CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

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

ETHI • NUMÉRO 134 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 5 février 2019

Président

M. Bob Zimmer

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

Le mardi 5 février 2019

● (1545)

[*Traduction*]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): Bienvenue, tout le monde, au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Il s'agit de la 134e séance, qui porte sur la protection des données personnelles dans les services gouvernementaux numériques.

Nous recevons aujourd'hui, à titre personnel, David Carroll, professeur agrégé, Parsons School of Design, The New School; Chris Vickery, directeur de la recherche sur les risques cybernétiques, UpGuard; et Jason Kint, chef de la direction, Digital Content Next.

Avant de passer à nos témoins — et, encore une fois, toutes nos excuses pour notre léger retard en raison du vote —, nous sommes saisis d'une motion dont il a été question jeudi et que nous allons aborder maintenant.

Monsieur Kent, la parole est à vous.

L'hon. Peter Kent (Thornhill, PCC): Merci beaucoup, monsieur le président. Je crois que nous pouvons régler ce point assez rapidement.

Depuis notre dernière séance, il y a eu des discussions avec le vice-président libéral, et on m'a informé que le nouveau comité est si récent que ses membres n'ont pas encore eu l'occasion de se réunir.

Je m'abstiendrai de Iaisser entendre que le gouvernement semble avoir annoncé le tout à la hâte, mais j'aimerais modifier ma motion de jeudi pour remplacer les mots « hauts fonctionnaires ». La motion devrait donc se lire comme suit: « Que le Comité invite la ministre à comparaître au nom du nouveau Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections pour discuter de la vision, du défi et des protocoles de fonctionnement. »

Le président: Y a-t-il des observations sur les modifications apportées à la motion?

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Non. Je crois que c'est un amendement raisonnable, et j'estime que la ministre Gould est mieux placée pour répondre aux questions que nous nous posons en ce moment.

L'hon. Peter Kent: Quel esprit de camaraderie.

M. Nathaniel Erskine-Smith: En effet.

M. Raj Saini (Kitchener-Centre, Lib.): Voilà qui est un peu insolent, tout de même.

M. Nathaniel Erskine-Smith: C'est seulement parce que je vous aime bien, Peter.

Le président: Monsieur Cullen.

M. Nathan Cullen (Skeena—Bulkley Valley, NPD): La chose que je me contenterai de dire pour la gouverne du Comité, sans nécessairement vouloir l'ajouter à la motion, c'est que nous nous sommes également entretenus avec Élections Canada au sujet de cette procédure. Je crois que le Comité devrait être disposé à parler aussi avec le directeur général des élections, qui est, bien entendu, un agent du parlement et dont le seul et unique mandat est d'assurer la tenue d'élections libres et justes au Canada, mandat qui relève également de notre comité en ce qui concerne l'aspect lié à l'ingérence étrangère et aux fausses nouvelles. Je ne sais pas; je n'ai pas posé cette question au directeur général des élections, mais je pense bien qu'il aurait de quoi contribuer à ce genre de conversation.

L'hon. Peter Kent: Nous sommes donc saisis d'un amendement à un sous-amendement?

M. Nathan Cullen: Ma proposition ne tenait même lieu d'un amendement

L'hon. Peter Kent: Pourrait-il s'agir d'un éventuel...?

M. Nathan Cullen: Oui. Je recommande simplement aux membres du Comité d'être ouverts à cette idée et de se rappeler que ce haut fonctionnaire en connaît évidemment beaucoup sur les élections et qu'il est chargé de diriger celles qui s'en viennnent.

Le président: On vient de m'informer qu'il vous faudrait obtenir l'accord de M. Gourde pour modifier votre propre motion.

L'hon. Peter Kent: Monsieur Gourde?

Le président: M. Gourde a dit qu'il est disposé à modifier la motion en fonction de ce qui vient d'être dit. C'est bien.

Y a-t-il d'autres observations?

(L'amendement est adopté.)

Le président: Tous ceux qui sont pour la motion?

Mme Mona Fortier (Ottawa—Vanier, Lib.): La motion modifiée.

Le président: La motion modifiée, merci.

(La motion modifiée est adoptée.)

Le président: Merci, tout le monde.

Passons aux exposés.

Monsieur Carroll, voulez-vous commencer? Vous avez 10 minutes.

M. David Carroll (professeur associé, Parsons School of Design, The New School, à titre personnel): Je tiens à remercier le président, le vice-président et les membres du Comité de me donner l'occasion de témoigner aujourd'hui. J'ai suivi d'assez près les travaux du Comité en ce qui concerne Cambridge Analytica, surtout en rapport avec les enquêtes menées au Royaume-Uni et aux États-Unis. J'ai été impressionné par les efforts inébranlables déployés par le Comité pour établir les faits et dire la vérité en interrogeant les représentants de la société au coeur de l'enquête sur les élections transnationales et les crimes liés aux données survenus en 2016: AggregateIQ, un fournisseur exclusif de SCL Elections Limited, qui est le contrôleur enregistré des données de Cambridge Analytica au Royaume-Uni.

Permettez-moi de vous donner une brève chronologie de mes efforts personnels pour avoir droit à la divulgation complète d'un profil d'électeur généré par SCL Elections à partir du cycle des élections présidentielles de 2016, aux termes de la Data Protection Act de 1998 du Royaume-Uni, à la suite de requêtes devant les tribunaux et grâce aux mesures d'exécution du Commissariat à l'information du Royaume-Uni.

En janvier 2017, j'ai déposé une demande d'accès par sujet sur le site cambridgeanalytica.org afin d'obtenir mon dossier d'électeur, après avoir été avisé de la possibilité d'un tel accès. J'ai dû payer des frais de 10 £ à SCL Elections Limited, en plus de fournir des copies d'une pièce d'identité délivrée par le gouvernement et d'une facture de services publics pour valider mon lieu de résidence.

En mars 2017, j'ai reçu un message de datacompliance@sclgroup.cc, en guise de tentative de réponse pour être conforme à la Data Protection Act de 1998. Le tout comprenait une lettre signée par le chef d'exploitation de SCL Group, Julian Wheatland, et une feuille de calcul Excel contenant des données sur l'inscription électorale et un modèle idéologique composé de 10 sujets politiques classés selon les prévisions d'allégeance politique et de participation. Je m'attendais à recevoir beaucoup plus de données, puisque le PDG de Cambridge Analytica, Alexander Nix, s'était fréquemment vanté de recueillir jusqu'à 5 000 points de données pour chaque électeur américain.

En juillet 2017, j'ai déposé une plainte auprès du Commissariat à l'information en vertu de l'article 7 de la Data Protection Act du Royaume-Uni, parce que SCL Elections Limited avait refusé de répondre à la moindre question ou préoccupation concernant les données fournies.

En octobre 2017, j'ai lancé une campagne de financement collectif dans le but d'intenter une poursuite contre SCL Elections et les sociétés connexes devant la Haute Cour de Justice.

En février 2018, j'ai témoigné devant le comité spécial de la Chambre des communes du Royaume-Uni sur le numérique, la culture, les médias et le sport, dans le cadre de ses audiences tenues à Washington, D.C.

En mars 2018, j'ai déposé et signifié une requête à l'encontre de SCL Group et de Cambridge Analytica aux termes de l'article 7 de la Data Protection Act pour exiger la divulgation complète de mon profil d'électeur. Le document comprenait des déclarations de témoins experts qui expliquaient en quoi les données fournies ne pouvaient pas être jugées complètes.

En mai 2018, le Commissariat à l'information a envoyé un avis d'exécution à SCL Elections Limited, lui demandant de se conformer à son ordonnance visant la pleine divulgation de mon profil de données d'électeur, sous peine de sanctions pénales.

En juin 2018, j'ai témoigné devant la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, aux côtés de la commissaire à l'information et des sous-commissaires à l'information. Au même moment, pendant notre comparution à Bruxelles, le délai accordé à SCL Elections prenait fin sans que celle-ci ait donné suite à l'ordonnance d'exécution.

En décembre 2018, j'ai donné instruction à un avocat spécialisé dans le domaine de l'insolvabilité de contester la tentative faite par les administrateurs pour liquider la plupart des entreprises de SCL Group, et j'ai obtenu une ordonnance du tribunal me donnant droit à la divulgation de tous les documents produits par les administrateurs, ce qu'ils ont refusé de nous transmettre.

En janvier 2019, le Commissariat à l'information du Royaume-Uni a intenté une poursuite contre SCL Elections pour ne pas avoir donné suite à l'ordonnance d'exécution visant la divulgation de mes données. Même si la société avait manifesté son intention de plaider non coupables dans ses documents publics, les coadministrateurs ont fini par déposer, à la surprise de tous, un plaidoyer de culpabilité, en plus de payer les frais de justice et les amendes connexes. Lors du procès, on a rapporté que le Commissariat à l'information avait finalement reçu les mots de passe aux serveurs saisis auprès de Cambridge Analytica/SCL aux termes d'un mandat en matière criminelle, délivré en mars 2018. Selon les communications auxquelles j'ai eu accès en décembre 2018 en vertu de l'ordonnance du tribunal, le Commissariat à l'information avait cherché à obtenir ces mots de passe probablement dès mai 2018.

● (1550)

En mars 2019, la Haute Cour britannique entendra notre contestation de la proposition formulée par les coadministrateurs pour liquider les entreprises de SCL Group. Nous présenterons des éléments de preuve qui mettent en évidence des préoccupations selon lesquelles les administrateurs et les directeurs ont induit le tribunal en erreur sur des questions cruciales. De plus, la Haute Cour a été mise au courant d'une preuve découverte par Chris Vickery, un de vos autres témoins d'aujourd'hui, preuve qui démontre comment les anciens employés de Cambridge Analytica et de SCL ont créé de nouvelles sociétés, tout en ayant accès aux bases de données de CA/SCL qui sont hébergées dans le nuage.

Nous continuerons à réclamer une divulgation complète de mon dossier de données et nous n'abandonnerons pas tant que nous n'aurons pas obtenu pleine réparation. Le Commissariat à l'information du Royaume-Uni et le comité du numérique, de la culture, des médias et du sport ont tous deux déclaré à maintes reprises que, les données des électeurs américains ayant été traitées au Royaume-Uni par SCL, l'affaire est assujettie à la Data Protection Act et relève du Commissariat à l'information du Royaume-Uni.

La quête en vue de rapatrier mon dossier d'électeur depuis le Royaume-Uni nous en dit long sur les droits fondamentaux en matière de données, droits que les États-Unis et le Canada n'ont pas encore établis et protégés dans l'intérêt de leurs citoyens. Nous comprenons bien maintenant comment le droit en matière de données sous-tend la protection des données et constitue un élément essentiel pour le maintien de la démocratie au XXI^{e} siècle.

Nous pouvons également mieux comprendre comment la protection des données et la politique de protection des renseignements personnels s'imbriquent dans les autres cadres juridiques, comme les traités internationaux, le droit de la faillite et de l'insolvabilité, la loi électorale, les règles sur le financement des campagnes et même les règles antitrust.

Je serai heureux de répondre aux questions des membres du Comité au sujet du périple que j'ai entrepris en réclamant mes données auprès de Cambridge Analytica et des conséquences possibles pour l'avenir de notre démocratie numérique.

Merci.

● (1555)

Le président: Merci, monsieur Carroll.

Nous passons maintenant à M. Vickery, qui se joint à nous par téléconférence, puis ce sera au tour de M. Kint.

À vous la parole, monsieur Vickery.

M. Chris Vickery (directeur de la recherche sur les risques cybernétiques, UpGuard, à titre personnel): Bonjour. C'est un plaisir de témoigner encore une fois devant le Comité. Je suis toujours ravi de discuter avec vous et je crois avoir beaucoup à apporter à la discussion.

J'ai analysé les enregistrements des précédentes réunions de ce sous-comité; il était question de données et de la protection de la vie privée en ce qui concerne la transition vers la numérisation en ligne des services gouvernementaux canadiens, de l'état actuel des choses et de ce qui est prévu, ainsi que les diverses préoccupations du Comité. Même si je suis disposé à répondre aux questions concernant AggregateIQ et Cambridge Analytica, il n'en sera pas question dans mon exposé. Je vais traiter de certains enjeux qui ont été soulevés lors des précédentes réunions que j'ai écoutées et analysées récemment.

Actuellement, nous avons l'impression que le Canada doit prendre une décision concernant la voie qu'il faut adopter ou que le pays souhaite adopter pour sa stratégie en matière de technologie. Nous avons la possibilité de nous lancer la tête première dans la mêlée avec tous les autres gros joueurs et d'essayer d'être à la fine pointe de la transition numérique des services gouvernementaux. Toutefois, j'ai l'impression que la position la plus naturelle d'après ce que j'ai entendu dans les précédentes discussions est de laisser les autres faire des erreurs et prendre la tête du peloton et d'ensuite intégrer les éléments qui fonctionnent dans vos systèmes et de ne pas inclure ce qui ne fonctionne pas. Cela semble être la position la plus avantageuse que j'ai entendue.

Certains se demandaient aussi si nous devrions imposer la transition vers la numérisation des services aux Canadiens qui se sentent peut-être méfiants ou qui ne se sentent pas suffisamment à l'aise pour confier tous leurs renseignements personnels et leurs données médicales à un système « Big Brother », pour le dire ainsi. Si vous imposez le tout, lorsqu'il y aura, le cas échéant, une atteinte à la protection des données ou une vulnérabilité ou un problème qui est exploité, cela risque de saper durement la confiance de la population dans le système.

Je recommande que le Canada essaie de favoriser une adoption en misant sur le succès du système au lieu de l'imposer aux gens. Ce serait beaucoup mieux d'avoir un voisin qui dit à un autre qu'il a obtenu un rendez-vous avec son docteur, que c'était très facile et qu'il lui conseille de le faire en ligne lui aussi que d'avoir ces deux voisins, s'il y a une atteinte à la protection des données, se dire à quel point ils ont détesté se voir imposer cette situation.

J'ai entendu beaucoup de discussions au sujet des chaînes de blocs, et certains ont essayé de laisser entendre que les chaînes de blocs sont la solution. Je me méfie énormément de la technologie de la chaîne de blocs dans son état actuel et même pour la suite des choses. Les chaînes de blocs sont en gros l'endroit où tout le monde consigne tout. C'est un grand livre qui est distribué. Ce n'est pas nécessairement une clé ou une technologie secrète. Je crois que les nombreux échecs importants des diverses monnaies qui reposent sur les chaînes de blocs ont mis en lumière les problèmes inévitables qui peuvent survenir, et cette technologie n'est pas suffisamment éprouvée pour le traitement de données médicales et personnelles et en particulier en ce qui concerne les votes. C'est un cauchemar.

Un autre enjeu qui a été soulevé est l'anonymisation des données et l'importance d'avoir ces bassins de données qui peuvent être étudiées par les ministères et échangées entre eux et être facilement importées d'une banque de données à une autre et la beauté de tout cela. Il est vrai que nous pouvons tirer une foule de renseignements d'une telle étude de l'ensemble des données, mais ce n'est pas possible d'avoir des données anonymisées. C'est un peu inexact de parler de données anonymisées. Vous pouvez avoir des données dont certains éléments sont supprimés ou laisser tomber certains aspects pour essayer de rendre difficile l'identification des gens; toutefois, tout ce que vous pouvez réellement faire lorsque vous anonymisez des données, c'est de rendre le plus difficile possible pour les petits joueurs de repersonnaliser les données. Je peux vous garantir que les grands courtiers en données, les banques et les compagnies d'assurances peuvent repersonnaliser les données de la majorité des ensembles de données anonymisées en se fondant tout simplement sur les données déjà en leur disposition et de référence. C'est simplement la quantité de données qu'a une entité qui détermine le temps qu'il lui faudra pour repersonnaliser les données. Bref, vous devez faire preuve d'une grande prudence quant aux données anonymisées et éviter de penser que c'est infaillible.

Je ne souhaite pas seulement soulever des enjeux ou des problèmes. Je souhaite aussi proposer des idées et faire un remue-méninges concernant divers moyens d'échanger de manière sécuritaire des données entre les ministères. L'idée selon laquelle la protection de la vie privée et la sécurité sont inhérentes est très forte.

● (1600)

À mon avis, si vous créez tout de A à Z, les lois physiques et les éléments constitutifs fondamentaux de l'écosystème dans lequel se trouveront vos données, vous avez l'occasion de chercher la façon de le faire pour que ce soit sécuritaire.

Je m'assurerais que la banque de données A et la banque de données B ne parlent même pas la même langue, qu'elles ne peuvent pas communiquer entre elles et qu'elles ne peuvent pas regrouper leurs données, et j'aurais un intermédiaire qui recevrait les données et qui les traduirait pour les banques de données.

C'est seulement une idée que j'ai eue. L'avantage de cette option est que vous pouvez décider que le traducteur n'est pas accessible 24 heures par jour, 7 jours par semaine. Lorsque tout le monde dort le samedi soir, vous n'avez pas à craindre qu'un individu malintentionné s'introduise dans une banque de données et ait ainsi accès à toutes les autres. C'est une question de segmentation, de morcellement et de fragmentation. Même si cela rend plus complexe la programmation, je crois que vous obtiendrez un meilleur résultat si vous prévoyez dès le départ de tels éléments, que vous faites bien les choses et que vous vous assurez que tous les intervenants adoptent le bon état d'esprit.

Enfin, je tiens à dire que, s'il y a bien une chose qui doit être faite à l'ancienne, c'est de voter. Le vote numérique est sujet à une vaste gamme de problèmes et à la corruption. S'il y a bien une chose que nous devons faire sur papier et à la main, c'est de voter. Je suis très déçu de la manière dont les États-Unis abordent la question du vote, et je souhaite que votre pays s'y prenne beaucoup mieux.

Merci.

Le président: Merci encore une fois, monsieur Vickery.

Monsieur Kint, vous avez 10 minutes.

M. Jason Kint (chef de la direction, Digital Content Next): Bonjour.

Merci de nous donner l'occasion de prendre la parole devant votre comité aujourd'hui. J'ai suivi de près les travaux du Comité, y compris la superbe représentation par le président et les vice-présidents en novembre dernier à l'occasion du Grand Comité international sur la désinformation et les fausses nouvelles. Je suis honoré d'être là, et je vous remercie de votre intérêt général pour la protection de la vie privée des consommateurs.

Je suis chef de la direction de DCN. Notre mission est de répondre aux besoins uniques et divers du contenu numérique de qualité. Cela comprend de petits et grands éditeurs haut de gamme, tant des nouveaux venus que des entreprises qui existent depuis des siècles. J'aimerais préciser que, parmi nos membres, nous ne comptons aucun réseau social, aucun moteur de recherche et aucun fournisseur de technologies publicitaires. Bien que 80 % des revenus numériques de nos membres proviennent de la publicité, nous collaborons avec eux pour qu'ils prennent de l'expansion et se diversifient.

DCN agit à titre de partenaire stratégique pour ses membres; nous fournissons des conseils et nous formulons des recommandations, le regard tourné vers l'avenir.

Comme vous le savez, les consommateurs peuvent trouver du contenu en ligne à divers endroits. En raison de cette dynamique, les éditeurs haut de gamme doivent impérativement maintenir la confiance des consommateurs. Notre entreprise se concentre sur le repérage des enjeux qui minent la confiance sur le marché, et je suis ravi de le faire aujourd'hui. Par conséquent, le renforcement de la protection de la vie privée des consommateurs et la croissance des intérêts de nos membres sont un enjeu critique et stratégique pour nous.

Depuis une décennie, nous avons connu une grande augmentation dans le domaine de l'automatisation de la distribution et de la monétisation du contenu, en particulier avec la publicité. Nous sommes passés à un monde où l'achat, la mise aux enchères, le commerce et la vente de publicités se produisent avec une intervention humaine minimale. Nous ne nous attendons pas à ce que cette tendance se renverse, et ce n'est pas ce que nous cherchons à accomplir, mais je vais essayer de vous présenter aujourd'hui certains grands défis qui ont des effets sur l'industrie, la population et la démocratie.

Le premier domaine dont j'aimerais parler est la montée de ce que votre rapport de décembre qualifie à juste titre de « monopoles de données ». Malheureusement, l'écosystème qui s'est développé impose très peu de contraintes légitimes en ce qui a trait à la collecte et à l'utilisation des données des consommateurs. Par conséquent, on accorde une plus grande valeur aux données personnelles qu'au contexte, aux attentes des consommateurs, au droit d'auteur ou même aux faits.

Aujourd'hui, des tiers inconnus collectent fréquemment les données des consommateurs à l'insu des consommateurs et sans qu'ils puissent exercer un quelconque contrôle. Les données servent ensuite à cibler des utilisateurs sur le Web, sans tenir compte du contexte et au coût le plus bas possible.

Selon nous, c'est le péché originel du Web, soit de permettre une surveillance continue des consommateurs dans de multiples contextes. Cette dynamique offre une motivation aux personnes malveillantes et parfois aux criminels, et c'est particulièrement vrai sur des plateformes non gérées comme les médias sociaux où l'objectif est d'aller chercher un clic de la part d'un consommateur ou d'un robot.

Quel est le résultat? Une concentration massive des entités qui profitent de la publicité numérique, nommément Google et Facebook. Il y a trois ans, DCN a réalisé la première analyse, et nous avons qualifié ce groupe de « duopole ». Les chiffres sont sidérants. Avec un marché de la publicité numérique en Amérique du Nord et dans l'Union européenne qui se chiffre à plus de 150 milliards de dollars, de 85 à 90 % de la croissance graduelle et plus de 70 % des dépenses totales en publicité vont à ces deux entreprises.

Nous avons ensuite cherché à en savoir plus et nous avons établi un lien, comme vous l'avez fait dans votre rapport, entre la concentration de leurs revenus et leurs pratiques relatives aux données. Ces deux entreprises réussissent à recueillir des données comme personne d'autre n'est capable de le faire. Les données sont la source de leur pouvoir. Google a des systèmes de balises de suivi qui permettent de recueillir des données sur les utilisateurs d'environ 75 % d'un million de sites Web parmi les plus fréquentés. Grâce aux renseignements fournis au Comité DCMS au Royaume-Uni, nous avons aussi appris que Facebook a des balises de suivi sur plus de huit millions de sites Web. Cela signifie que les deux entreprises sont en mesure de voir une très grande partie de votre historique de navigation et de position.

Même si vos travaux se concentrent principalement sur Facebook, nous vous encourageons fortement à vous pencher aussi sur le rôle de Google sur le marché des publicités numériques. DCN a récemment contribué à la diffusion d'une recherche réalisée par Doug Schmidt de l'Université Vanderbilt qui portait sur la collecte de données à grande échelle de Google.

Google a profité de sa dominance inégalée comme navigateur, système d'opération et moteur de recherche pour devenir l'entité qui profite le plus de la prestation de services de technologies publicitaires. Google est sans égal à toutes les étapes de la chaîne d'approvisionnement des publicités: l'achat, la vente, le commerce et la mesure de publicités. Si cela concernait tout autre marché, ce serait illégal. Dans le milieu financier, c'est l'équivalent d'être le courtier en valeurs mobilières, le preneur ferme, la bourse et les actions en soi.

Par conséquent, nous croyons que les recommandations 12 et 13 de votre rapport sont importantes parce que vous cherchez à comprendre la relation claire entre la concurrence et la politique sur les données. L'essor de ces monopoles de données a entraîné un décalage entre les créateurs de contenu et ceux qui en profitent. Cette situation a permis un cycle vicieux dans lequel les règles concernant l'industrie et la vie privée des consommateurs visent à protéger les intérêts des membres de l'industrie au lieu de préserver la confiance des consommateurs.

● (1605)

Nous vous encourageons aussi à examiner de plus près les arguments du professeur de droit, Maurice Stucke, et d'Anthony Durocher de votre Bureau de la concurrence dont la recommandation est de délaisser l'analyse axée sur le prix étant donné que les entreprises offrent des produits gratuits pour exploiter les données des consommateurs. Compte tenu des conclusions du Commissariat à l'information du Royaume-Uni concernant les pratiques de Facebook en matière de protection de la vie privée de 2007 à 2014, que vous avez qualifiées dans votre propre rapport de « sévères », j'attire votre attention sur un rapport de recherche qu'a publié la semaine dernière Dina Srinivasan. Ce rapport s'intitule *The Antitrust Case Against Facebook*, et Mme Srinivasan y décrit la pratique de leurre publicitaire qu'utilisait Facebook à ses débuts. Au départ, Facebook utilisait la protection de la vie privée comme principal élément pour se démarquer dans le milieu très concurrentiel des réseaux sociaux gratuits où la concurrence reposait sur la qualité des produits, et la qualité de la protection de la vie privée a diminué au fil du temps.

Enfin, le scandale impliquant Facebook et Cambridge Analytica expose la dynamique dysfonctionnelle actuelle. Sous prétexte de mener des recherches, GSR a recueilli des données sur des dizaines de millions d'utilisateurs de Facebook. Comme nous le savons maintenant, Facebook n'a pratiquement rien fait pour s'assurer que GSR ne diffuse pas ces données. Les données de Facebook ont finalement été vendues à Cambridge Analytica pour diffuser des publicités et des messages ciblés à saveur politique, notamment durant les élections américaines de 2016.

Avec le pouvoir que détient Facebook sur notre écosystème d'information, nos vies et notre démocratie, il est essentiel de savoir si cette société est digne de confiance. Bon nombre de ses pratiques avant la publication des rapports sur le scandale impliquant Cambridge Analytica justifient clairement une forte méfiance à son endroit. Même si nous avons eu droit à une série d'excuses bien documentées et interminables, il est important de noter qu'il y a eu très peu de changements au sein de la direction et de la gouvernance de l'entreprise. Dans cet esprit, une enquête plus approfondie est vraiment nécessaire, et les refus répétés de l'entreprise de laisser son chef de la direction témoigner devant le Comité DCMS ou votre grand comité ne font que renforcer cette nécessité. Nous avons entendu que le responsable est le chef de la direction, Mark Zuckerberg, mais il évite les questions les plus difficiles de reddition de comptes. Il y a encore beaucoup d'éléments à apprendre au sujet de ce qui s'est passé et de l'ampleur de ce que Facebook savait au sujet du scandale avant qu'il éclate au grand jour. La chronologie me laisse perplexe.

Le témoignage de M. Zuckerberg devant le Comité sénatorial américain de la justice nous a permis d'apprendre qu'il avait été décidé de ne pas informer les utilisateurs de Facebook que leurs données avaient été vendues à Cambridge Analytica après la publication de l'article du *Guardian* en décembre 2015. Le journaliste du *Guardian* affirme avoir communiqué avec GSR dès la fin de 2014, soit près d'un an avant l'article. Le cofondateur de GSR, Aleksandr Kogan, a confirmé au sénateur John Thune que son partenaire et lui avaient rencontré des représentants de Facebook à plusieurs reprises en 2015. Ce que j'ai encore plus de mal à croire, c'est que Facebook a embauché Joseph Chancellor, le prétendu partenaire à part égal de Kogan chez GSR, le 9 novembre 2015, soit un mois avant l'article du *Guardian*. Des questions ont été posées à maintes reprises à Facebook pour comprendre le moment exact où M. Zuckerberg a été mis au courant au sujet de Cambridge Analytica. Or, Facebook donne seulement une pseudo-réponse et affirme que M. Zuckerberg a appris en mars 2018 que les données n'avaient pas été supprimées. Personnellement, je trouve cette réponse obtuse et offensante.

Étant donné que la FTC a conclu un jugement convenu avec Facebook concernant le signalement de toute utilisation fautive de données, c'est extrêmement pertinent de savoir quand le chef de la direction a été mis au courant au sujet de Cambridge Analytica. Nous savons maintenant que Facebook a consacré beaucoup plus de temps et de ressources en 2016 en vue d'aider Cambridge Analytica à acheter et à diffuser des campagnes publicitaires que ce que la société a investi pour réparer ce qu'elle appelle son « abus de confiance ». Même si le chef de la direction de Facebook a affirmé devant le Congrès américain en avril 2018 que l'entreprise s'est immédiatement mise au travail pour s'assurer de la suppression des données après avoir été mise au courant de la situation en 2015, Facebook a déjà présenté au Comité DCMS des renseignements selon lesquels Cambridge Analytica n'a fourni une attestation légale à cet effet que tard en 2017 lorsque son chef de la direction a envoyé un bout de papier relativement inutile.

Enfin, Facebook a annoncé en septembre 2018 que M. Chancellor n'était plus employé de Facebook, et ce, sans fournir d'explications et après une enquête de près de six mois, qui a seulement débuté après que l'émission *60 Minutes* a permis d'attirer davantage l'attention sur son rôle.

Ce qui est tout aussi troublant dans toute cette histoire, outre les promesses verbales de Facebook, c'est que nous ne savons pas clairement ce qui pourrait empêcher cette situation de se reproduire. Pour la suite des choses, nous demandons aux décideurs et à l'industrie d'offrir une plus grande transparence et plus de choix aux consommateurs en ce qui a trait à la collecte de données dans le cas de pratiques auxquelles les consommateurs ne sont pas en droit de s'attendre. Les consommateurs s'attendent à ce que les propriétaires du site Web ou de l'application recueillent des renseignements à leur sujet pour s'assurer du fonctionnement du site Web ou de l'application. La collecte de données dans un contexte précis tend à correspondre aux attentes des consommateurs en la matière, parce qu'il y a un lien direct entre ces activités et l'expérience des consommateurs et que les données des consommateurs sont recueillies et utilisées de manière transparente dans ce même contexte. Toutefois, comme nous l'avons vu dans le cas de Facebook et de Cambridge Analytica, les données recueillies dans un contexte et utilisées dans un autre ont tendance à aller à l'encontre des attentes des consommateurs.

● (1610)

Par ailleurs, il est important de souligner que les consommateurs ne profitent normalement pas directement de l'utilisation secondaire de données. Nous vous recommandons de vous demander si nous devrions même permettre l'utilisation secondaire de données par des fournisseurs de services qui peuvent recueillir des données sur une vaste gamme de sites Web, d'applications et d'appareils, et ce, sans obtenir le consentement éclairé et explicite des consommateurs. En imposant des normes plus rigoureuses en la matière, nous pourrions régler bon nombre des enjeux qui ont déjà été mentionnés.

Enfin, il est important de faire la lumière sur ces pratiques et de trouver la meilleure manière de les encadrer à l'avenir. Je vous remercie de vos travaux en vue de mieux comprendre le monde numérique. Vos travaux en vue de dévoiler ce qui s'est passé et d'en tirer des leçons contribueront à créer un marché sain et à rétablir la confiance des consommateurs.

Le président: Merci, monsieur Kint.

Nous commencerons par une série de questions de sept minutes. La parole est en premier à M. Erskine-Smith.

M. Nathaniel Erskine-Smith: Merci beaucoup.

Je vais poser à chacun d'entre vous des questions différentes.

Je vous remercie tous de votre présence ici aujourd'hui.

Monsieur Vickery, j'aimerais poser en premier une question sur le gouvernement numérique, soit un sujet qui sera au coeur de nos discussions pour les prochaines semaines au Comité. Par exemple, en ce qui concerne les chaînes de blocs, vous avez soulevé quelques inquiétudes en ce qui concerne la protection de la vie privée concernant la transition d'autres services en ligne. Le modèle à la base de cette étude est le modèle estonien, et ce modèle comporte trois principaux éléments qui contribuent à la protection de la vie privée, selon ce que j'en comprends.

Le premier élément est l'identification numérique, et c'est un appareil chiffré qui me permet d'avoir accès aux services gouvernementaux et qui nécessite d'autres niveaux d'authentification. Deuxièmement, la technologie de la chaîne de blocs est utilisée. Ce pays l'utilisait avant que le reste d'entre nous comprenne qu'il s'agit de la technologie de la chaîne de blocs. C'est la technologie de la chaîne de blocs KSI. C'est une sorte de technologie de la chaîne de blocs qui aurait été inventée en Estonie, et plus de 100 pays dans le monde l'utilisent. Troisièmement, lorsque des fonctionnaires accèdent aux profils des gens, le système consigne l'heure, et la raison pour laquelle le fonctionnaire a eu accès à cette information est transparente.

Ce que je souhaite réellement vous demander, c'est de nous dire ce qui cloche avec le modèle estonien.

● (1615)

M. Chris Vickery: Le problème avec ce modèle est qu'il suffit d'un petit défaut dans la protection pour gâcher l'ensemble du système. Depuis quelques années, je me consacre jour et nuit à répertorier les atteintes à la protection des données. J'en ai trouvé bon nombre, et les entreprises qui sont victimes de ces atteintes à la protection des données mentionnent sur leur site Web que l'entreprise respecte les pratiques courantes de l'industrie ou qu'elle utilise un niveau élevé de sécurité et de chiffrement, etc. Je constate que ces banques de données sont accessibles au public sur Internet et qu'elles ne sont pas chiffrées. Les systèmes ne sont pas protégés par un mot de passe ou un nom d'utilisateur. Il suffit d'un seul développeur qui gâche le tout, qui coupe les coins ronds et qui fait quelque chose d'un peu trop risqué et non conforme aux pratiques exemplaires.

M. Nathaniel Erskine-Smith: À titre de précision, si vous réussissez à trouver un moyen d'accéder au système en Estonie, j'aimerais le savoir, parce que je crois comprendre que les autorités révoquent le certificat, si l'identification numérique est volée. Je crois comprendre que ce système est en place depuis 2000 et que les autorités affirment qu'il n'y a eu aucun vol d'identité.

Si ce système avait un grave problème, une telle situation serait déjà survenue, étant donné que le système est en place depuis très longtemps, mais je me trompe peut-être.

M. Chris Vickery: Comparez cela aux affirmations du gouvernement indien concernant la banque de données du système Aadhaar. Les autorités indiennes ont fait des affirmations semblables concernant cette banque de données. Or, à plusieurs reprises, il a été démontré que ce système a été victime d'importantes atteintes à la protection des données en ce qui concerne le portail d'accès et le système d'encodage de base de la carte d'identité du système Aadhaar.

Je ne sais pas si je crois les autorités estoniennes lorsqu'elles affirment n'avoir jamais connu d'atteintes à la protection des données ou de problèmes ou si ces affirmations cherchent à nous tromper. C'est peut-être un aspect que je pourrais approfondir un peu plus.

M. Nathaniel Erskine-Smith: Si vous pouviez prendre le temps d'examiner le tout avec vos yeux d'expert et nous envoyer par écrit vos constatations, je vous en serais reconnaissant. Cela nous serait grandement utile.

Monsieur Carroll, d'après ce que vous avez vu, vous avez soulevé des inquiétudes concernant la transformation en armes des données et l'érosion d'un discours commun. Vous vous êtes évidemment vous-même penché de manière très utile sur cette question pour comprendre cet important scandale et vraiment trouver le plus de réponses possible.

M. Kint a fait référence à certaines de nos recommandations. Avez-vous aussi lu notre rapport?

M. David Carroll: Oui.

M. Nathaniel Erskine-Smith: D'accord. Sommes-nous passés à côté de quelque chose?

M. David Carroll: J'aimerais avoir l'occasion de relire votre rapport en ayant cette question en tête, mais je crois que j'admire l'audace du rapport de proposer une possible manière pour nos partis politiques de se réglementer eux-mêmes sur ces questions. Selon moi, cette recommandation allait plus loin que celle de Mme Denham, la commissaire à l'information, qui visait à imposer un frein éthique sur le microciblage.

J'en suis heureux. Je crois que c'est la principale question pour de nombreux gouvernements dans le monde. Comment l'exemption pour le ciblage à des fins politiques cause-t-elle la perte de l'ensemble du système? Dans le cas de Cambridge Analytica, les données politiques ont été utilisées à des fins commerciales, et les données commerciales ont été utilisées à des fins politiques. C'est assez difficile...

M. Nathaniel Erskine-Smith: Je crois qu'il est juste de mentionner que ce serait certainement illégal ici, même selon les règles actuelles.

Prenons l'exemple d'une modification que le gouvernement a adoptée avec le projet de loi C-76 en ce qui concerne une banque de données. Il faut verser les publicités politiques dans une banque de données consultable. Nous avons ensuite recommandé que ce soit le plus convivial possible, et je dirais qu'il faut vraiment concevoir ce système avec les journalistes en tête pour leur donner les moyens d'accomplir leur travail et de demander des comptes à des gens comme moi pour les publicités que nous avons diffusées durant les élections. Est-ce suffisant?

Lorsque vous parlez d'un discours commun et de chambres d'écho, pour ainsi dire, croyez-vous cette réponse suffisante?

● (1620)

M. David Carroll: C'est un premier pas important. Je crois qu'il faut imposer un degré maximal de transparence pour demander des comptes en ce qui a trait aux publicités. Par exemple, la majorité des utilisateurs de Facebook ne sont pas conscients que des partis et des campagnes politiques versent leurs données sur les dossiers d'inscription des électeurs dans Facebook pour les cibler personnellement avec leur nom. C'est très difficile de trouver cette information dans l'interface de Facebook, et ce marketing personnalisé n'apparaît même pas dans l'outil de transparence de Facebook qui a été lancé ici au Canada.

Je crois qu'une divulgation maximale sera aussi bénéfique pour les citoyens inquiets. Je crois que ce sont les détails qui comptent. Vous devriez être informé que vous avez été ciblé en tant qu'électeur pour recevoir des messages précis au lieu d'entendre Facebook parler des segments. Par ailleurs, les gens doivent aussi être informés s'ils ont été affectés à ce que nous appelons des « auditoires similaires ». Cette situation crée une sorte de ciblage personnalisé sans que votre nom y soit attaché.

Je préconise le plus de divulgation possible en ce qui concerne les publicités politiques et peut-être les publicités en général.

M. Nathaniel Erskine-Smith: Mon temps est écoulé, mais j'accepte votre proposition. Après votre deuxième lecture de notre rapport, faites-nous parvenir par écrit les éléments à côté desquels nous sommes passés.

Le président: Merci, monsieur Erskine-Smith.

Monsieur Kent, vous avez sept minutes.

L'hon. Peter Kent: Merci, monsieur le président.

J'aimerais commencer par vous, monsieur Vickery. Il ne fait aucun doute que l'établissement du gouvernement numérique au Canada sera très différent de celui en Estonie, étant donné que nous avons des provinces, des territoires, des administrations municipales, des gouvernements régionaux et le gouvernement fédéral et que les champs de compétences sont clairement définis.

Même pour ce qui est des premières formes d'un gouvernement numérique limité... Disons que le gouvernement canadien examine seulement ses champs de compétences qui touchent l'ensemble de la population du pays. Il va sans dire que nous aurions raison de nous attendre à ce qu'il y ait une sorte de ruée vers l'or pour les entreprises qui souhaitent s'occuper de la création ou de l'administration ou devenir des partenaires, pour le dire ainsi, en vue de mener cette transition numérique d'envergure.

L'Association des banquiers canadiens ou, du moins, son président, a laissé entendre que les banques sont les gestionnaires de données personnelles les plus dignes de confiance. Elles ont des méthodes d'authentification à deux facteurs et elles sont plus responsables que, par exemple, les Equifax de ce monde, les autres entreprises qui collectent des données, les courtiers en données et certainement plus responsables que des sociétés comme Alphabet, Google, Facebook, etc.

Quelles lignes directrices suggériez-vous au gouvernement s'il souhaitait mettre en place un gouvernement numérique? À quels types d'entreprises lui recommanderiez-vous de confier à l'interne la création et la maintenance pour se porter garantes de la sécurité?

M. Chris Vickery: Je crois que le secteur bancaire n'est pas un mauvais choix. C'est une industrie très réglementée qui a l'habitude d'avoir des audits très approfondis, de conserver des traces écrites et de faire tout à la lettre, du moins c'est ce que nous espérons. Je crois que c'est effectivement un exemple d'une bonne industrie. Toutefois, je ferais preuve d'une extrême prudence concernant l'utilisation possible des données à d'autres fins. J'établirais des limites claires de concert avec le groupe choisi pour profiter de son expertise et de son infrastructure pour indiquer ce qui est acceptable et ce qui ne l'est pas. Vous ne pouvez pas broncher ou brouiller les limites. Il s'agit d'une limite claire, et les contrevenants sont passibles de sanctions. Vous devez ensuite faire respecter le tout, le cas échéant.

L'hon. Peter Kent: En ce qui a trait au modèle estonien, là où il y a un cloisonnement — selon la différente autorité concernée, l'éducation, la santé, les taxes, etc. —, un jeton est utilisé pour avoir accès aux renseignements personnels d'une personne ou aux renseignements qui peuvent être demandés, et cela fonctionne en vase clos. Toutefois, vous avez soulevé des préoccupations concernant la circulation des renseignements entre les systèmes en vase clos et les possibles points d'intrusion en raison d'un acte délibéré ou accidentel au moment de la création.

● (1625)

M. Chris Vickery: Oui. Je vous préviens de ne pas permettre aux banques de données segmentées qui fonctionnent en vase clos de communiquer entre elles. Si vous avez besoin de données, obtenez-les en les demandant au propriétaire des données, parce que les données n'appartiennent pas vraiment au citoyen si les banques de données peuvent communiquer entre elles. Ces systèmes ne jouent alors qu'un rôle de gardien facultatif.

L'hon. Peter Kent: Proposez-vous que chaque système en vase clos soit géré par le créateur du programme central?

M. Chris Vickery: À mon avis, si vous mélangez les administrateurs, cela revient à mélanger les banques de données. Les administrateurs sont humains, et la nature humaine fait que nous voulons réduire le travail et simplifier le plus possible les choses. C'est là que nous coupons les coins ronds.

L'hon. Peter Kent: J'ai quelques questions pour MM. Carroll et Kint.

En raison des conséquences du scandale impliquant Facebook-Cambridge Analytica-AggregateIQ et des histoires que nous avons entendues, nous avons vu des gens fermer leur compte Facebook. Il règne un certain scepticisme et de la peur chez certains concernant l'atteinte à la vie privée par l'entremise des médias sociaux. Comment pouvons-nous donner l'assurance à la population que les services numériques fournis par le gouvernement peuvent être sécuritaires et protégés et qu'une atteinte à la vie privée est improbable, voire impossible?

Monsieur Carroll, vous pouvez y aller en premier.

M. David Carroll: Je crois que la réaction à l'égard du scandale impliquant Cambridge Analytica montre que nous avons une réaction viscérale par rapport à cette situation. Nous ne comprenons pas exactement pourquoi cela nous fâche, mais ce nom est devenu du jour au lendemain bien connu dans le monde. En ce qui concerne précisément cet aspect, nous comprenons qu'il y a des motivations qui entrent en ligne de compte, et le gouvernement ne cherche pas à tirer profit des données ou à nécessairement s'en servir pour commettre des actes répréhensibles. Nous n'avons pas l'impression que des personnes sans scrupule pourraient exploiter à mauvais escient ce système.

Tant que nous nous protégeons au gouvernement contre les atteintes à la vie privée, soit le pire des scénarios, je crois que la confiance dans le gouvernement numérique est beaucoup plus probable que la confiance dans les publicités numériques.

M. Jason Kint: J'aimerais seulement ajouter que cela illustre bien pourquoi Facebook doit rendre des comptes. Edelman réalise chaque année une étude, soit le Baromètre de la confiance, et nous avons vu que la confiance dans les institutions a chuté en raison du scandale Facebook. Edelman est allé plus loin pour la première fois et a commencé à décortiquer ce qui se passait, surtout en ce qui a trait à la confiance dans les médias, ce qui est l'élément qui me préoccupe le plus dans mon rôle. La confiance dans le journalisme était en hausse ou reprenait du mieux, et le problème était en fait la confiance des gens dans la plateforme. Ces plateformes font partie de nos vies et elles commencent à miner la confiance dans d'autres domaines. Bref, la confiance que nous avons dans les médias a commencé à être minée par ce qui se passe avec Facebook et le déclin de la confiance par rapport à cette plateforme.

Edelman vient de publier sa nouvelle recherche il y a trois semaines, et il y avait un écart de 30 points entre la confiance dans les médias sociaux et la confiance dans les médias traditionnels. Je suis inquiet de voir que, lorsque les choses tournent au vinaigre avec une plateforme, cela commence à nuire à l'ensemble.

L'hon. Peter Kent: Comment le gouvernement pourra-t-il en donner l'assurance à la population pour les mêmes raisons? Êtes-vous d'accord avec les raisons que M. Carroll...

M. Jason Kint: Je crois qu'il faut demander des comptes à Facebook. Cela forcera la société à restaurer la confiance des gens à l'égard de son propre produit, ce qui pourrait prendre beaucoup de temps. Elle sera peut-être prise dans cette spirale négative. Cela permettra de renforcer la confiance à l'égard de l'ensemble de la plateforme.

Le président: Merci. Vous avez cinq secondes.

L'hon. Peter Kent: Ça va, je vais y revenir plus tard.

Le président: Nous allons y revenir. Il nous restera du temps tout à l'heure.

Notre prochain intervenant est M. Cullen, pour sept minutes.

Merci d'avoir réintégré le Comité et de nous faire l'honneur de votre présence. Nous sommes heureux de vous revoir.

M. Nathan Cullen: Monsieur le président, après ma série de questions, vous pourrez décider si ma présence est à la hauteur, mais je vous remercie de toute manière.

Merci à nos témoins d'être ici.

Il y a beaucoup de choses que j'aimerais approfondir, mais notre temps est limité, alors je vais essayer d'être clair et bref, et de me contenter de suivre le cours des événements qui ont marqué, disons, l'ingérence ou la tentative de corruption — ou la corruption réussie — relativement aux élections américaines et au vote sur le Brexit.

Monsieur Kint, dans votre intervention, vous avez parlé de responsabilité. Est-ce que la chaîne commence par l'accès, illégal ou non, aux bases de données que les partis détiennent sur les citoyens? Les partis recueillent une énorme quantité de renseignements sur les électeurs, sur les intentions de vote et sur les lieux de vote, et sans doute aussi sur le revenu et les préférences des électeurs. Or, une fois qu'ils ont été piratés — à cause de lacunes sur le plan de la sécurité —, ces renseignements ont pu être utilisés à mauvais escient par les médias sociaux. Dans votre dernière intervention, vous avez évoqué la responsabilité de Facebook.

Pour cette entreprise, il s'agit d'un événement qui met sa survie en péril. La confiance est importante pour toute entreprise, en particulier pour les médias sociaux. Quelle a été la réaction depuis que ce scénario a été prouvé, c'est-à-dire le piratage du Comité national démocrate et des républicains, les mensonges ciblés qui ont ensuite été diffusés lors de cette élection et le fait que Facebook n'ait pas de compte à rendre à ses utilisateurs concernant la sécurité de leurs données?

● (1630)

M. Jason Kint: De notre point de vue, cela est très décevant. En novembre 2016, au moment des élections, j'ai envoyé une lettre à M. Zuckerberg au nom de notre association pour lui demander de prendre les grands moyens, compte tenu de l'ampleur du problème. Il ne fait aucun doute que l'entreprise dispose de certains des meilleurs ingénieurs au monde et qu'elle a d'énormes ressources pour résoudre des problèmes comme celui-là.

Nous avons été très déçus. Jusqu'ici, il s'agit davantage d'une stratégie de relations publiques que d'autre chose, et il semble que Facebook s'en soit servi encore plus résolument au cours des derniers mois.

M. Nathan Cullen: Vous voulez dire, de cette stratégie de relations publiques.

M. Jason Kint: De cela et de la critique des médias et de tous ceux qui essaient de les tenir responsables.

M. Nathan Cullen: D'accord, c'est ce que je recherche. Chaque entreprise a une culture, et sa réaction au fait d'avoir été exposé de façon importante rend compte de la description que cette entreprise se fait de sa culture.

Récemment, le gouvernement a présenté une stratégie pour lutter contre les fausses nouvelles lors des prochaines élections, élections qui auront lieu dans à peine huit ou neuf mois. Lorsque nous en sommes arrivés à la partie du plan qui traitait des médias sociaux, les mots « espoir » et « attentes » ont été évoqués, mais il n'y avait aucune exigence pour les plateformes de médias sociaux.

Monsieur Carroll ou monsieur Kint, je ne sais pas si vous avez eu vent en tout ou en partie de cette annonce. Quoi qu'il en soit, la question est d'établir ce que les médias sociaux doivent faire pour protéger les Canadiens de toute ingérence étrangère ou autre. Suffit-il d'espérer et de s'attendre à ce que des groupes comme Facebook et Google fassent ce qu'il faut pour protéger les données, pour empêcher l'utilisation à mauvais escient de fausses nouvelles et le ciblage des électeurs, pour aiguiller les électeurs vers les mauvais bureaux de vote et les tromper quant à leurs intentions?

M. Jason Kint: Selon moi, particulièrement en ce qui concerne Facebook, nous sommes rendus plus loin que cela, et c'est là que j'espère que la Federal Trade Commission interviendra et fera appliquer le décret de consentement. C'est en probation depuis sept ou huit ans.

Pour bon nombre des problèmes que vous avez évoqués dans votre question, y compris la façon dont les partis politiques utilisent les données, il faut aller beaucoup plus loin en amont de la collecte et de l'utilisation réelles des données. En ce qui concerne Facebook, c'est là que les choses se passent. Je peux vous donner 10 autres manifestations de ce problème, depuis les robots et la fraude publicitaire jusqu'au recours à des dispositifs de blocage de la publicité par les utilisateurs. Je peux vous donner toute une liste d'exemples sur la façon dont cela touche mon monde, mais ce sont tous des symptômes du problème. Même la désinformation est un symptôme de l'existence d'un problème, et ce problème est l'omniprésence de la collecte de données sur le Web. Or, pour les entreprises qui ont accès à la plupart des activités qui s'y déroulent, cette collecte doit être encadrée.

M. Nathan Cullen: Vous remettez en question leur modèle d'affaires même. La collecte de données et la commercialisation de ces données, c'est en plein leur domaine, et c'est une activité très lucrative. Quels sont les chiffres que vous avez évoqués? Il était question d'un marché publicitaire de 150 milliards de dollars pour l'ensemble...

M. Jason Kint: Oui, pour l'ensemble des États-Unis et de l'Amérique du Nord, et 85 % de la croissance se retrouve dans les actifs de deux entreprises dont l'activité est la collecte de données.

M. Nathan Cullen: Cela se fonde sur la collecte de données.

M. Jason Kint: Oui. Pour en revenir à leur stratégie, l'une des choses les plus problématiques, c'est que M. Zuckerberg et Mme Sandberg affirment que c'est leur secteur d'activité et que dans ce secteur, c'est comme cela que les choses fonctionnent. S'ils ne font pas cela, il faudra que tout le monde paie pour le produit, ce qui représente 2,3 milliards de personnes à l'échelle mondiale, dont beaucoup sont dans des pays en développement.

Certaines mesures peuvent être prises dans l'intervalle pour les forcer à appliquer des normes plus rigoureuses, ce qui se traduira par une diminution modeste de leurs revenus.

M. Nathan Cullen: Parlons de ces normes plus rigoureuses.

Monsieur Carroll, je ne sais pas si vous pouvez commenter ou non. Je pense que le Comité a proposé que les partis politiques — qui recueillent aussi beaucoup de données — soient tenus de respecter les normes de protection des renseignements personnels auxquelles les entreprises privées doivent se conformer. Or, cette disposition n'est pas dans le nouveau projet de loi du gouvernement sur les élections. Le directeur général des élections a fait une sortie, hier, pour dire qu'il était très déçu que cela n'ait pas été inclus dans le projet de loi.

Croyez-vous que cela devrait être enchâssé dans les lois canadiennes?

M. David Carroll: Oui, je pense que c'est une mesure audacieuse, mais nécessaire. J'ai dit tout à l'heure que j'admirais l'audace de l'adoption de cette position.

Une chose que l'on a perdue de vue en cours de route, c'est que, selon la loi britannique, il était illégal de créer des profils politiques d'Américains. Il y a eu un grand débat afin d'établir si la psychométrie fonctionnait ou non, et s'il s'agissait d'un moyen d'échapper au profilage illégal dont fait état la loi britannique. À bien des égards, il semble que les directeurs de Cambridge Analytica/SCL ont mal compris la question de la juridiction. La question cardinale qu'il faut se poser est la suivante: pourquoi cette entreprise s'est-elle internationalisée? Pourquoi ces données sur les électeurs américains ont-elles été traitées dans un autre pays?

En ce qui concerne la protection des renseignements personnels, je pense que la première chose qu'il convient d'examiner, c'est la manière dont nous pouvons garder les données des électeurs à l'intérieur du pays où ces électeurs sont appelés à voter.

● (1635)

M. Nathan Cullen: Voulez-vous dire que les partis politiques devraient d'entrée de jeu être tenus de prévenir les piratages?

M. David Carroll: Oui. Déjà, comment un parti politique peut-il justifier l'embauche d'une compagnie étrangère pour travailler sur sa campagne? En quoi cela peut-il seulement être acceptable?

M. Nathan Cullen: Le gouvernement a accordé un contrat de 100 000 $ à Cambridge Analytica. Ce n'est pas beaucoup d'argent, mais nous ne savons pas quel était le but ou l'intention de ce contrat. Puis, le scandale a éclaté et nous ne savons toujours pas de quoi il retourne.

Nous recherchons les leçons très difficiles et douloureuses qui ont été apprises aux États-Unis, au Royaume-Uni, en France et en Allemagne. Nous sommes à l'aube de la prochaine élection. Parmi ces douloureuses leçons, quelle est celle que le Canada devrait faire sienne en priorité? Le cycle électoral est en cours. Nous commençons à penser en fonction du vote qui se tiendra en octobre. Quelle est, selon vous, la première chose qui doit être faite?

M. David Carroll: Compte tenu des infrastructures en place, comment les citoyens, la société civile, le milieu universitaire et le gouvernement lui-même peuvent-ils examiner à la loupe les campagnes et les fournisseurs? Pour inciter les parties concernées à se comporter de manière exemplaire, il faut leur donner l'impression que leurs activités sur le plan politique sont scrutées à la loupe. C'est ce que nous pouvons faire de mieux. Mais pour la suite des choses, il faudra absolument procéder à des changements en profondeur.

Le président: Merci, monsieur Cullen. Je suis convaincu qu'il nous restera du temps à la fin pour poser toutes les questions qui doivent être posées. C'est ce dont je présume, mais je sais que nous en avons beaucoup en réserve.

Le prochain intervenant est M. Baylis, pour sept minutes.

M. Frank Baylis (Pierrefonds—Dollard, Lib.): Merci, monsieur le président.

Avec ces mastodontes — Facebook et Google — deux choses se sont produites. Vous en avez mentionné une, monsieur Kint, et c'est le profit. Ces sociétés font des profits phénoménaux, mais elles engrangent ces recettes en se servant d'oeuvres dont elles n'ont pas les droits. Elles vont chercher un clip qu'elles savent que je vais aimer et elles me le montrent. Elles mettront une annonce à côté et garderont l'argent; le musicien n'aura rien. Elles pourraient aussi utiliser une superbe photo qu'aurait prise un photographe, photo qui, autrefois, aurait pu être vendue à des journaux ou à d'autres. Elles la prendront et la numériseront, et quelqu'un la cherchera. Ces entreprises s'en emparent et elles en tirent un profit.

Elles font cela aux journalistes, aux écrivains, aux musiciens, aux artistes de toutes les sortes... Je ne cherche pas le contenu qu'aurait produit Google. Je ne suis pas intéressé. Facebook ne produit aucun contenu.

Je veux d'abord et avant tout parler de l'argent, du but lucratif. Ces sociétés ont été protégées par ce que l'on appelle la « sphère de sécurité », ce qui signifie qu'elles peuvent dire: « Hé, vous vouliez voir ça? Je viens de vous le montrer. Je n'ai rien à me reprocher ici. » Or, ici au Canada, bon nombre de nos médias souffrent énormément. Ils ont aussi perdu tous leurs revenus publicitaires. Cela ne veut pas dire que les gens ne lisent pas leurs articles. Ils les lisent, mais ils les lisent au moyen d'un agrégat Google ou de quelque chose du genre et, encore une fois, c'est Google qui récolte les profits.

Avez-vous une idée de ce que le Canada peut faire pour régler ce problème? Et si ce n'est pas possible pour le Canada d'agir seul, devrions-nous collaborer avec nos alliés afin de faire cesser cette pratique consistant à profiter du travail de tous ces gens? C'est cette dynamique qui a créé ce pouvoir phénoménal.

M. Jason Kint: Oui. Votre rapport contient un certain nombre de recommandations qui sont des pistes de solutions pour commencer à s'attaquer à ce problème. Nous avons beaucoup parlé de la question des données: il faut limiter l'utilisation que ces sociétés font des données, parce que c'est ainsi que la valeur se crée. Dès que vous imposez des limites à ce chapitre, les recettes diminuent.

Il y a des développements très intéressants, en particulier en Europe, autour du droit d'auteur, et il semble qu'ils progressent à nouveau depuis hier. J'examinerais ce qui se fait là-bas. Ils sont déjà venus à bout d'une grande partie de la difficile conciliation entre le droit d'auteur et la protection de la liberté d'expression.

Oui, il y a des choses à faire à cet égard. Dans votre rapport, certains des témoignages fournis par Tristan Harris et quelques autres se penchaient sur les moyens de tenir ces sociétés responsables lorsque des recommandations sont formulées. Cela m'intéresse lorsque nous commençons à parler des liens vers le contenu, certes, mais aussi de l'utilisation qu'elles font de leur intelligence artificielle pour présenter des recommandations. Nous devons leur faire porter le chapeau. La vraie raison pour laquelle ces sociétés gagnent de l'argent, c'est qu'elles n'ont aucune responsabilité à l'égard de quoi que ce soit. Et pourtant, ce sont elles qui ramassent tout. Quand il y a un problème, ce n'est pas le leur: c'est celui d'Internet ou de la société.

● (1640)

M. Frank Baylis: Monsieur Vickery, avez-vous quelque chose à dire à ce sujet?

M. Chris Vickery: L'une des choses qui sont à l'origine de ce problème, c'est le concept de microciblage. Le fait d'avoir l'Internet, un index et des sources agrégés ainsi que tout ce qui est utile pour faire des recherches mérite qu'on s'y attarde. Nous avons toujours eu des annuaires téléphoniques et des choses de ce genre, mais ils étaient généralement les mêmes pour tout le monde. Quand je regarde *La Joconde*, je n'en ai pas une version personnalisée que je trouve plus attirante que celle qui pourrait plaire davantage à mon prochain. C'est une expérience humaine que de vivre ce que tout le monde vit.

C'est lorsque l'on fait entrer le microciblage dans l'équation, que l'on se rend compte de la valeur de ces données et de ce que l'on peut en tirer...

M. Frank Baylis: Vous parlez de la capacité qu'ont ces sociétés d'utiliser les données pour procéder à des ciblages très précis.

Permettez-moi de parler d'un autre aspect de la façon dont elles recueillent les données.

Dès que j'achète mon iPhone et que je consens aux conditions d'utilisation, j'accepte implicitement que l'on m'espionne. Or, je ne veux pas qu'Apple m'espionne pour l'année dernière, même si l'entreprise fait valoir que c'est nécessaire. Ce n'est pas vrai. C'est un mensonge; ce n'est pas nécessaire. On ne m'a jamais permis d'aller négocier mes conditions d'utilisation.

Serait-ce une bonne idée d'encadrer ce que ces sociétés peuvent et ne peuvent pas faire en matière de collecte de données? Cela ne veut pas dire que tout le monde observerait ces règles, mais pour des gens comme Google et Facebook, si les peines sont assez sévères, nous pourrions utiliser leurs conditions d'utilisation et dire: « Peu importe sur quoi vous mettez vos conditions d'utilisation, lorsque vous vous adressez à vos clients canadiens, voici ce que vous pouvez et ne pouvez pas faire par contrat. »

J'aimerais vous entendre tous les trois là-dessus. Nous pourrions commencer par vous, monsieur Carroll.

M. David Carroll: Il serait vraiment intéressant de créer des mesures incitatives pour amener l'industrie à délaisser les données personnelles au profit des données non personnelles.

M. Frank Baylis: Je parle de ce qui arriverait si le gouvernement fixait des règles obligatoires. Je me fiche de ce que vous faites: vous n'avez pas le droit de faire ceci, vous n'avez pas le droit de faire cela. Quoi que vous pensiez avoir le droit de faire... En ce moment, vous pouvez faire tout ce que vous voulez.

M. David Carroll: Certainement. La question est de savoir comment le gouvernement peut pousser l'industrie à abandonner les données personnelles et à se tourner vers une façon de capitaliser sur les données non personnelles. Il existe des moyens d'obtenir des résultats similaires sans utiliser de données personnelles.

En ce qui concerne la question du droit d'auteur, il n'y a pas eu beaucoup de discussions ou de remue-méninges sur la façon dont la fiscalité peut relancer les industries, qu'il s'agisse de taxer les données personnelles et d'exempter les données non personnelles, ou d'imposer l'utilisation pour financer les droits d'auteur et pour soutenir financièrement le journalisme. Il y a différents modèles qui pourraient être examinés pour régler ces problèmes dans leur ensemble, parce qu'il est difficile de parler du droit d'auteur sans parler aussi des données. Il est difficile de parler d'antitrust sans parler de données. Les liens qui unissent ces différents enjeux sont fort délicats.

M. Frank Baylis: Monsieur Kint, qu'en pensez-vous?

M. Jason Kint: J'essaierais d'éviter l'idée de demander au gouvernement d'imposer cela. En revanche, il y a des choses que nous pouvons apprendre du RGPD, le règlement général sur la protection des données dans l'Union européenne. Il s'agit probablement de la réglementation la plus discutée à l'heure actuelle en matière de données, et c'est probablement celle qui est la plus tournée vers l'avenir.

Il y a quelque chose que l'on appelle la limitation de finalité, qui dit essentiellement que si je vous donne mon consentement pour utiliser mes données à une certaine fin, vous ne pouvez pas les utiliser pour autre chose. Cela renvoie à une bonne partie de ce que j'ai dit dans mon exposé liminaire au sujet du contexte et des attentes des consommateurs.

Il s'agit d'utiliser les données de la manière dont l'utilisateur s'attend à ce qu'elles soient utilisées en fonction de la négociation ou de la relation initiale, puis de les limiter à cela. Par exemple, Google fait de l'argent en passant par Gmail pour faire un suivi de localisation, etc.

M. Frank Baylis: Ensuite, ils extraient mes données de mon téléphone. Ils suivent mes données en mon nom depuis l'année dernière. Je ne veux pas qu'ils le fassent. Ce n'est pas nécessaire, et je n'ai pas le pouvoir de négocier avec Apple afin de faire stopper ce suivi. Seul le gouvernement peut les empêcher de le faire.

M. Jason Kint: À ce que je sache, Apple n'utilise pas ces données pour ensuite vous envoyer des annonces microciblées ou pour s'en servir à toute autre fin.

M. Frank Baylis: Absolument.

Si vous allez à un restaurant, ils savent que vous y êtes allé. Ensuite, ils vous demandent comment était le restaurant. Ces données sont utilisées constamment.

● (1645)

M. Jason Kint: Cela se passe à l'intérieur de l'appareil. Nous pouvons nous enfoncer dans les méandres, mais c'est...

M. Frank Baylis: Les données sont vendues. Si je recherche des restaurants, par exemple, que j'envisage d'en visiter un en particulier et que je finis par le faire, je reçois par la suite une invitation à rédiger une critique du restaurant. Ils sont au courant en raison des données qu'Apple a vendues à quelqu'un. Ils combinent cela avec les résultats de mes recherches et le suivi de mes déplacements, ce qui leur permet de faire le lien. Par conséquent, ils le font assurément.

M. Jason Kint: D'une manière ou d'une autre, sans nous enfoncer dans les méandres de qui fait quoi, je pense qu'un relèvement de la barre s'impose assurément et qu'il faudrait en parler aux entreprises qui observent un nombre considérable de nos activités. Je les appelle les fournisseurs de services. Cela pourrait vouloir dire qu'ils ne peuvent pas utiliser les données dans ce but. C'est tout à fait la même chose que, lorsque vous entrez dans un magasin, disons Target, et qu'ils suivent vos données dans le cadre de l'expérience en magasin. C'est probablement acceptable, puisque vous pouvez choisir de ne plus jamais visiter un magasin Target, parce que vous n'aimez pas leur façon de faire les choses. Toutefois, si vous visitez un magasin Target et qu'ensuite, ils vous suivent à l'extérieur du magasin, partout où vous allez, nous faisons face au problème dont vous parlez, et c'est dans ce contexte que la barre doit être relevée.

Le président: Merci, monsieur Baylis.

Le prochain intervenant est M. Gourde, qui dispose de cinq minutes.

[*Français*]

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

Ma question s'adresse à tous les témoins.

Le monde numérique que nous connaissons présentement semble être le même au Canada, aux États-Unis et ailleurs. Dans ce monde numérique, la réalité a dépassé la fiction. Ce qu'on n'arrivait même pas envisager en 2015 est devenu une réalité. Il semble que les grandes compagnies comme Facebook, Google ou d'autres encore qui pourraient voir le jour dans l'avenir ne soient aucunement limitées pour ce qui est d'obtenir nos renseignements personnels, de les accumuler et de les stocker pour de nombreuses années.

Selon vous, des limites devraient-elles être imposées à ces compagnies quant à nos renseignements personnels et à la période pendant laquelle elles peuvent les conserver?

Monsieur Carroll, vous pouvez répondre en premier.

[*Traduction*]

M. David Carroll: Le RGPD de l'Union européenne et, dans une certaine mesure, la nouvelle Consumer Privacy Act de la Californie, qui entrera en vigueur en 2020, nous offrent des modèles pour fixer des limites. L'une des limites que vous proposez est celle qui concerne la conservation des données. L'un des aspects intéressants du RGPD, c'est la nécessité de divulguer la durée de conservation des données au moment de l'obtention du consentement. Lorsque vous vous abonnez à un service, ils doivent vous dire qu'ils conserveront vos données pendant six mois, et vous prenez connaissance de cette limite au moment où vous vous abonnez et vous donnez votre consentement.

J'estime que nous disposons maintenant de bons modèles que nous pouvons utiliser pour évaluer les limites et pour constater comment elles sont fixées. Les autres limites auxquelles mon collègue, M. Kint, a fait allusion — c'est-à-dire une utilisation limitée en fonction du contexte de la collecte des données et l'interdiction d'utiliser ces données d'un contexte à l'autre — seraient aussi des cadres qu'il serait important d'établir. L'élément-clé qui nous occupe est aussi l'observation de ces limites. Mon expérience de travail avec le Commissariat à l'information et le système judiciaire du Royaume-Uni montre que le respect de ces limites est là où le bât blesse.

M. Jason Kint: Je confirmerais ce dernier point.

J'ai vu que vous recommandiez de conférer plus de pouvoirs au commissaire à la protection de la vie privée. Cela revêt une grande importance. Je pense que les pouvoirs dont jouissait la commissaire à l'information du Royaume-Uni lui avaient été conférés à la dernière minute. Elle avait de la chance de les avoir, alors je recommanderais la même chose. Le RGPD a certainement un véritable mordant avec ses amendes correspondant à 4 % des revenus totaux de l'entreprise. Cela fait une différence, et nous commençons à observer certaines mesures d'application.

J'ai coché un grand nombre de vos recommandations. Bon nombre d'entre elles sont vraiment excellentes. Celles à côté desquelles j'ai mis des étoiles sont des recommandations extrêmement importantes, comme la modernisation de la Loi sur la concurrence et le fait de reconnaître vraiment que ces entreprises — avec lesquelles, comme M. Baylis l'a signalé, vous ne pouvez pas parvenir à négocier une entente équitable parce qu'elles jouissent de tellement de pouvoirs et de tellement de données que vous êtes forcé d'utiliser leurs services, étant donné aussi qu'il y a seulement deux systèmes d'exploitation, disons, ou seulement un moteur de recherche — devraient en fait être évaluées en fonction de leurs données, dans le cadre de l'estimation de leur valeur d'échange. Le fait que leurs services sont gratuits ne devrait pas leur permettre d'exercer un monopole.

● (1650)

[*Français*]

M. Jacques Gourde: Monsieur Vickery, la parole est à vous.

[*Traduction*]

M. Chris Vickery: J'aimerais soulever la notion selon laquelle les données ne disparaissent jamais vraiment. Les entreprises peuvent affirmer qu'elles les ont effacées ou dire ce qui leur chante, mais les données ont déjà été intégrées dans d'autres bases de données au moment de leur suppression. Elles font déjà partie de produits dérivés, et les entreprises ont probablement conservé des copies de sauvegarde de ces données.

Je me concentrerais davantage sur le fait que les données deviendront désuètes après un certain temps. Mettez donc en oeuvre de nouvelles règles, de nouveaux règlements ou de nouvelles lois afin de restreindre leurs capacités de recueillir des quantités superflues de données, et laissez les autres données devenir désuètes et inutiles en raison de leur âge. Ne vous préoccupez pas d'essayer de leur arracher ces données, car vous ne réussirez jamais.

[*Français*]

M. Jacques Gourde: Je vous remercie.

[*Traduction*]

Le président: Madame Fortier, vous disposez de cinq minutes.

[*Français*]

Mme Mona Fortier: Merci, monsieur le président.

Mesdames et messieurs, je veux revenir à l'étude que nous réalisons présentement. Dans le cadre de celle-ci, nous voulons déterminer quelles sont les conséquences de la numérisation des services gouvernementaux sur la protection des renseignements personnels. Nous nous sommes penchés entre autres sur le modèle estonien et avons entendu certains de vos commentaires à ce sujet.

Y a-t-il d'autres modèles ou d'autres initiatives réalisées ailleurs dans le monde que nous devrions regarder de près, à votre avis, pour les fins de notre étude?

Je vais d'abord poser la question à M. Carroll et faire ensuite le tour des autres témoins.

[*Traduction*]

M. David Carroll: L'un des aspects importants et valables du modèle estonien, c'est le principe de collecte unique. Le concept clé de cette identité nationale unifiée consiste à ne pas exiger que les citoyens saisissent sans cesse leurs données, et cela prévient le problème auquel les citoyens font face dans la plupart des pays, en fournissant constamment les mêmes renseignements à plusieurs entités différentes. Chaque fois qu'ils le font, un nouveau point faible est créé.

Il est parfaitement logique de vouloir comprendre comment concevoir le modèle qui permettrait de fournir les renseignements une seule fois et de les sécuriser à jamais, parce que cela contribuerait également à séparer l'identité des autres données. La création de mécanismes de dépersonnalisation et d'anonymisation, ainsi que leur intégration dans la structure, fonctionne bien.

Un autre système d'identité nationale, le modèle Aadhaar, a vu le jour en Inde. Je peux corroborer ce que M. Vickery a dit à son sujet. Certains de mes étudiants, qui mènent leurs propres recherches, ont découvert que ces systèmes étaient dangereusement faciles à pénétrer, du moins en Inde. L'utilisation d'un modèle numérique qui ne s'accompagne pas d'un système robuste de protection des données est une entreprise hasardeuse. À certains égards, il se pourrait que l'Estonie soit bien positionnée, parce qu'elle bénéficie d'un gouvernement numérique lié à une tradition de 20 ou 30 années de protection des données européennes.

Nous considérons aussi la Chine comme un extrême dans l'autre direction, où une industrie de la surveillance... La distinction entre le secteur privé et le gouvernement est complètement floue, et l'utilisation de la surveillance à des fins de coercition et de contrôle sociaux est très alarmante. Nous examinons effectivement les nouveaux modèles de protection de la vie privée et des données qui surgissent à l'échelle mondiale afin de déterminer les endroits qui se débrouillent bien dans ce domaine.

[*Français*]

Mme Mona Fortier: D'accord.

Monsieur Kint, la parole est à vous.

[*Traduction*]

M. Jason Kint: Je ne suis pas un expert en sécurité, alors je vais céder la majeure partie de mon temps à Chris. J'ai entendu des commentaires positifs à propos du modèle estonien, et je n'ai pas entendu parler de préoccupations en matière de sécurité à son sujet. La façon dont le modèle est décrit est logique, mais je n'ai pas entendu parler de problèmes liés à ce système. C'est l'exemple qui est le plus souvent cité de façon positive, et on commence à étudier le modèle. Il suffit peut-être de laisser passer du temps pour s'assurer que c'est le bon modèle, mais je vais laisser Chris intervenir à ce sujet.

[*Français*]

Mme Mona Fortier: Monsieur Vickery, vous avez la parole.

● (1655)

[*Traduction*]

M. Chris Vickery: Je pense que le mieux c'est de présumer en tout temps qu'une atteinte à la protection des données est survenue, de rendre le système si segmenté et résilient que, même si une atteinte à la sécurité est survenue, vous pouvez la trouver et y remédier rapidement de manière à ce que les dommages soient minimaux. Cependant, je ne crois pas que vous devriez mettre tous vos œufs dans le même panier. J'estime que la solution au problème lié au fait de demander aux gens de présenter les mêmes renseignements à plusieurs reprises consiste à minimiser la quantité de renseignements que vous devez obtenir d'eux. Par exemple, aux États-Unis, nous ne sommes pas censés, d'après le gouvernement, fournir constamment notre numéro de sécurité sociale. Et pourtant, tous les cabinets de médecins demandent ce numéro, alors qu'ils ne devraient pas le faire.

Il faut minimiser, optimiser et simplifier les données, mais je ne crois pas qu'il soit bon de mettre tous vos œufs dans le même panier.

Le président: Il vous reste une minute et 30 secondes.

[*Français*]

Mme Mona Fortier: Une autre particularité du Canada est qu'il compte plus d'un ordre de gouvernement, soit le fédéral, le provincial et le municipal. En revanche, on parle d'un modèle unique dans le cas de l'Estonie. Si vous avez des idées sur la manière dont nous pourrions composer avec le fait d'avoir trois ordres de gouvernement, faites-le-nous savoir. C'est une question que nous considérons dans notre étude. Je ne pense pas disposer d'assez de temps de parole pour vous laisser répondre à cette question.

[*Traduction*]

Le président: Le prochain intervenant est M. Kent, qui prendra la parole pendant cinq minutes.

L'hon. Peter Kent: J'aimerais revenir premièrement à M. Vickery. Les ministères canadiens — c'est-à-dire plusieurs d'entre eux ou un certain nombre d'entre eux — ont été piratés à plusieurs reprises au cours des 10 dernières années, notamment par des utilisateurs chinois qui étaient soit engagés à forfait par le gouvernement chinois, soit soupçonnés de servir les intérêts du gouvernement chinois.

En 2007, le gouvernement de l'Estonie a résisté à une énorme cyberattaque menée par la Russie. Je vais simplement citer le site Web estonien qui rassure les Estoniens à propos de la sécurité de leur site, en déclarant ce qui suit:

> Après avoir vécu les cyberattaques de 2007, l'Estonie a élaboré la technologie évolutive des chaînes de blocs pour assurer l'intégrité des données stockées... L'Estonie est devenue l'hôte du Centre d'excellence en cyberdéfense coopérative de l'OTAN et de l'agence européenne responsable des TI.

Cela dit — et leur système semble effectivement excellent —, croyez-vous que leur système est impénétrable pour ceux qui chercheraient à le pirater soit par l'intermédiaire d'organismes en général, soit par l'intermédiaire d'organismes gouvernementaux qui détiennent des données, soit par l'entremise de l'un de ses utilisateurs, l'un des propriétaires d'une carte d'identité et de la puce qu'elle contient?

M. Chris Vickery: Absolument pas. Je ne considérerais pas comme la pure vérité les assurances qu'ils donnent à cet égard sur leur propre site Web. S'ils citent un événement qui est survenu en 2007, cela date de 12 ans. Personne n'a essayé de pirater leur système depuis? Ne peuvent-ils pas trouver d'autres exemples? Du point de vue d'Internet, un événement qui s'est produit il y a 12 ans remonte pratiquement à la nuit des temps.

L'hon. Peter Kent: Cela dit, ils semblent convaincus qu'ils n'ont pas été piratés depuis. Ils reconnaissent l'attaque qui a eu lieu à l'époque et qui a été documentée et analysée...

M. Chris Vickery: Je vous garantis qu'ils ont été piratés depuis. Je vous le garantis. Ils ne l'admettent peut-être pas, et il se peut qu'ils n'en sachent rien, mais je peux vous garantir que cela est arrivé.

L'hon. Peter Kent: D'accord.

Messieurs Carroll et Kint, lorsque le RGPD est entré en vigueur en mai dernier, un nombre important d'agences ordinaires de nouvelles nord-américaines ont retiré à leurs abonnés européens l'accès à leurs sites Web par crainte que, dans leur forme actuelle, ils violent de façon importante certaines des nouvelles règles du RGPD. À votre connaissance — et je vous pose la question à tous les deux —, l'une ou l'autre de ces entreprises a-t-elle communiqué avec vous, par l'intermédiaire d'universitaires ou du marché, afin de vous demander des conseils ou des directives, ou afin de reconnaître ou de vous aviser qu'elle est en train de modifier certaines des activités de son site Web?

M. Jason Kint: Selon la presse, les sites qui ont retiré leur accès ne sont pas aussi nombreux que vous le pensez. Je pense que c'est un argument qu'aiment utiliser ceux qui ne sont pas favorables au RGPD, comme Google, en particulier. Tribune Publishing — qui s'appelait Tronc à l'époque —, qui possédait de nombreuses entreprises, a décidé de se retirer. Cela représentait de nombreux sites. Leur inquiétude était liée à l'amende correspondant à 4 % de tous leurs revenus... et leurs activités numériques et probablement le nombre de leurs utilisateurs en Europe n'étaient pas très importants, en tant que propriétaires de journaux locaux. Ils ont pris une décision qui était simplement un compromis entre les risques encourus et la valeur des revenus générés.

Le vrai problème, c'est que la mise en oeuvre du RGPD, en particulier, était inquiétante pour la plupart des maisons d'édition. Nous avons envoyé une lettre à Google, au nom de 5 000 maisons d'édition d'Amérique du Nord et d'Europe, parce que la société a attendu jusqu'à un mois avant la mise en oeuvre du règlement pour réagir. Ce processus a littéralement duré deux ans. Pendant longtemps, nous avons tenté de savoir quels étaient ses plans puis, un mois avant l'entrée en vigueur du RGPD, la société a décidé d'informer tout le monde de ses plans. Elle souhaitait vivement obliger les maisons d'édition à obtenir le consentement des utilisateurs. Chaque maison d'édition a donc été forcée d'obtenir le consentement de ses utilisateurs par l'entremise Google, puis d'assumer cette responsabilité. Nous avons envoyé une lettre à la commissaire de la concurrence de l'Union européenne, Mme Vestager, précisément à ce sujet. Cela a contraint un grand nombre de maisons d'édition à prendre des décisions de dernière minute.

● (1700)

L'hon. Peter Kent: Aucun changement n'a été apporté depuis?

M. Jason Kint: Non.

Les maisons d'édition que vous avez mentionnées et qui s'étaient retirées n'ont pas réintégré le marché, mais je crois qu'il est probable qu'elles le feront. Évidemment, lorsque la presse libre n'est pas accessible en raison d'une réglementation, c'est un mauvais dénouement.

L'hon. Peter Kent: Monsieur Carroll.

M. David Carroll: De bien des façons, j'ai eu l'occasion de discuter avec l'industrie et le marché avant la mise en oeuvre du RGPD. Par exemple, lorsqu'en 2015, Apple a permis le blocage des annonces par le système d'exploitation iOS, cela a provoqué de nombreuses discussions dans l'industrie de l'édition à propos des effets que cela aurait. J'ai noué le dialogue avec l'industrie à ce moment-là.

Ce que je trouve intéressant en repensant à ce débat, c'est qu'on se demandait si les annonces étaient agaçantes ou si elles étaient une source d'anxiété relative à la protection de la vie privée. Je tentais de faire valoir qu'elles étaient une source d'anxiété relative à la protection de la vie privée, mais les intervenants ne voulaient pas me croire.

Après Cambridge Analytica et le RGPD, il est possible démontrer que l'anxiété relative à la protection de la vie privée était l'un des éléments moteurs de l'enjeu du blocage des annonces. Alors, comment cela est-il lié aux interfaces de consentement du RGPD, qui expliquent l'industrie aux consommateurs afin qu'ils puissent comprendre comment la monétisation fonctionne? Selon moi, c'est l'idée que le RGPD était un genre d'occasion d'apprentissage pour les consommateurs et l'industrie, en ce sens qu'il indiquait la façon dont cette industrie fonctionne.

Le problème, c'est que la recherche démontre que plus les gens comprennent comment fonctionne la publicité numérique, moins elle leur plaît.

Le président: Merci, monsieur Kent.

Le prochain intervenant est Michel, qui dispose de cinq minutes.

M. Michel Picard (Montarville, Lib.): Merci.

J'aimerais revenir sur les services numériques, et je poserai mes questions en français.

[*Français*]

Lorsque j'achète une marchandise dans un magasin, je ne suis pas obligé de donner mon adresse courriel ou une autre information, même si cela confond énormément la personne à la caisse, qui se demande quoi faire sur sa machine. Je suis capable d'acheter quelque chose sans donner de l'information personnelle. Je ne devrais pas avoir à donner de l'information pour acheter de l'équipement sportif.

En revanche, sauf erreur, lorsque je fais affaire avec le gouvernement, je suis obligé de donner de l'information personnelle. On me donnera un numéro d'assurance sociale si je peux donner au moins mon nom et quelques références. C'est la même chose pour mon permis de conduire. À défaut de fournir des références, je ne peux pas obtenir de permis de conduire ni de numéro d'assurance sociale. Par conséquent, je ne peux pas trouver un travail légitime parce que l'employeur a besoin de mon numéro d'assurance sociale. Je suis obligé de donner de l'information personnelle au gouvernement.

Dans un désir d'offrir un service optimal et plus performant, le gouvernement ne peut faire autrement que de se tourner vers le numérique et le Web. Il doit concevoir des techniques, des moyens et des outils pour offrir un service plus performant. Je suis de l'école de pensée qu'il n'existe aucun système qui soit à 100 % sécuritaire, ne serait-ce qu'en raison du facteur humain ou de la possibilité d'un coup monté de l'intérieur, qui sont les pires menaces qu'on ne peut pas contrôler. Le gouvernement est donc condamné à concevoir un service qui sera vulnérable.

Jusqu'où peut-il aller? Jusqu'où doit-il aller? Doit-il considérer malgré tout qu'il est dans l'obligation d'offrir des services numériques?

[*Traduction*]

M. Jason Kint: J'ai entendu quelques thèmes dans votre question qui constituent d'importantes observations, à mon avis. L'une d'elles est que les règles qui régissent le contenu hors ligne, qu'elles soient ce qui est approprié ou qu'elles découlent simplement du droit actuel, ne se sont pas bien adaptées au contenu en ligne. Lorsque vous êtes en ligne, vos attentes devraient être les mêmes que lorsque vous achetez quelque chose dans un magasin, c'est-à-dire que vous devriez vous attendre à ce qu'on ne vous demande pas des renseignements qui ne sont pas indispensables — c'est la minimisation des données dont Chris a parlé.

Je pense que c'est important, et je m'arrêterai à ce point.

● (1705)

M. David Carroll: Je pense que la métaphore que M. Kint a employée pour souligner le fait que le monde en ligne doit correspondre aux attentes et aux pratiques du monde réel est très importante. Nous considérons cette métaphore de la protection de la vie privée chez soi comme une manière intéressante d'envisager la protection de la vie privée numérique. Quand on invite quelqu'un chez soi, on ne laisse peut-être pas cette personne entrer plus loin que le pas de la porte s'il s'agit d'un étranger. D'autres personnes pourraient aller jusque dans la cuisine, et d'autres encore pourront utiliser votre salle de bains. Laissez-vous n'importe qui fouiller dans votre table de chevet? Non. La protection de la vie privée s'échelonne sur un spectre, et je pense que ce spectre doit être éclairci en ce qui concerne les services gouvernementaux pour que lorsque les citoyens fournissent leurs justificatifs d'identité, ils comprennent de quoi il en retourne en dressant un parallèle avec la vie hors ligne.

Bien entendu, le gouvernement est différent du marché, et la validation de l'identité d'un citoyen diffère de la validation de l'identité d'un consommateur.

M. Michel Picard: Monsieur Vickery.

M. Chris Vickery: J'éviterais de faire trop de métaphores avec le monde réel pour aider les gens à comprendre le monde en ligne, car les bonnes métaphores sont rares. Le fait de comparer un site Web à une maison ne fonctionne pas du tout pour moi. Oui, il faudra offrir les services gouvernementaux en ligne et mettre en oeuvre le gouvernement numérique. C'est inévitable, à moins que l'on ne veuille être une société préhistorique, ce qui n'est certainement pas votre cas. Il faut donc établir des normes et des pratiques acceptables pour le monde en ligne, sans faire trop de métaphores avec le monde réel, car il n'y a pas tellement d'analogies qui fonctionnent au cas par cas.

M. Michel Picard: Merci.

Le président: Merci.

Avant que j'accorde la parole au dernier intervenant sur la liste, je vous avise que nous disposons d'une vingtaine de minutes. Si vous avez une question à poser, faites-le savoir à la présidence et nous inscrirons votre nom sur la liste. Nous utilisons ainsi tout le temps dont nous disposons.

Vous avez trois minutes, monsieur Johns.

M. Gord Johns (Courtenay—Alberni, NPD): Merci, monsieur le président.

Je vous remercie de témoigner aujourd'hui pour nous prodiguer vos conseils.

À mesure qu'une société devient de plus en plus numérisée, considérez-vous qu'il faudrait apporter des modifications à la Loi sur la protection de la vie privée ou à d'autres lois concernant les partis politiques pour protéger les renseignements personnels des Canadiens?

Je commencerai par vous, monsieur Kint.

M. Jason Kint: J'ai proposé de mettre des cases à cocher à côté de vos recommandations, et j'ai des points d'interrogation pour deux d'entre elles. À dire vrai, ce point en faisait partie. Celui qui porte sur la capacité de joindre certains utilisateurs est également pertinent. Les limites qu'impose la Loi sur la protection de la vie privée actuelle quant à l'utilisation de l'information dans les discours politiques constituent un point que j'aimerais mieux comprendre avant de donner une opinion ferme sur la question.

M. Gord Johns: Souhaitez-vous ajouter quelque chose, monsieur Carroll?

M. David Carroll: Certainement. Je pense que si j'ai tiré une leçon de mon analyse des données de Cambridge Analytica, c'est celle de la nécessité fondamentale du droit d'accès. Ce dernier doit être appliqué horizontalement à l'ensemble de la société civile, que ce soit sur le marché ou au sein du gouvernement.

Pour ce qui est du concept voulant que les citoyens ou les consommateurs devraient pouvoir réclamer leurs données à une entité et être certains de les obtenir, quels autres droits ajouteriez-vous à cela? Dans le cas d'un parti politique, si vous demandiez à un parti de vous fournir votre profil d'électeur, il devrait avoir l'obligation de vous le donner. Si le citoyen veut le contester ou l'effacer, c'est une demande raisonnable.

M. Gord Johns: D'accord.

Pour ce qui est du fossé numérique, comment pouvons-nous faire en sorte que les gens qui n'ont peut-être pas accès à Internet ou qui, comme moi, vivent dans des régions rurales où le service à large bande est lamentable bénéficient d'un accès égal aux services gouvernementaux? Avez-vous des commentaires à formuler à cet égard?

Monsieur Kint, peut-être pourriez-vous répondre en premier.

● (1710)

M. Jason Kint: L'égalité de l'accès a toujours été source de préoccupation, particulièrement pour nos nouveaux membres. La question a d'ailleurs fait l'objet d'une initiative importante, du moins aux États-Unis. La concurrence est extrêmement importante sur le plan de ce que nous appelons la distribution multinationale d'émissions vidéo, dans le domaine des télécommunications, où il faut notamment assurer la protection de l'Internet ouvert pour veiller à offrir l'accès et à effectuer des investissements, et ce, afin que le domaine soit subventionné pour que le plus de gens possible aient accès à Internet. Je pense que nous avons effectué bien des démarches à ce sujet au cours des trois ou quatre dernières années sur le plan de la politique aux États-Unis.

M. Gord Johns: Monsieur Carroll.

M. David Carroll: Je peux établir un lien avec l'État de New York, où je réside. Un important fournisseur de services de télécommunications était censé, aux termes des conditions de sa fusion, fournir les services à large bande dans les régions rurales de cet État, mais il ne l'a pas fait. L'État l'a alors menacé de l'évincer de son territoire s'il ne s'exécutait pas. Tout est une question d'exécution. Quand on accorde des privilèges à une entreprise, elle doit respecter les conditions qui lui sont imposées.

Le président: Merci. Nous avons trois interventions de cinq minutes sur la liste.

Nous commencerons par M. Saini, qui sera suivi par Mme Vandenbeld. M. Erskine-Smith clora la discussion.

Vous avez la parole, monsieur Saini.

M. Raj Saini: Monsieur Carroll, j'ai une brève question à vous poser.

Vous avez évoqué le passé. Je pensais que nous avions terminé l'étude sur Cambridge Analytica, mais vous avez suscité chez moi une question à laquelle je n'ai toujours pas reçu de réponse.

Facebook affirme que les données ont été effacées. Cambridge Analytica a indiqué qu'on lui avait demandé de les détruire et qu'elle avait obtempéré. Avons-nous la confirmation qu'elles ont bien été détruites?

M. David Carroll: Nous n'avons pas encore obtenu cette confirmation. L'information...

M. Raj Saini: Nous ne savons pas encore si les 50 millions de profils Facebook ont été effacés.

M. David Carroll: Non.

Sachez que la semaine dernière, la première d'un documentaire sur Netflix a eu lieu à l'occasion du festival du film de Sundance. Je pense que certains membres du Comité y figurent, car le comité britannique du monde numérique, de la culture, des médias et du sport y tient une place prépondérante. Un ancien employé figurant dans ce film présente des preuves montrant que des clients sont encore bombardés de données s'appuyant sur leur profit de Facebook, même si l'entreprise affirme les avoir effacées.

Nous voyons donc encore émerger des preuves montrant que l'entreprise n'a pas dit la vérité. Voilà pourquoi l'affaire n'est pas encore terminée.

M. Raj Saini: Si je soulève la question, c'est parce que, comme vous le savez, Cambridge Analytica a fermé ses bureaux de Londres. Ses entités constitutives ont été dissoutes, d'une manière ou d'une autre, puis recréées avec les mêmes acteurs, mais sous des noms différents. En fait, les 50 millions de profils existent toujours, et les entreprises peuvent non seulement encore y glaner de l'information, mais aussi en rajouter. Est-ce vrai?

M. David Carroll: Oui. J'ai observé des irrégularités dans les procédures d'insolvabilité. M. Vickery m'a également présenté des preuves judiciaires qui justifient vos inquiétudes.

M. Raj Saini: Me reste-t-il du temps?

Le président: Vous disposez de trois minutes.

M. Raj Saini: L'autre question que j'ai est la suivante. Nous avons beaucoup parlé des atteintes à la protection des données. Je voudrais réorienter la conversation, d'une certaine manière. Je pense que notre intention consistait jusqu'à présent à prévenir les atteintes à la protection des données, mais je doute qu'on soit jamais capable de le faire, peu importe l'entité concernée, qu'il s'agisse du gouvernement ou d'une entreprise privée. Ces dernières, malgré leur richesse immense, sont encore victimes d'atteintes.

Ne vaudrait-il pas mieux envisager la question différemment? Nous pouvons augmenter les sanctions imposées aux contrevenants. Je comprends qu'il s'agit parfois d'acteurs non étatiques qui échappent à notre sphère de compétences, mais de bien des manières, nous pouvons augmenter les sanctions et, surtout, peut-être diversifier l'information.

L'étude porte en partie sur le gouvernement numérique. En Estonie, les données ne sont pas conservées dans une seule base de données, mais dans plusieurs dépôts, le tout étant relié par X-Road. Ainsi, si on accède à une partie du système, on n'obtiendra pas toute l'information.

Est-ce là une manière différente d'envisager les choses? Nous devrons bien finir par adopter une solution, que ce soit cette année ou l'année suivante. La technologie ne peut être arrêtée. Nous ne pouvons pas empêcher les citoyens d'utiliser des services. Nous ne pouvons revenir au papier et aux crayons. Soit nous gérerons le problème, soit nous devrons comprendre comment nous pouvons limiter les dégâts quand un problème survient. Qu'en pensez-vous?

● (1715)

M. David Carroll: Selon moi, il importe d'assurer d'abord la transparence du système. Si on donne aux gens le droit d'accès et qu'ils exercent ce droit, cela lèvera le voile sur la boîte noire. J'entends par là qu'ils n'obtiendront pas seulement leurs données, mais aussi la teneur confidentielle des prédictions, dont Chris a parlé. La manière dont nos données sont entrées dans des modèles, puis appliquées à autre chose exige de la transparence.

À cet égard, la responsabilité relative à la collecte de données réduirait l'accumulation et la mise en commun de renseignements. Comme nous l'avons fait remarquer, le fait que deux entreprises aient amassé autant de profils leur confère un pouvoir excessif.

M. Raj Saini: J'ai une dernière question.

Le président: Il vous reste une minute.

M. Raj Saini: C'est un point que les gens ne comprennent pas entièrement, selon moi. Quand le gouvernement commence à recueillir des données, il fait concurrence aux entreprises privées qui s'adonnent à ces activités. Comment pouvons-nous faire en sorte que ces entreprises fassent partie de la solution au lieu d'empiéter sur leurs platebandes? Vous n'ignorez pas que la collecte de données est d'une importance cruciale. Quand le gouvernement commence à recueillir des données, qui peuvent parfois être des renseignements auxquels les entreprises privées n'ont pas accès, comme des dossiers médicaux privés, comment pouvons-nous veiller à ce que le secteur privé fasse partie de la solution au lieu de lui faire concurrence?

M. David Carroll: Les motivations d'une entreprise privée qui tente de tirer profit des données et celles d'une entité gouvernementale qui veut fournir des services sans chercher directement à les monétiser sont très différentes. Les gens paient leurs impôts et reçoivent des services au lieu de voir leurs données utilisées pour attirer leur attention à des fins mercantiles. Des questions d'ordre technique doivent être examinées, mais il est difficile de concilier des fins aussi différentes.

M. Raj Saini: On en arrivera à un point de connexion où le secteur privé devra révéler une partie des renseignements au gouvernement, car si les gens ont un compte bancaire ou d'autres renseignements financiers et que le gouvernement exige qu'ils préparent leur déclaration de revenus, il doit y avoir un moyen de faire un lien entre les secteurs public et privé.

M. David Carroll: Oui. C'est étrange aux États-Unis, où l'Internal Revenue Service connaît toutes les transactions et pourrait préparer notre déclaration de revenus pour nous; l'organisme n'en a tout simplement pas le droit. Je pense qu'il existe effectivement des façons de faire intéressantes à ce sujet.

Le président: Merci, monsieur Saini.

La parole est maintenant à Mme Vandenbeld.

Mme Anita Vandenbeld (Ottawa-Ouest—Nepean, Lib.): Je vous remercie de nous fournir des renseignements fort intéressants.

Je veux aborder la question de la propriété et du droit d'accès, en revenant sur le fait que le gouvernement a des motifs très différents de recueillir des données, car il veut fournir des services et non faire du profit. Si c'est une entreprise ou un parti politique qui est propriétaire des données et qu'un citoyen leur indique qu'il veut qu'ils les éliminent, on peut aisément voir pourquoi ils devraient les détruire. En ce qui concerne le casier judiciaire ou le dossier de l'Agence du revenu du Canada, le citoyen n'a manifestement pas le même droit de les faire détruire ou modifier, voire d'en consulter toutes les données. Il s'agit de situations très différentes sur le plan des données que recueille le gouvernement. Je voulais vous interroger à ce sujet.

Monsieur Vickery, c'est vous qui avez indiqué que la seule manière d'être propriétaire des données consiste à empêcher la communication entre les bases de données. Vous avez également parlé des transferts de données entre les diverses bases de données, pratique à laquelle le gouvernement s'adonne constamment; c'est du moins quelque chose qu'il serait proposé de faire si nous disposions d'un tel système.

Quelles devraient être les règles en matière de protection des renseignements personnels, de propriété, de consentement et de droit d'accès dans le contexte du gouvernement numérique?

Je commencerai par M. Carroll, puis j'entendrai M. Vickery s'il souhaite ajouter quelque chose.

M. David Carroll: Le droit d'accès doit certainement faire l'objet d'exemptions particulières au gouvernement, mais j'ajouterais une autre exemption qui s'impose afin de protéger le journalisme et les journalistes. Je pense que le Règlement général sur la protection des données s'applique dans une certaine mesure, mais le fait est que les journalistes doivent protéger leurs sources et qu'une personne s'opposant à un reportage peut révéler par inadvertance une source en effectuant une demande d'accès à ce sujet. Vous devez faire très attention en établissant ces privilèges et ces responsabilités, qui existent sous une forme quelconque dans le secteur privé et assurément dans le secteur public.

Je pense que vous pouvez certainement dire par défaut que la transparence est souhaitable. Vous devez donc déterminer dans quelles situations la transparence ne fonctionne pas au lieu de chercher des occasions d'assurer la transparence.

● (1720)

Mme Anita Vandenbeld: Des exemptions au lieu de...

M. David Carroll: Privilèges, oui.

Mme Anita Vandenbeld: Monsieur Vickery?

M. Chris Vickery: Je recommande dans l'avenir un modèle qui définit essentiellement les conditions de manières très strictes. Si des données sont accessibles sans l'autorisation de la personne concernée, cette dernière n'en est pas la gardienne, elle n'en est pas propriétaire et elle ne les contrôle pas. Si le gouvernement possède le casier judiciaire de quelqu'un, cette personne n'en est pas propriétaire; il s'agit d'un dossier conservé à son sujet. Cependant, si Walmart a son historique d'achat, on peut adopter des lois stipulant que cette personne doit autoriser l'entreprise à recueillir ces renseignements. Ce sont deux situations très différentes, et il faut faire savoir aux gens que le gouvernement conserve à leur sujet des données qu'ils ne possèdent et ne contrôlent pas. Ce n'est tout simplement pas possible.

Mme Anita Vandenbeld: Merci.

Le président: Nous entendrons enfin M. Erskine-Smith.

M. Nathaniel Erskine-Smith: Monsieur Carroll, vous avez beaucoup parlé du droit de savoir ou du droit d'accès. À titre de politicien, j'utiliserai ici des exemples qui peuvent être très éloignés du sujet. Au cours des élections, M. Zimmer veut peut-être savoir qui possède un fusil et je veux peut-être savoir qui possède un animal de compagnie; nous irons donc frapper aux portes pour tenter de cibler les gens. Je pense que le droit d'accès a une influence modératrice nécessaire, en ce sens que je suis moins susceptible de recueillir une montagne de renseignements si je sais que vous, à titre d'électeur, pourrez voir ce que je recueille à votre sujet. Je ne recueillerai probablement pas de renseignement sur votre divorce si la Loi sur le divorce a été convenablement modifiée afin de bien vous protéger. Si vous pouvez accéder à l'information, je ne vais pas recueillir des tonnes de données. Je pense que c'est un droit très important. À titre de politiciens, je pense que nous devrions tous respecter ce droit des citoyens.

Le droit de modifier l'information me semble logique également. C'est préférable pour moi et pour les électeurs.

Pour ce qui est du droit d'effacer des renseignements, j'ignore si vous avez porté attention à d'autres droits à ce sujet. Comme je suis candidat, je peux accéder à certains renseignements qu'Élections Canada me fournit, des renseignements que l'organisme ne fournit pas aux personnes qui ne se présentent pas aux élections. À mon avis, ces renseignements ne devraient pas être détruits.

Quant aux autres renseignements, jusqu'où devrait aller le droit à l'effacement? Si je sais que vous êtes fort préoccupé par le Pacte mondial pour les migrations et que je ne veux pas vraiment que vous alliez voter parce que je considère que c'est une position déraisonnable à adopter, devrais-je effacer cette information si vous me le demandez?

M. David Carroll: Je ne veux pas esquiver la question, mais ma réponse va aller dans le sens de la décision de la commissaire à l'information du Royaume-Uni dans le cadre de son enquête. Les données inférées sont considérées comme étant des données personnelles quand elles sont liées à une identité. C'est le principe de la création de prédictions au sujet de personnes, alors que vous liez ces prédictions à leur dossier d'électeur. Ce sont des données personnelles.

Je crois que c'est lié à votre question sur les campagnes qu'on mène pour essayer de prédire le comportement des électeurs éventuels, et que cela s'appuie sur des prédictions plutôt que sur des faits vérifiables et déterministes. C'est une limite qu'il faudrait négocier davantage. Par exemple, si je détiens un permis d'armes à feu, vous avez alors un fait vérifiable qui vous dit que je suis pour le droit aux armes à feu. Cependant, si vous vous fiez à ce que je dis sur les médias sociaux pour tirer des conclusions sur ce que je pense du droit aux armes à feu, c'est un seuil différent qu'il faut définir.

M. Nathaniel Erskine-Smith: Monsieur Kint, vous avez dit avoir deux interrogations concernant des recommandations de notre rapport. Quelle est l'autre?

M. Jason Kint: Je savais que cela se produirait. C'était au sujet de la modération du contenu. C'était l'idée voulant qu'il soit possible, à l'intérieur d'une période donnée — vous avez suggéré 24 heures, je crois —, d'éliminer du contenu. Je sais qu'on est à mettre cela en œuvre dans quelques pays d'Europe. Je crois qu'il serait sage de surveiller et d'étudier ce qui se passe.

M. Nathaniel Erskine-Smith: Pour ce qui est de la première recommandation, vous avez un point d'interrogation concernant la nécessité de tenir compte des obligations de mener des activités d'information et de sensibilisation démocratique, ce qui, je l'espère, répond à vos préoccupations.

M. Jason Kint: Oui.

M. Nathaniel Erskine-Smith: Puisque vous aimez lire des études parlementaires canadiennes…

Des voix: Oh, oh!

… je préciserais qu'avant de nous pencher sur le scandale de Cambridge Analytica, nous avons publié un rapport sur notre loi visant la protection de la vie privée, la LPRPDE. Une de nos recommandations visait l'enjeu de l'adhésion pour les utilisations à des fins secondaires. Notre recommandation était d'exiger l'adhésion explicite pour les utilisations à des fins secondaires, ce qui devrait, je crois, répondre à bon nombre des préoccupations que vous avez soulevées.

● (1725)

M. Jason Kint: Tout à fait.

M. Nathaniel Erskine-Smith: Quant aux études que le Comité pourrait mener à l'avenir, quelques témoins ont suggéré les questions relatives à l'antitrust, et l'idée d'une IA éthique. Je vais terminer sur une chose dont M. Baylis a parlé et qui a un certain lien avec les deux. Quand je mets une vidéo de musique par exemple sur Facebook, et que Facebook est en mesure de la rentabiliser — en la faisant passer sur des fils de nouvelles dont elle est maintenant l'éditeur —, il me semble que les règles d'exonération ne devraient pas s'appliquer de la même manière.

Je ne sais pas si vous avez une opinion à ce sujet.

M. Jason Kint: J'en ai une. Je pense que c'est un élément intéressant des recommandations. Je crois que c'était dans le témoignage de Tristan Harris.

L'exonération de responsabilité est très utilisée, y compris aux États-Unis. Les médias ont beaucoup parlé récemment des préjudices, dans le cadre des recommandations — pour YouTube et l'IA, dont l'objectif est manifestement le profit, et c'est conçu par des humains. C'est un problème.

M. Nathaniel Erskine-Smith: Je pense bien que le principe, étant donné que les algorithmes remplacent les éditeurs, c'est que nous devons de la même façon tenir responsables ceux qui utilisent les algorithmes pour faire des profits.

M. Jason Kint: Il y a là aussi le principe de la vérification des algorithmes, ce que je trouve très sage d'envisager.

M. Nathaniel Erskine-Smith: Merci beaucoup.

Le président: En tant que président, je vais poser une seule question.

Sans vouloir simplifier les choses à l'excès, j'y vois une solution assez simple. La commissaire à l'information du Royaume-Uni nous a aussi parlé de pénalités. C'est quelque chose qu'il nous faut aussi pour restreindre la collecte de données, et il faut comprendre qu'il y a de nombreux niveaux aux données et qu'il n'est pas simplement question de données en général.

Nous vous donnons la parole. Nous vous écoutons très attentivement. Ce que je vais vous demander à tous les trois est simple. S'il y a une seule chose que vous voulez que nous retenions, quelle est cette chose? Qu'est-ce que vous voulez que nous retenions en particulier concernant notre discussion d'aujourd'hui sur la collecte de données et les services gouvernementaux en particulier, ou en général?

Commençons par M. Vickery.

M. Chris Vickery: Je vous laisserais sur de très sombres perspectives à ce sujet. Il faut que les choses changent radicalement.

En ce moment, la situation est 10 fois pire que vous le pensez, et il faut agir. Il faut parler moins et agir plus.

Le président: Nous avons du temps pour cela, mais qu'entendez-vous quand vous dites que la situation est 10 fois pire que nous le pensons? Pouvez-vous nous expliquer cela un peu?

M. Chris Vickery: Tout le monde est lassé par les atteintes à la protection des renseignements personnels, avec tout ce qu'on voit aux nouvelles. Le nombre d'atteintes à la protection des renseignements personnels qui sont mentionnées dans les articles représente une proportion infinitésimale. Le nombre réel d'atteintes à la protection des renseignements personnels et la quantité de données qui circulent, c'est 10 fois, 100 fois plus que ce que vous pouvez vous imaginer, si vous voulez compter les employés qui diffusent trop d'information ou qui envoient de l'information à leur courriel personnel, entre autres, dans le cadre des activités normales. En ce moment, la situation est horrifiante.

Le président: Merci, monsieur Vickery.

Ce sera M. Carroll, puis M. Kint.

M. David Carroll: Les États-Unis, le Canada et d'autres pays doivent adopter une version du RGPD — une adaptation de ce que ce modèle comporte. La California Act fait avancer les choses aux États-Unis, et ce sera une course effrénée d'ici à ce que la California Act prenne effet, en vue de l'adoption d'une quelconque loi nationale visant la protection des renseignements personnels et ayant priorité sur les lois des États.

Il s'agit vraiment d'un moment clé: les États-Unis et le Canada pourraient se faire des chefs de file et, d'une certaine façon, rattraper les 20 années de retard dans la protection des données par rapport à nos amis de l'autre côté de l'Atlantique.

Le président: Monsieur Kint.

M. Jason Kint: Je suis tout à fait d'accord pour dire que le modèle du RGPD est important. Cependant, en plus de cela, je mettrais vraiment en évidence ce qui se trouve dans les recommandations 12 et 13 concernant la Loi sur la concurrence et l'intersection avec les données et la valeur des données. Cela résout bien des choses: les problèmes de responsabilité, notamment, et la question de la responsabilisation des gros joueurs.

Si vous prenez cela comme point de départ, vous avez votre point d'intersection avec ce que je considère comme étant vraiment le problème fondamental: la collecte de données pour faire de l'argent d'une manière qui dépasse nettement les attentes des consommateurs. À cela vous ajoutez l'application de la loi.

La semaine passée, j'étais à une importante conférence sur la protection de la vie privée, à Bruxelles. Je faisais partie du groupe d'experts de la commissaire Denham, et nous avons beaucoup discuté du consentement et des données. Aux 300 personnes présentes, j'ai demandé à celles qui utilisent un produit Google de lever la main. Tout le monde a levé la main. Puis je leur ai demandé de lever la main si elles trouvaient correct que Google suive et collecte des données sur tout ce qu'elles faisaient. Naturellement, personne n'a levé la main.

J'ai ensuite regardé la commissaire Denham, et j'ai dit: « Vous avez un problème d'application, car 90 % des personnes présentes ont consenti à quelque chose qu'elles ne veulent pas vraiment. »

Nous devons résoudre ce problème, et vous avez l'occasion d'être à l'avant-garde de la communauté internationale, ici, en misant sur ce que l'Europe a accompli.

● (1730)

Le président: Je vais terminer en vous remerciant tous d'avoir comparu aujourd'hui. Je sais que certains d'entre vous ont parcouru une grande distance pour être ici et je vous en remercie. Vos témoignages sont précieux. Encore une fois, merci d'avoir témoigné et d'être venus au Canada.

M. Jason Kint: Je suis honoré d'être ici. Je vous remercie.

M. David Carroll: C'est en effet un honneur d'être ici. Merci de nous avoir accueillis.

Le président: La séance est levée.