, et je vous en suis très reconnaissant. Je vous remercie également de votre patience pendant les votes, comme je vous remercie d'avoir bien voulu reporter votre comparution devant nous à cette semaine.

Je vais laisser partir les témoins, car j'ai deux ou trois choses à dire au Comité. Ce ne sont que quelques petites nouvelles.

J'ai reçu une demande de réunion d'urgence. Nous la tiendrons mercredi. L'avis devrait être publié sous peu.

Je vous dirai également que nous avons reçu la confirmation de Google et de Meta que ses représentants comparaitront devant le Comité dans le cadre de cette étude le mercredi 13 décembre. Des représentants de ces deux entités comparaitront devant nous la semaine prochaine.

Comme il n'y a pas d'autres points à l'ordre du jour, je vais lever la séance.

Merci à tous de votre participation. Merci à nos analystes, à notre greffière et à nos techniciens.

La séance est levée.

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante :
<https://www.noscommunes.ca>

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: <https://www.ourcommons.ca>