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 155 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mercredi 29 mai 2019

Président

M. Bob Zimmer

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

Le mercredi 29 mai 2019

● (0835)

[*Traduction*]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): La 155e séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique est ouverte.

Il s'agit de la dernière de nos grandes réunions internationales cette semaine, celle du Grand Comité international sur les mégadonnées, la protection des renseignements personnels et la démocratie.

Nous accueillons aujourd'hui, de chez Amazon, Mark Ryland, directeur de l'ingénierie de sécurité, au Bureau du dirigeant principal de la sécurité de l'information pour Amazon Web Services.

Marlene Floyd, directrice nationale des Affaires commerciales, et John Weigelt, agent national de technologie, représentent Microsoft Canada inc.

De la Mozilla Foundation, nous recevons Alan Davidson, vice-président, Politique mondiale, confiance et sécurité.

Enfin, de chez Apple Inc., nous accueillons Erik Neuenschwander, gestionnaire pour la vie privée des utilisateurs.

Nous allons passer aux témoignages. Je tiens à signaler que nous avons invité les PDG. Il est regrettable qu'ils ne se soient pas présentés. Comme je l'ai dit à nombre d'entre vous avant la séance, il doit s'agir ici d'une réunion constructive pour chercher les moyens d'apporter des améliorations. Certaines propositions que vos sociétés ont faites d'emblée sont bonnes, et c'est pourquoi nous souhaitions accueillir les PDG, qui auraient pu répondre à nos questions. Nous sommes néanmoins heureux que vous soyez parmi nous.

Nous entendrons d'abord M. Ryland, qui aura 10 minutes.

M. Mark Ryland (directeur, Ingénierie de sécurité, Bureau du dirigeant principal de la sécurité de l'information pour Amazon Web Services, Amazon.com): Merci beaucoup.

Bonjour, monsieur le président Zimmer, et mesdames et messieurs les membres du Comité. Je salue également les invités venus de l'étranger.

Je m'appelle Mark Ryland, et je suis directeur de l'ingénierie de sécurité au Bureau du dirigeant principal de la sécurité de l'information pour Amazon Web Services, la division de l'infonuagique chez Amazon.

Merci de m'avoir invité à m'entretenir avec vous. C'est un plaisir de me joindre à cette importante discussion. Je chercherai surtout à expliquer comment Amazon place la sécurité et la confiance des consommateurs au centre de toutes ses activités.

La mission d'Amazon est d'être l'entreprise la plus axée sur la clientèle au monde. Sa philosophie d'entreprise est profondément ancrée dans une démarche qui consiste à faire le cheminement inverse, à partir des besoins du client, et à innover constamment pour lui offrir ensuite un meilleur service, un choix plus vaste et des prix plus bas. Cette approche s'applique à tous ses secteurs d'activité, y compris ceux qui concernent la protection des renseignements des consommateurs et la cybersécurité.

Amazon est au service des clients canadiens depuis le lancement d'amazon.ca, en 2002. L'entreprise compte plus de 10 000 employés à temps plein au Canada et elle a annoncé en 2018 qu'elle comptait créer 6 300 emplois de plus.

Amazon a également deux carrefours technologiques, l'un à Toronto et l'autre à Vancouver. Ces regroupements de bureaux emploient plus d'un millier d'ingénieurs en logiciels et un certain nombre de techniciens de soutien. Ils élaborent certains de nos systèmes mondiaux les plus avancés. Il y a également des bureaux à Victoria pour www.abebooks.com et la filiale AWS Thinkbox, à Winnipeg.

L'entreprise exploite sept centres de traitement au Canada, et quatre autres ont été annoncés. Ils ouvriront tous leurs portes cette année, en 2019.

Un mot maintenant au sujet de notre plateforme infonuagique.

Il y a un peu plus de 13 ans, Amazon a lancé Amazon Web Services, son entreprise d'infonuagique. C'est à Montréal que se trouve le siège d'AWS au Canada, où AWS compte un certain nombre de centres de données distincts. Nous avons lancé AWS parce qu'après plus d'une décennie passée à construire et à exploiter Amazon.com, nous nous sommes aperçus que nous avions acquis une compétence fondamentale dans l'exploitation d'une infrastructure technologique et de centres de données à très grande échelle. Nous nous sommes engagés dans une mission plus vaste, celle de servir les développeurs et les entreprises en leur offrant des services de technologie de l'information qu'ils peuvent utiliser pour gérer leurs propres entreprises.

Le terme « infonuagique » désigne la prestation sur demande de ressources de TI sur Internet ou sur des réseaux privés. Le nuage d'AWS s'étend sur un réseau de centres de données répartis dans 21 régions géographiques dans le monde entier. Au lieu de posséder et d'entretenir leurs propres centres de données, nos clients peuvent acquérir des technologies telles que la puissance de calcul, le stockage et les bases de données en quelques secondes, au gré des besoins, en appelant simplement une API ou en cliquant sur une console graphique.

Nous fournissons l'infrastructure et les services de TI de la même façon que le consommateur qui appuie sur l'interrupteur d'une lampe chez lui reçoit l'électricité d'un fournisseur.

L'une des préoccupations du Comité est la démocratie. Eh bien, nous démocratisons vraiment l'accès à des services de TI que seulement de très grandes organisations pouvaient s'offrir auparavant, vu l'importance du dispositif nécessaire. Maintenant, les plus petites organisations peuvent avoir accès à ce même type de technologie de pointe très perfectionnée en cliquant simplement sur un bouton et en payant uniquement leur consommation.

Aujourd'hui, AWS fournit des services informatiques à des millions de clients actifs dans plus de 190 pays. Les entreprises qui se prévalent des services d'AWS vont de grandes entreprises canadiennes comme Porter Airlines, Shaw, la Banque Nationale du Canada, TMX Group, Corus, Capital One et Blackberry jusqu'à de jeunes entreprises novatrices comme Vidyard et Sequence Bio.

Je tiens à souligner que la protection de la vie privée commence au fond par la sécurité. Il n'est possible de se conformer aux règlements et aux attentes en matière de protection des renseignements personnels que si la confidentialité des données est prise en compte dès la conception même des systèmes. Chez AWS, nous disons que la sécurité est la fonction primordiale: elle est encore plus importante que la toute première priorité. Nous savons que, si la sécurité n'est pas assurée, notre entreprise ne peut pas exister.

AWS et Amazon veillent jalousement à la sécurité et à la protection des renseignements des consommateurs et ont mis en œuvre des mesures techniques et physiques perfectionnées pour bloquer tout accès non autorisé aux données.

La sécurité est la responsabilité de tous. Bien que nous ayons une équipe d'experts en sécurité de calibre mondial qui surveille nos systèmes 24 heures sur 24 et 7 jours sur 7, afin de protéger les données des clients, chaque employé d'AWS, peu importe son rôle, est responsable de veiller à ce que la sécurité fasse partie intégrante de toutes les facettes de notre entreprise.

La sécurité et la protection des renseignements personnels sont une responsabilité partagée d'AWS et du client. Cela signifie qu'AWS est responsable de la sécurité et de la protection des renseignements personnels dans le nuage même, et que les clients sont responsables de la sécurité et de la confidentialité dans leurs systèmes et leurs applications qui fonctionnent dans le nuage. Par exemple, les clients doivent tenir compte de la sensibilité de leurs données et décider s'il faut les crypter et comment. Nous offrons une grande variété d'outils de cryptage et des conseils pour aider les clients à atteindre leurs objectifs en matière de cybersécurité.

Nous disons parfois: « Dansez comme si personne ne vous regardait. Cryptez comme si tout le monde était aux aguets. » Le cryptage est également utile pour garantir la confidentialité des données. Dans de nombreux cas, les données peuvent être effacées de façon efficace et permanente simplement en supprimant les clés de cryptage.

● (0840)

De plus en plus, les organisations prennent conscience du lien entre la modernisation de la TI offerte par le nuage et une meilleure posture en matière de sécurité. La sécurité dépend de la capacité de garder une longueur d'avance dans un contexte de menaces qui évolue rapidement et continuellement, ce qui exige à la fois agilité opérationnelle et technologies de pointe.

Le nuage offre de nombreuses caractéristiques avancées qui garantissent que les données sont stockées et manipulées en toute sécurité. Dans un environnement classique, sur place, les organisations consacrent beaucoup de temps et d'argent à la gestion de leurs propres centres de données et se préoccupent de se défendre contre une gamme complète de menaces très variables et en constante évolution qu'il est difficile de prévoir. AWS met en œuvre des mesures de protection de base, comme la protection contre les DDoS ou la protection contre les dénis de service distribués; l'authentification, le contrôle d'accès et le cryptage. À partir de là, la plupart des organisations complètent ces protections en ajoutant leurs propres mesures de sécurité pour renforcer la protection des données de l'infonuagique et resserrer l'accès à l'information délicate dans le nuage. Elles disposent également de nombreux outils pour atteindre leurs objectifs en matière de protection des données.

Comme la notion de « nuage » est une nouveauté pour bien des gens, je tiens à souligner que les clients d'AWS sont les propriétaires de leurs propres données. Ils choisissent l'emplacement géographique où ils entreposent leurs données dans nos centres hautement sécurisés. Leurs données ne bougent pas à moins qu'ils ne décident de les déplacer. Nous n'accédons pas aux données de nos clients et nous ne les utilisons pas sans leur consentement.

La technologie est un élément important de la vie moderne et elle a le potentiel d'offrir des avantages extraordinaires dont nous commençons à peine à prendre conscience. Les solutions basées sur les données offrent des possibilités illimitées d'améliorer la vie des gens, qu'il s'agisse de poser des diagnostics médicaux beaucoup plus rapides ou de rendre l'agriculture beaucoup plus efficace et durable. Face à de nouveaux enjeux liés à la technologie, il se peut qu'il faille de nouvelles approches réglementaires, mais elles devraient éviter de nuire aux incitatifs à l'innovation et de limiter les gains d'efficience importants comme les économies d'échelle et la portée des technologies.

Nous croyons que les décideurs et les entreprises comme Amazon ont des objectifs très semblables: protéger la confiance des consommateurs et les renseignements personnels et promouvoir les nouvelles technologies. Nous partageons l'objectif de trouver des solutions communes, surtout en période d'innovation rapide. À mesure que la technologie évoluera, nous aurons tous la possibilité de travailler ensemble.

Merci. Je me ferai un plaisir de répondre à vos questions.

Le président: Merci, monsieur Ryland.

Nous passons maintenant à Microsoft. Entendrons-nous Mme Floyd ou M. Weigelt?

Mme Marlene Floyd (directeur national, Affaires commerciales, Microsoft Canada inc.): Nous allons nous partager le temps de parole.

Le président: D'accord. À vous.

[*Français*]

M. John Weigelt (agent national de technologie, Microsoft Canada inc.): Merci, monsieur le président.

Nous sommes heureux d'être ici avec vous aujourd'hui.

[*Traduction*]

Je m'appelle John Weigelt. Je suis l'agent national de technologie pour Microsoft au Canada. Ma collègue, Marlene Floyd, directrice nationale des affaires commerciales chez Microsoft Canada, m'accompagne. Nous sommes heureux d'avoir l'occasion de comparaître devant le Comité. Le travail que vous avez entrepris est important, compte tenu de la place de plus en plus grande du numérique et de l'incidence de la technologie sur les emplois, la protection des renseignements personnels, la sécurité, la participation de tous et l'équité.

Depuis la création de Microsoft Canada, en 1985, notre présence ici s'affirme de plus en plus, au point que nous avons désormais 10 bureaux régionaux aux quatre coins du pays, et ils emploient plus de 2 300 personnes. Au centre de développement de Microsoft à Vancouver, plus de 700 employés mettent au point des produits qui sont utilisés dans le monde entier. Des recherches de pointe sur l'intelligence artificielle sont également menées par des docteurs et des ingénieurs au laboratoire de recherche de Microsoft à Montréal. Ils travaillent en partenariat avec les universités de cette ville.

Des technologies puissantes comme l'infonuagique et l'intelligence artificielle transforment notre façon de vivre et de travailler et apportent des solutions à certains des problèmes les plus urgents du monde. Chez Microsoft, nous considérons avec optimisme les avantages de ces technologies, mais nous sommes aussi lucides devant les défis qui exigent une réflexion qui va au-delà de la technologie pour garantir l'application de principes éthiques forts et de lois adaptées. Quel rôle la technologie devrait-elle jouer dans la société? Pour répondre, il faut que des représentants de l'État, du milieu universitaire, du monde des affaires et de la société civile conjuguent leurs efforts pour modeler l'avenir.

Il y a plus de 17 ans, lorsqu'il a affirmé que « l'informatique fiable » était au premier rang des priorités chez Microsoft, Bill Gates a changé radicalement la façon dont cette société offre des solutions sur le marché. Cet engagement a été réitéré par l'actuelle PDG, Satya Nadella, en 2016. Nous croyons que la vie privée est un droit fondamental. Notre approche à l'égard de la protection de la vie privée et des données personnelles repose sur notre conviction que les clients sont propriétaires de leurs propres données. Par conséquent, nous protégeons la vie privée de nos clients et leur donnons le contrôle de leurs données.

Nous avons préconisé l'adoption de nouvelles lois sur la protection de la vie privée dans un certain nombre de pays, et nous avons été parmi les premiers à appuyer le RGPD en Europe. Nous reconnaissons que, pour les gouvernements, il est très important d'avoir une capacité informatique située près de leurs administrés. Microsoft a des centres de données dans plus de régions que tout autre fournisseur de services infonuagiques, avec plus d'une centaine de centres de données répartis dans plus de 50 régions du monde. Nous sommes très fiers que deux de ces centres de données soient situés ici, au Canada, soit en Ontario et au Québec.

La protection de nos clients et de la collectivité en général contre les cybermenaces est une responsabilité que nous prenons très au sérieux. Microsoft continue d'investir plus de 1 milliard de dollars par année dans la recherche et le développement en matière de sécurité, et des milliers de professionnels de la sécurité mondiale travaillent avec notre centre de renseignement sur les menaces, notre unité de la criminalité numérique et notre centre des opérations de cyberdéfense. Nous entretenons une étroite collaboration avec le Centre canadien pour la cybersécurité annoncé récemment par le gouvernement du Canada. Nous avons établi des partenariats avec des gouvernements du monde entier dans le cadre du Government Security Program, cherchant à échanger de l'information technique et des renseignements sur les menaces et même à coopérer pour démanteler des réseaux de zombies. En outre, Microsoft a pris la tête du Cybersecurity Tech Accord, signé par plus d'une centaine d'organisations mondiales qui se sont rassemblées pour défendre tous les clients de partout contre les cyberattaques malveillantes et rendre Internet plus sûr.

● (0845)

Mme Marlene Floyd: Microsoft a également été fière de signer l'Appel de Paris pour la confiance et la sécurité dans le cyberespace lancé en novembre par le président français, Emmanuel Macron, lors du Forum de Paris sur la paix. Avec plus de 500 signataires, il s'agit du plus important engagement multipartite à l'égard des principes de protection du cyberespace.

Le Comité a également mis l'accent sur l'ingérence croissante d'acteurs malveillants dans les processus démocratiques de nombreux pays. Nous sommes tout à fait d'accord pour dire que le secteur de la technologie doit faire davantage pour aider à protéger le processus démocratique. Plus tôt cette semaine, nous avons eu le plaisir d'appuyer la Déclaration du Canada sur l'intégrité électorale en ligne annoncée par la ministre Gould.

Microsoft a pris des mesures pour aider à protéger l'intégrité de nos processus et institutions démocratiques. Il a créé le Programme de défense de la démocratie, qui travaille avec les intervenants des pays démocratiques pour promouvoir l'intégrité des élections, la sécurité des campagnes électorales et la défense contre la désinformation.

Dans le cadre de ce programme, Microsoft offre sans frais un service de sécurité appelé AccountGuard aux clients d'Office 365 dans l'écosystème politique. Il est actuellement proposé dans 26 pays, dont le Canada, les États-Unis, le Royaume-Uni, l'Inde, l'Irlande et la plupart des autres pays de l'Union européenne. Il protège actuellement plus de 36 000 comptes de courriel. AccountGuard identifie les cybermenaces, y compris les attaques d'États-nations, et met en garde les particuliers et les organisations. Depuis le lancement du programme, des centaines d'avis de menaces ont été envoyés aux participants.

Nous avons également utilisé la technologie pour assurer la résilience du processus électoral. Plus tôt ce mois-ci, nous avons annoncé ElectionGuard, une trousse de développement de logiciels libres et gratuits visant à rendre le vote plus sûr en fournissant une vérification de bout en bout des élections, en ouvrant les résultats à des organismes tiers pour permettre une validation sécurisée, et en donnant à chaque électeur la possibilité de confirmer que son vote a été compté correctement.

Chez Microsoft, nous travaillons fort pour nous assurer de développer les technologies de manière qu'elles soient centrées sur l'être humain et qu'elles permettent un accès large et équitable pour tous. L'évolution rapide de la puissance informatique et la croissance des solutions d'IA nous aideront à être plus productifs dans presque tous les domaines de l'activité humaine et conduiront à une plus grande prospérité, mais il faut relever les défis avec un sens de la responsabilité commune. Dans certains cas, cela signifie qu'il faut avancer plus lentement dans le déploiement d'une gamme complète de solutions d'IA tout en travaillant de façon réfléchie et délibérée avec les responsables gouvernementaux, le milieu universitaire et la société civile.

Nous savons que nous devons en faire plus pour continuer à gagner la confiance, et nous comprenons que nous serons jugés à nos actes, et pas seulement d'après nos paroles. Microsoft est déterminée à continuer de travailler dans le cadre d'un partenariat délibéré et réfléchi avec le gouvernement au fur et à mesure que nous progressons dans le monde du numérique.

Merci. Ce sera un plaisir de répondre à vos questions.

Le président: Merci, madame Floyd.

Nous passons maintenant à M. Davidson, de Mozilla.

M. Alan Davidson (vice-président, Politique mondiale, confiance et sécurité, Mozilla Corporation): Mesdames et messieurs les membres du Grand Comité et du Comité permanent, merci.

Si je témoigne aujourd'hui, c'est parce que tout ne va pas bien dans le monde d'Internet. Il est certain que l'Internet ouvert est le moyen de communication le plus puissant que nous ayons jamais connu. À son mieux, il fait apparaître de nouvelles occasions d'apprendre à résoudre de grands problèmes pour bâtir un sens commun de l'humanité, et pourtant, nous avons aussi vu le pouvoir d'Internet utilisé pour miner la confiance, accentuer les dissensions et violer la vie privée. Nous pouvons faire mieux, et je suis ici pour vous faire part de quelques idées sur la façon de s'y prendre.

Je m'appelle Alan Davidson. Je suis vice-président chargé de la politique, de la confiance et de la sécurité à la Mozilla Corporation. Mozilla est une entité assez inhabituelle sur Internet. Nous appartenons entièrement à un organisme sans but lucratif, la Mozilla Foundation. Nous sommes une entreprise de logiciels libres axée sur une mission. Nous produisons le navigateur Web Firefox, Pocket et d'autres services.

Chez Mozilla, nous sommes déterminés à rendre Internet plus sain. Depuis des années, nous nous faisons les champions de l'ouverture et de la protection de la vie privée en ligne. Ce n'est pas qu'un slogan; c'est notre principale raison d'être. Nous essayons de montrer par l'exemple comment créer des produits pour protéger les renseignements personnels. Nous fabriquons ces produits avec le concours non seulement de nos employés, mais aussi de milliers d'intervenants de la base, partout dans le monde.

Chez Mozilla, nous croyons qu'Internet peut être meilleur. Pendant la période qui m'est accordée, je voudrais aborder trois sujets: premièrement, le fait que la protection de la vie privée commence par une bonne conception des produits; deuxièmement, le rôle de la réglementation en matière de protection de la vie privée; et troisièmement, certaines des questions de contenu dont vous avez parlé ces derniers jours.

Tout d'abord, nous croyons que notre industrie est en mesure de beaucoup mieux protéger la vie privée grâce à nos produits. C'est exactement ce que nous essayons de faire chez Mozilla. Permettez-moi de vous donner un exemple tiré de notre travail sur le pistage en ligne.

Lorsque les utilisateurs se rendent sur un site Web d'information, ils s'attendent à y voir des annonces de l'éditeur, du propriétaire de ce site. Or, les visiteurs des principaux sites d'information, du moins aux États-Unis, y trouvent des dizaines de dispositifs de pistage provenant de sites autres que celui qu'ils visitent, parfois même une trentaine ou une quarantaine. Certains de ces dispositifs de pistage sont rattachés à des entreprises fort bien connues, mais d'autres sont ceux d'entreprises totalement obscures dont la plupart des consommateurs n'ont jamais entendu parler.

Quoi qu'il en soit, les données recueillies par ces dispositifs causent des préjudices réels. Ils permettent de lancer des publicités politiques clivantes, d'influencer les décisions en matière d'assurance-maladie, d'encourager la discrimination dans le domaine du logement et de l'emploi. La prochaine fois que vous verrez un élément de désinformation en ligne, demandez-vous d'où viennent les données qui ont permis de croire que vous seriez une cible attrayante pour cette désinformation.

Chez Mozilla, nous avons décidé d'essayer de lutter contre le pistage en ligne. Nous avons créé ce que nous appelons le Facebook Container, qui limite grandement les données que Facebook peut recueillir sur l'utilisateur qui navigue sur Firefox. En passant, c'est maintenant l'une des extensions les plus populaires que nous ayons jamais produites. Nous sommes en train de mettre en place ce qu'on appelle la protection améliorée contre le pistage. Il s'agit d'une nouvelle fonction majeure du navigateur Firefox qui bloque presque tout le pistage effectué par des tiers. Cela va grandement limiter la capacité d'entreprises que vous ne connaissez pas de vous suivre secrètement pendant que vous naviguez sur le Web.

Nous l'offrons à un plus grand nombre de personnes, et notre but ultime est de l'appliquer par défaut à tout le monde. J'insiste là-dessus, parce que nous avons appris que la création de produits avec protection de la vie privée par défaut est un moyen très puissant pour les utilisateurs. Et il ne faut pas oublier des efforts comme nos pratiques de gestion allégée des données, que nous utilisons pour limiter les données que nous recueillons dans notre propre produit. C'est une approche que d'autres adopteront, nous l'espérons, parce que nous avons appris qu'il est vraiment irréaliste de s'attendre à ce que les utilisateurs s'y retrouvent dans toutes les politiques sur la protection des renseignements personnels et toutes les options que nous pouvons leur offrir pour qu'ils se protègent. Si nous voulons que la protection de la vie privée devienne réalité, le fardeau doit passer des consommateurs aux entreprises. Malheureusement, ce n'est pas une conviction partagée par tout le monde dans notre industrie.

Je passe maintenant à mon deuxième point: nous croyons que la réglementation sera un élément essentiel de la protection de la vie privée en ligne. L'Union européenne a été un chef de file dans ce domaine. Beaucoup d'autres entreprises dans le monde emboîtent le pas et essaient maintenant d'élaborer leurs propres lois sur la protection des données. C'est important, car l'approche que nous avons adoptée au cours des deux dernières décennies dans notre industrie ne fonctionne manifestement plus. Par le passé, nous avons vraiment adopté la notion de notification et de choix, c'est-à-dire que si nous disons simplement aux navigateurs ce que nous allons recueillir comme données et en leur permettant de s'exclure, tout ira bien. Nous avons constaté que cette approche ne fonctionne vraiment pas pour eux. Nous avons été les promoteurs de ces nouvelles règles de protection des données, et nous espérons que vous le serez aussi.

Nous croyons qu'une bonne loi sur la protection de la vie privée devrait comporter trois éléments principaux. Il faut pour les entreprises des règles claires sur ce qu'elles peuvent recueillir et utiliser; il devrait y avoir des droits solides pour les personnes, y compris le consentement granulaire et révocable au sujet d'utilisations précises; et la loi devrait être appliquée par un organisme efficace et doté de pouvoirs, ce qui n'est pas toujours le cas. C'est là un élément important, à notre avis.

● (0850)

Nous croyons qu'il est essentiel d'élaborer ces lois et d'y inclure ces éléments tout en préservant l'innovation et les utilisations bénéfiques des données. C'est pourquoi nous appuyons une nouvelle loi fédérale sur la protection des renseignements personnels aux États-Unis et nous travaillons avec les organismes de réglementation en Inde, au Kenya et ailleurs pour promouvoir des lois de cette nature.

Troisièmement, étant donné les échanges que vous avez tous eus ces derniers jours, il serait utile de dire au moins un mot de certaines de nos opinions sur les grandes questions de réglementation du contenu. De toutes les questions étudiées par le Comité, c'est la plus ardue, selon nous.

Nous avons constaté que de nombreux éléments, dans l'industrie, sont incités à encourager la propagation de la désinformation et des abus, mais nous voulons aussi nous assurer que nos réactions à ces préjudices réels ne minent pas elles-mêmes la liberté d'expression et l'innovation qui ont été une force constructive dans la vie des utilisateurs d'Internet.

Chez Mozilla, nous avons adopté quelques approches différentes. Nous travaillons actuellement à ce que nous appelons des « processus de responsabilisation ». Plutôt que de nous concentrer sur des éléments de contenu individuels, nous devrions réfléchir au genre de processus que les entreprises devraient mettre en place pour s'attaquer à ces problèmes. Cela peut se faire au moyen d'une approche fondée sur des principes. Elle doit être adaptée au rôle et proportionnelle à la taille des différentes entreprises, de sorte qu'elle n'ait pas d'incidence disproportionnée sur les petites entreprises, mais donne plus de responsabilités aux grandes entreprises qui jouent un rôle plus important dans l'écosystème.

Nous nous sommes également beaucoup occupés des problèmes de désinformation, surtout en prévision des élections législatives européennes qui viennent de se tenir. Nous sommes signataires du Code de bonnes pratiques de l'Union européenne sur la désinformation, qui est, à mon avis, une initiative d'autoréglementation très importante et utile, assortie d'engagements et de principes visant à stopper la propagation de la désinformation. Pour notre part, nous avons créé des outils dans Firefox pour aider les navigateurs à résister à la manipulation en ligne, à mieux choisir et comprendre ce qu'ils regardent en ligne.

Nous avons également déployé des efforts pour inciter les autres signataires du Code à en faire davantage en matière de transparence et de publicité politique. Il nous semble possible d'en faire beaucoup plus à cet égard. Honnêtement, il y a eu des résultats discutables chez certains de nos collègues. Il y a encore beaucoup de place pour améliorer les outils, en particulier ceux que Facebook a mis en place pour assurer la transparence de la publicité. Il y a peut-être aussi du travail à faire chez Google. Si nous n'arrivons pas à faire ce qu'il faut, nous aurons besoin de mesures plus énergiques de la part des gouvernements. La transparence devrait être un bon point de départ pour nous.

En conclusion, je dirai qu'aucune des questions examinées par le Comité n'est simple. La mauvaise nouvelle, c'est que la progression de la technologie — avec l'intelligence artificielle, la montée de l'Internet des objets et la réalité augmentée — ne fera que rendre la tâche plus difficile.

Une dernière réflexion: nous devons vraiment songer aux moyens de bâtir la capacité de la société d'affronter ces problèmes. Par exemple, chez Mozilla, nous avons participé à ce qu'on a appelé le défi de l'informatique responsable. Il s'agit d'aider à former la prochaine génération de technologues pour qu'ils comprennent les implications éthiques de ce qu'ils élaborent. Nous appuyons les efforts déployés aux États-Unis pour rétablir l'Office of Technology Assessment afin de renforcer la capacité de l'État de comprendre ces questions et de travailler avec plus de dextérité. Nous travaillons à améliorer la diversité dans notre propre entreprise et notre industrie, ce qui est essentiel si nous voulons renforcer la capacité de régler ces problèmes. Nous publions chaque année un rapport, *Bulletin de santé d'Internet*, qui a paru il y a quelques semaines. Cela fait partie de ce que nous considérons comme l'énorme projet que nous voulons tous réaliser pour sensibiliser le public afin qu'il puisse affronter ces problèmes.

Ce ne sont là que quelques exemples et quelques idées sur la façon de travailler à de nombreux niveaux. Il s'agit de concevoir de meilleurs produits, d'améliorer notre réglementation publique et d'investir dans notre capacité de relever ces défis à l'avenir.

Nous vous remercions sincèrement de nous avoir donné l'occasion de vous parler aujourd'hui et nous avons hâte de travailler avec vous et vos collègues du monde entier pour bâtir un Internet meilleur.

Merci.

● (0855)

Le président: Merci, monsieur Davidson.

Enfin, nous accueillons Erik Neuenschwander, d'Apple Inc. Je vous en prie. Vous avez 10 minutes.

M. Erik Neuenschwander (gestionnaire pour la vie privée des utilisateurs, Apple Inc.): Merci.

Bonjour, mesdames et messieurs les membres du Comité, et merci de m'avoir invité à vous parler aujourd'hui de l'approche d'Apple en matière de protection des renseignements personnels et de sécurité des données.

Je m'appelle Erik Neuenschwander et je suis ingénieur en logiciels chez Apple depuis 12 ans. J'ai été l'ingénieur principal en analyse de données sur le premier iPhone. J'ai géré l'équipe de performance du logiciel du premier iPad, et j'ai fondé l'équipe d'ingénierie de la protection de la vie privée d'Apple. Aujourd'hui, je gère l'équipe chargée des aspects techniques de la conception des caractéristiques de confidentialité d'Apple. Je suis fier de travailler dans une entreprise qui accorde la priorité au client et fabrique d'excellents produits qui améliorent la vie des utilisateurs.

Chez Apple, nous croyons que la vie privée est un droit fondamental et qu'elle est essentielle à tout ce que nous faisons. C'est pourquoi nous intégrons la protection de la vie privée et la sécurité à chacun de nos produits et services. Ces considérations architecturales vont très loin, jusqu'au silicium très physique de nos appareils. Chaque appareil que nous expédions combine des logiciels, du matériel et des services conçus pour fonctionner ensemble pour une sécurité maximale et une expérience utilisateur transparente. Aujourd'hui, j'ai hâte de discuter avec vous de ces éléments clés de conception, et je renvoie également le Comité au site Web d'Apple sur la protection des renseignements personnels, qui donne beaucoup plus de détails sur ces éléments et d'autres facteurs dont il est tenu compte dans la conception dans nos produits et services.

L'iPhone est devenu une partie essentielle de nos vies. Nous l'utilisons pour stocker une quantité incroyable de renseignements personnels, comme nos conversations, nos photos, nos notes, nos contacts, nos calendriers, nos renseignements financiers, nos données sur la santé, et même de l'information sur nos allées et venues. Notre principe, c'est que les données appartiennent à l'utilisateur. Tous ces renseignements doivent être protégés contre les pirates informatiques et les criminels qui voudraient les voler ou les utiliser à notre insu ou sans notre permission.

C'est pourquoi le cryptage est essentiel à la sécurité des dispositifs. Les outils de cryptage sont offerts dans les produits d'Apple depuis des années, et la technologie de cryptage intégrée à l'iPhone d'aujourd'hui est la meilleure sécurité de données qui soit à la disposition des consommateurs. Nous avons l'intention de poursuivre dans cette voie, parce que nous sommes fermement opposés à ce que les données de nos clients soient vulnérables aux attaques.

En établissant un code d'accès, l'utilisateur protège automatiquement l'information de son appareil au moyen d'un cryptage. Apple ne connaît pas le code d'accès de l'utilisateur. En fait, ce code n'est stocké nulle part sur l'appareil ou sur les serveurs d'Apple. Chaque fois, il appartient à l'utilisateur et à lui seul. Chaque fois qu'un utilisateur saisit son mot de passe, l'iPhone est jumelé à l'identificateur unique que l'iPhone fusionne dans son silicium au moment de la fabrication. L'iPhone crée une clé à partir de ce jumelage et tente de décrypter les données de l'utilisateur. Si la clé fonctionne, alors le mot de passe doit avoir été correct. Si cela ne fonctionne pas, l'utilisateur doit réessayer. Nous avons conçu l'iPhone pour protéger ce processus à l'aide d'une enclave sécurisée spécialement conçue, un gestionnaire de clés qui fait partie du matériel, isolé du processeur principal et offrant une couche de sécurité supplémentaire.

En concevant des produits, nous nous efforçons également de recueillir le moins de données possible sur les clients. Nous voulons que vos appareils sachent tout sur eux, mais nous ne pensons pas que nous devions tout savoir.

Par exemple, nous avons conçu notre matériel et nos logiciels de manière qu'ils fonctionnent ensemble pour offrir d'excellentes fonctions en traitant efficacement les données sans que celles-ci ne quittent jamais l'appareil de l'utilisateur. Lorsque nous recueillons des renseignements personnels, nous disons avec précision et transparence à quoi ils serviront, car le contrôle par l'utilisateur est essentiel à la conception de nos produits. Ainsi, nous avons récemment ajouté une icône de confidentialité qui apparaît sur les appareils Apple lorsque des renseignements personnels sont recueillis. L'utilisateur peut s'en servir pour en apprendre davantage sur les pratiques d'Apple en matière de protection des renseignements personnels, le tout étant expliqué en langage simple.

Nous utilisons également la « confidentialité différentielle locale », une technique qui permet à Apple d'en apprendre davantage sur un groupe d'utilisateurs sans en savoir plus sur les membres du groupe. Nous avons fait œuvre de pionnier en ce qui concerne les avis « juste-à-temps », de sorte que, lorsque des applications tierces cherchent à accéder à certains types de données, l'utilisateur a un choix et un contrôle sérieux sur les renseignements recueillis et utilisés. Cela signifie que les applications tierces ne peuvent pas accéder aux données des utilisateurs comme les contacts, les calendriers, les photos, la caméra ou le microphone sans demander et obtenir l'autorisation explicite de l'utilisateur.

Ces caractéristiques de conception, parmi d'autres, sont au cœur d'Apple. Les clients s'attendent à ce qu'Apple et d'autres entreprises de technologie fassent tout en leur pouvoir pour protéger les renseignements personnels. Chez Apple, nous sommes profondément engagés à cet égard parce que la confiance de nos clients signifie tout pour nous. Nous passons beaucoup de temps à réfléchir à la façon dont nous pouvons offrir à nos clients non seulement des produits qui transforment l'existence, mais aussi des produits fiables, sûrs et sécuritaires. En intégrant la sécurité et la protection de la vie privée à tout ce que nous faisons, nous avons prouvé que les expériences formidables n'ont pas à se faire aux dépens de la vie privée et de la sécurité. Ils peuvent plutôt les appuyer.

Je suis honoré de participer à cette importante séance. Je me ferai un plaisir de répondre à vos questions.

Merci.

● (0900)

Le président: Merci, monsieur Neuenschwander.

Nous allons passer aux questions des membres du Comité. Mon collègue Damian Collins sera ici sous peu. Il regrette d'être retenu par autre chose.

Nous allons commencer par M. Erskine-Smith, qui aura cinq minutes.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Merci beaucoup.

Merci à tous de vos exposés. Je sais que Microsoft appuie le RGPD et des règles plus strictes en matière de protection de la vie privée. De toute évidence, Tim Cook a publiquement appuyé le RGPD. Chez Amazon, appuyez-vous également ce règlement?

M. Mark Ryland: Nous appuyons les principes de protection de la vie privée que sont le contrôle par l'utilisateur, le consentement et ainsi de suite. La loi actuelle est plutôt récente et elle entraîne un fardeau qui, à notre avis, ne favorise pas directement une meilleure protection de la vie privée des utilisateurs. Bien que nous nous conformions tout à fait aux principes et que nous les appuyions pleinement, nous ne pensons pas nécessairement que c'est un dispositif qui devrait être appliqué universellement pour l'instant.

M. Nathaniel Erskine-Smith: Le soutien des principes s'étend au principe de la minimisation des données.

M. Mark Ryland: Oui, ainsi qu'au contrôle par l'utilisateur. C'est vraiment le principe fondamental.

M. Nathaniel Erskine-Smith: Chez Microsoft, approuvez-vous le principe de la minimisation des données?

M. John Weigelt: Oui, nous sommes d'accord

M. Nathaniel Erskine-Smith: Bien.

En ce qui concerne la protection des renseignements des consommateurs, une façon de s'y prendre consiste à obtenir des consentements positifs supplémentaires qui sont explicites pour des fins secondaires. Par exemple, dans le cas d'Echo d'Amazon, la Californie proposait des règles sur les haut-parleurs intelligents selon lesquelles il faudrait obtenir le consentement pour que l'information soit stockée. Êtes-vous d'accord sur ces règles?

● (0905)

M. Mark Ryland: Nous croyons que l'expérience des utilisateurs devrait être très fluide et claire, et que les attentes des gens devraient être très raisonnablement satisfaites. Par exemple, dans le cas du dispositif Echo, on utilise une application mobile pour configurer son appareil, et les règles de confidentialité sont très claires.

M. Nathaniel Erskine-Smith: Y a-t-il consentement explicite pour enregistrer ces conversations?

M. Mark Ryland: Il ne s'agit pas d'un consentement explicite, mais il indique clairement les enregistrements et vous en donne le plein contrôle. Il donne une liste complète des enregistrements et la capacité de supprimer un enregistrement en particulier, ou tous les enregistrements. Il s'agit d'une interface utilisateur très explicite et claire.

M. Nathaniel Erskine-Smith: Si le RGPD était en vigueur, il faudrait un consentement explicite.

M. Mark Ryland: Peut-être. Il peut y avoir des décisions juridiques que nous... Cela fait partie du problème. Beaucoup de détails ne seront pas clairs tant qu'il n'y aura pas plus de décisions des pouvoirs réglementaires ou des tribunaux sur la signification exacte de certains des principes généraux.

M. Nathaniel Erskine-Smith: Le représentant d'Apple pourrait-il dire si sa société pratique le pistage en ligne?

M. Erik Neuenschwander: Nous n'avons pas le genre de destinations sur Internet où se fait ce genre de pistage. Bien sûr, notre magasin en ligne, par exemple, entretient une relation directe de première partie avec les utilisateurs qui le visitent.

M. Nathaniel Erskine-Smith: Il est probablement raisonnable de s'attendre à ce que, lorsque je me rends sur le site d'Apple, cette société veuille communiquer avec moi par la suite, mais si je me rends sur d'autres sites non connexes sur Internet, Apple ne pratiquerait aucun pistage.

M. Erik Neuenschwander: Non, Apple ne le fait pas. En réalité, notre système intelligent de prévention du pistage est activé par défaut dans notre navigateur Web Safari. Si Apple essayait de faire du pistage, le système de prévention chercherait à l'en empêcher.

M. Nathaniel Erskine-Smith: Je m'adresse à Microsoft et à Amazon. Faites-vous comme Apple ou faites-vous du pistage en ligne sur de nombreux sites Internet?

M. Mark Ryland: Nous sommes engagés dans l'écosystème du Web et nous avons la capacité de comprendre d'où viennent les utilisateurs et où ils vont lorsqu'ils quittent notre site.

Encore une fois, notre principal modèle d'affaires consiste à vendre des produits à des clients. Le pistage n'est pas pour nous un moyen de recueillir de l'argent pour l'entreprise.

M. Nathaniel Erskine-Smith: Était-ce un oui au pistage en ligne, de façon assez générale?

M. Mark Ryland: Nous participons à l'écosystème de la publicité. Alors c'est oui.

M. Nathaniel Erskine-Smith: C'est ainsi que j'interprète votre réponse.

Les représentants de Microsoft ont-ils quelque chose à dire?

M. John Weigelt: Nous avons nos propriétés particulières, comme les autres groupes. Nous avons le magasin Microsoft et les propriétés de MSN. Nous sommes donc en mesure de trouver l'origine de nos clients.

M. Nathaniel Erskine-Smith: Si je pose la question, c'est qu'hier, un témoin nous a dit que le consentement, parfois, n'était pas suffisant, et je comprends que, dans certains cas, ce soit vrai. Comme je suis raisonnablement occupé, on ne peut pas s'attendre à ce que je lise chaque entente sur les modalités. On ne peut pas s'attendre à ce que je lise tout. S'il y a des consentements secondaires dans chaque application que j'utilise et que je dois donner 10 consentements différents, vais-je vraiment pouvoir protéger mes renseignements personnels? Nous ne devrions pas nous attendre à cela des consommateurs, et c'est pourquoi nous avons une loi sur la protection des consommateurs et des garanties implicites dans d'autres contextes.

Hier, Roger McNamee a laissé entendre que certaines choses devraient être strictement exclues. J'ai dit à Google qu'il ne devrait peut-être pas être en mesure de lire mes courriels et de me cibler en fonction de publicités — cela devrait être exclu. Pensez-vous, chez Apple, que certaines choses devraient tout simplement être exclues?

M. Erik Neuenschwander: Oui, lorsque nous... Notre service iCloud est un lieu où les utilisateurs peuvent stocker leurs photos ou leurs documents chez Apple, et nous n'exploitons pas ce contenu pour créer des profils de nos utilisateurs. Nous considérons qu'il s'agit des données de l'utilisateur. Nous les stockons grâce à notre service, mais elles demeurent la propriété de l'utilisateur.

M. Nathaniel Erskine-Smith: Même question pour Microsoft et Amazon: pensez-vous que la collecte de certaines données devrait être complètement exclue?

M. John Weigelt: L'une des choses qui nous tiennent à coeur, c'est que les utilisateurs puissent savoir quelles données ils ont communiquées à certaines organisations. Nous avons travaillé en étroite collaboration — je l'ai fait personnellement — avec les commissaires à l'information et à la protection de la vie privée de tout le Canada. Nous avons discuté du consentement et du sens à donner à ce terme. Lorsque nous avons mis en place des outils comme Cortana, par exemple, nous avons travaillé avec le Commissariat à la protection de la vie privée du Canada pour arriver à comprendre laquelle des 12 étapes du consentement pour les consommateurs était particulièrement importante.

M. Nathaniel Erskine-Smith: Mais je propose que, au-delà de la question du consentement, certains éléments soient exclus d'emblée. Par exemple, mes photos personnelles sur mon téléphone. Devrait-on pouvoir les numériser, après quoi je recevrais des annonces ciblées?

M. John Weigelt: Soyons clairs: nous ne numérisons pas cette information...

M. Nathaniel Erskine-Smith: Eh bien, je sais que vous ne le faites pas...

M. John Weigelt: ... mais nous fournissons...

M. Nathaniel Erskine-Smith: ... mais certaines choses devraient-elles être exclues? Voilà où je veux en venir.

M. John Weigelt: ... une certaine visibilité pour les clients afin qu'ils comprennent où leurs données sont utilisées et qu'ils en aient le plein contrôle.

Notre tableau de bord sur la protection des renseignements personnels, par exemple, permet de voir quelles données se trouvent dans l'environnement Microsoft, puis l'utilisateur peut contrôler ces données et être en mesure de mieux gérer la situation. Il s'agit d'avoir cette interaction avec les utilisateurs pour qu'ils comprennent la proposition de valeur de cette capacité de communiquer des données.

M. Nathaniel Erskine-Smith: Les représentants d'Amazon sont-ils d'avis qu'il faudrait exclure certaines choses?

M. Mark Ryland: Je ne pense pas qu'on puisse dire, a priori, que certaines choses sont toujours inacceptables, parce que, encore une fois, l'expérience client est essentielle, et si les gens veulent une meilleure expérience client fondée sur les données qu'ils communiquent... Le consentement, évidemment, et le contrôle sont essentiels.

M. Nathaniel Erskine-Smith: Prenons le cas des enfants de moins de 18 ans, par exemple. Nous ne devrions peut-être pas être en mesure de recueillir des renseignements sur les jeunes de moins de 18 ans, de moins de 16 ans ou de moins de 13 ans.

Les enfants, disons. Faudrait-il exclure les données qui les concernent?

● (0910)

M. Mark Ryland: Nous allons nous conformer à toutes les lois des pays où nous menons nos activités, si...

M. Nathaniel Erskine-Smith: Êtes-vous en train de dire que vous n'avez pas d'opinion éthique sur la collecte de renseignements auprès des enfants?

M. Mark Ryland: Nous sommes certainement d'avis que les parents devraient être responsables de l'expérience en ligne des enfants, et nous donnons aux parents le plein contrôle de cette expérience dans nos systèmes.

M. Nathaniel Erskine-Smith: Merci beaucoup.

Il est tellement difficile de dire oui.

Le président: Nous passons maintenant à M. Kent, qui aura cinq minutes.

L'hon. Peter Kent (Thornhill, PCC): Merci, monsieur le président.

Je remercie tous nos témoins qui comparaissent aujourd'hui.

Ma première question s'adresse à M. Ryland, d'Amazon.

En septembre dernier, le vice-président et avocat général associé d'Amazon, M. DeVore, témoignant devant un comité du Sénat américain, a critiqué vivement, je crois que le mot est juste, la loi sur la protection des consommateurs qui avait été adoptée en Californie.

Parmi les nouveaux droits reconnus aux consommateurs dans cette loi auxquels il s'est opposé, il y avait le droit des utilisateurs de connaître toutes les données commerciales recueillies à leur sujet et le droit de s'opposer à la vente de ces données. La loi institue, en Californie, le droit d'interdire la vente de ces données à des tiers. Il a dit que la loi avait été adoptée trop rapidement et que la définition de renseignements personnels était trop large.

Je me demande si vous pourriez nous aider aujourd'hui en nous disant comment Amazon définit les renseignements personnels à protéger.

M. Mark Ryland: Tout d'abord, permettez-moi de dire que je travaille aux services Web d'Amazon dans le domaine de la sécurité et de la protection des données sur notre plateforme infonuagique. Je ne connais pas à fond l'ensemble de nos politiques de protection des renseignements personnels.

Toutefois, je dirai que certains éléments des données sur les consommateurs sont utilisés dans les secteurs de base de l'entreprise. Par exemple, si nous vendons un produit à un client, nous devons en faire un certain suivi à des fins fiscales et juridiques, de sorte qu'il est impossible de dire qu'un consommateur a un contrôle total sur certaines choses. Il y a d'autres raisons juridiques, par exemple, pour lesquelles les données doivent parfois être conservées.

L'hon. Peter Kent: Des utilisateurs vous ont-ils demandé de l'information sur les données qui ont été recueillies à leur sujet et si elles avaient été vendues?

M. Mark Ryland: Oui, assurément.

Tout d'abord, je tiens à dire qu'Amazon ne vend pas de données sur ses clients. Point à la ligne.

Deuxièmement, nous avons une page de renseignements personnels protégés où l'utilisateur peut voir toutes les données le concernant que nous avons accumulées: l'historique de ses commandes, ses commandes numériques, ses commandes de livres, etc. Nous avons une page similaire pour notre service Alexa Voice. Tout cela permet aux utilisateurs de contrôler et de comprendre les données que nous utilisons.

L'hon. Peter Kent: Ainsi, malgré les critiques de M. DeVore, Amazon se conforme à la loi californienne, et je suppose qu'elle se conformerait à toute autre loi semblable adoptée ailleurs dans le monde.

M. Mark Ryland: Nous nous conformerons toujours aux lois qui s'appliquent à nous partout où nous faisons des affaires. Certainement.

L'hon. Peter Kent: Merci.

J'aimerais maintenant poser une question à M. Davidson au sujet de Mozilla.

Je sais que Mozilla, avec toutes ses bonnes pratiques et son mandat d'intérêt public sans but lucratif, travaille avec Google et avec Bing. Je me demande simplement quels genres de pare-feu vous établissez pour empêcher l'accumulation de données sur les utilisateurs par ces deux entreprises qui, autrement, les recueilleraient et les monétiseraient.

M. Alan Davidson: Voilà une excellente question. Chez nous, c'est assez simple. Nous ne leur envoyons tout simplement pas de données au-delà de ce qu'ils obtiendraient normalement d'un visiteur qui se rend sur leur site Web, l'adresse IP, par exemple.

Nous avons pour pratique de ne pas recueillir de renseignements. Si, à partir de Firefox, vous faites une recherche sur Bing ou Google, nous n'en gardons aucune trace, nous ne conservons rien et nous ne transmettons rien de spécial. Cela nous a permis de nous distancer, honnêtement, et nous n'avons aucun incitatif financier à recueillir cette information.

L'hon. Peter Kent: J'ai une question pour M. Neuenschwander.

En septembre dernier, on a appris que l'application Mac Adware Doctor, qui était censée protéger les utilisateurs d'Apple contre les menaces à la protection de la vie privée, enregistrait en fait les données de ces utilisateurs et les transmettait à un serveur en Chine. Apple y a mis fin depuis, mais je voudrais savoir combien de temps a duré cette exposition. Avez-vous déterminé qui exactement exploitait ce serveur en Chine?

M. Erik Neuenschwander: Je me souviens de cet événement et des mesures prises par l'équipe de l'App Store. Je ne peux pas, de mémoire, vous dire exactement quelle a été la durée de l'exposition. Je me ferai un devoir de vérifier cette information et de vous revenir là-dessus.

● (0915)

L'hon. Peter Kent: Vous ne connaissez pas la durée de l'exposition…

M. Erik Neuenschwander: Sur le moment, je ne pourrais pas le dire exactement.

L'hon. Peter Kent: Je crois savoir que c'était une application Mac très populaire. Dans quelle mesure examinez-vous rigoureusement ces applications, dans la ruée capitaliste, bien compréhensible, pour monétiser ces nouvelles merveilles?

M. Erik Neuenschwander: Pour les applications gratuites en magasin, il n'y a pas de monétisation pour Apple dans l'App Store.

Depuis que nous avons lancé l'App Store, nous effectuons un examen manuel et, ces dernières années, un examen automatisé de chaque application proposée au magasin, puis de chaque mise à jour de ces applications. Elles sont soumises à l'examen d'une équipe d'experts spécialisés de l'App Store.

Il y a une limite que nous ne dépassons pas. Nous ne surveillons pas l'utilisation des applications par nos utilisateurs. Une fois l'application installée sur l'appareil d'un utilisateur, nous nous interdisons, par respect pour la vie privée de l'utilisateur, de surveiller le trafic réseau ou les données qu'il envoie. Cela nous semblerait inconvenant.

Nous continuons d'investir du côté de l'App Store pour tâcher d'avoir un examen aussi rigoureux que possible. À mesure que les applications et leurs fonctionnalités changent, nous continuons de renforcer notre examen pour saisir les fonctionnalités qui ne répondent pas à nos politiques de confidentialité dans les magasins.

L'hon. Peter Kent: J'ai une question pour les représentants de Microsoft, Mme Floyd en particulier. En 2013, la Commission européenne a imposé à Microsoft une amende d'environ 561 millions d'euros pour non-respect des engagements relatifs au choix de navigateur. Il ne semble pas y avoir eu de violation depuis. Tire-t-on des leçons d'amendes aussi lourdes? On nous dit que les amendes, même s'élevant à des centaines de millions de dollars ou d'euros — même celles dépassant le milliard de dollars —, ne découragent pas les grandes entreprises numériques. Je m'interroge sur l'utilité de fortes sanctions pécuniaires, qui n'existent pas actuellement au Canada, comme moyen pour assurer la conformité, ou pour inciter à la conformité.

M. John Weigelt: Comme nous l'avons dit, la confiance est le fondement de notre entreprise. Chaque fois qu'il y a un jugement prononcé contre notre entreprise, nous constatons que la confiance s'érode, et cela se répercute sur toute l'organisation, non seulement du côté des consommateurs, mais aussi au sein de l'entreprise.

Cette amende était lourde. Nous avons donné suite à ce jugement en modifiant la façon dont nous offrons nos produits sur le marché, en donnant aux consommateurs le choix d'acheter des produits sans navigateur intégré.

Lorsque nous examinons le pouvoir de rendre des ordonnances, ici au Canada ou ailleurs, nous devons conclure qu'un jugement défavorable aura une incidence beaucoup plus grande sur l'entreprise que certaines de ces sanctions pécuniaires.

L'hon. Peter Kent: Pensez-vous que le gouvernement canadien devrait renforcer ses règlements et ses sanctions en cas de non-respect des règles de protection de la vie privée?

M. John Weigelt: J'encouragerais le gouvernement canadien à se faire entendre sur la façon dont les technologies sont mises en place dans le contexte canadien. Nous avons des gens sur place qui sont là pour l'entendre et modifier en conséquence la façon dont nous offrons nos services.

L'hon. Peter Kent: Merci.

Le président: Allez-y, monsieur Angus. Vous avez cinq minutes.

M. Charlie Angus (Timmins—Baie James, NPD): Merci, monsieur le président.

Je parlais à un ami chez Apple de l'achat, en 1984, de mon premier Mac Plus, muni d'une disquette de 350 kilobits, que je voyais comme un outil révolutionnaire qui allait changer le monde pour le mieux. Je continue de croire que le monde a changé pour le mieux, mais nous constatons aussi des dérapages vraiment regrettables.

Maintenant que j'ai moi-même pris de l'âge, je peux prendre du recul et m'imaginer ce qui se serait passé si, dans les années 1980, Bell avait écouté mes conversations téléphoniques. Des accusations auraient été portées, même si Bell se justifiait en disant: « Nous écoutons vos conversations simplement parce que nous voulons vous offrir des trucs vraiment astucieux et nous pourrons mieux vous servir si nous savons ce que vous faites. » Que se passerait-il si le bureau de poste lisait mon courrier avant de me le livrer, non dans un but illicite, mais pour me mettre au courant de choses très intéressantes que je devrais connaître et pour me proposer son aide? Des accusations seraient certainement portées.

Pourtant, dans le monde numérique, nous avons maintenant affaire à des entreprises qui nous offrent toutes sortes de possibilités alléchantes. C'est sur ce point que mon collègue, M. Erskine-Smith, essayait d'obtenir des réponses claires.

Je pense que, en tant que parlementaires, nous allons vraiment au-delà de cette discussion sur le consentement. Le consentement n'a plus aucun sens si on nous espionne, si on nous surveille et si notre téléphone sert à nous pister. Le consentement est en train de devenir un terme trompeur parce qu'il s'agit de récupérer un espace dans nos vies que nous n'avons pas cédé. Si nous suivions les anciennes règles, il ne serait pas possible d'écouter nos conversations téléphoniques et de nous pister en ligne au mépris de nos droits, mais c'est tout à coup devenu acceptable dans le monde numérique.

Monsieur Davidson, je m'intéresse beaucoup au travail que fait Mozilla.

Pensez-vous qu'il soit possible pour les parlementaires d'établir des règles de base raisonnées pour protéger le droit à la vie privée des citoyens, des règles qui n'entraîneront pas la ruine complète des gens de Silicon Valley, n'en feront pas tous des assistés sociaux, et qui permettront au modèle d'affaires de réussir? Est-il possible d'établir des règles simples?

● (0920)

M. Alan Davidson: Oui.

Je peux en dire plus.

M. Charlie Angus: Allez-y.

M. Alan Davidson: Je pense que c'est effectivement…

M. Charlie Angus: J'adore ça quand on est d'accord avec moi.

M. Alan Davidson: Nous cherchions des feux verts.

Vous connaissez déjà certains exemples. Nous croyons fermement qu'il est possible d'établir de bonnes entreprises rentables tout en respectant la vie privée des gens. Vous avez pris connaissance de quelques exemples aujourd'hui, dont certains de notre part. Il existe des exemples de bonnes lois, y compris le RGPD.

Il y a des choses qui dépassent probablement toutes les bornes, pour lesquelles nous avons besoin d'interdictions claires ou de mesures de sécurité très rigoureuses. À mon avis, il ne faut pas rejeter complètement l'idée du consentement. Ce qu'il nous faut, c'est un consentement plus précis parce que je pense que les gens ne comprennent pas vraiment…

M. Charlie Angus: Le consentement explicite.

M. Alan Davidson: ... le consentement explicite.

Il y a toutes sortes de façons de l'encadrer, mais il y a une forme plus parcellaire de consentement explicite. C'est qu'il y aura des moments où des gens voudront profiter d'applications sur la santé ou faire connaître à des proches et à leur famille où ils se trouvent. Ils devraient pouvoir le faire, mais ils devraient vraiment comprendre ce que cela implique.

Nous croyons qu'il demeure possible de créer des entreprises qui le permettraient.

M. Charlie Angus: Merci.

Certaines des préoccupations sur lesquelles nous nous sommes penchés concernent l'intelligence artificielle. Il s'agit de l'arsenalisation des médias numériques. L'intelligence artificielle pourrait jouer un rôle très positif ou très négatif.

Monsieur Ryland, Amazon a certainement fait beaucoup de progrès en matière d'intelligence artificielle. Cependant, elle a également été qualifiée d'entreprise novatrice du XXI^{e} siècle, mais dont les pratiques de travail appartiennent au XIX^{e} siècle.

Au sujet des allégations selon lesquelles les travailleurs faisaient l'objet d'une surveillance, pouvant mener jusqu'à leur congédiement, au moyen d'un pistage par intelligence artificielle, est-ce bien la politique d'Amazon?

M. Mark Ryland: Notre politique est certainement de respecter la dignité de notre main-d'œuvre et de traiter tout le monde comme il se doit.

Je ne connais pas les détails de cette allégation, mais je me ferai un devoir de vous fournir de plus amples renseignements.

M. Charlie Angus: C'était dans un article retentissant sur Amazon. On y lisait que les travailleurs étaient surveillés, jusqu'à la seconde près, par des moyens d'intelligence artificielle et que ceux qui étaient trop lents étaient congédiés.

Je suis peut-être de la vieille école, mais je pense que ce serait illégal en vertu des lois du travail de notre pays. C'est apparemment la façon dont l'intelligence artificielle est utilisée dans les centres de traitement. À mon avis, c'est une utilisation très problématique de l'intelligence artificielle. N'êtes-vous pas au courant de cela?

M. Mark Ryland: Je ne suis pas au courant, et je suis presque certain qu'il y aurait un examen humain de toute décision de congédiement. Il est impossible de prendre une telle décision sans au moins un examen humain des types d'algorithmes d'apprentissage machine.

M. Charlie Angus: C'était un article assez accablant, et le sujet a été repris par de nombreux journaux étrangers.

Pourriez-vous faire un suivi de cette question et transmettre une réponse au Comité?

M. Mark Ryland: Je me ferai un plaisir d'y donner suite.

M. Charlie Angus: Je ne cherche pas à vous mettre sur la sellette, mais je voudrais avoir une réponse à ce sujet. Je pense que nous aimerions certainement pouvoir nous faire une idée de l'optique dans laquelle Amazon utilise l'intelligence artificielle pour faire la surveillance des travailleurs dans les centres de traitement. Si vous pouviez faire parvenir cela au Comité, ce serait très utile.

M. Mark Ryland: Je ne manquerai pas de le faire.

Le président: Merci, monsieur Angus.

Nous passons maintenant à nos délégations.

Nous allons commencer par celle de Singapour.

Allez-y, vous avez cinq minutes.

Mme Sun Xueling (secrétaire parlementaire principale, Ministère des affaires intérieures et Ministère du développement national, Parlement de Singapour): Merci, monsieur le président.

J'ai quelques questions à poser à M. Davidson.

J'ai lu avec intérêt le Manifeste Mozilla. Je suppose que j'avais un peu de temps libre. Je pense qu'il y a 10 principes dans votre manifeste. Je m'arrête en particulier sur le principe 9, qui est formulé comme suit: « L'investissement commercial dans le développement d'Internet apporte de nombreux bénéfices; un équilibre entre les bénéfices commerciaux et l'intérêt public est crucial. »

C'est textuellement ce que dit le principe 9.

Seriez-vous d'accord, alors, pour dire que les entreprises de technologie, même si elles ont un objectif de croissance et de rentabilité, ne devraient pas abdiquer leur responsabilité d'empêcher l'utilisation abusive de leurs plateformes?

M. Alan Davidson: Nous sommes tout à fait d'accord avec cela. Je dirais que le manifeste, pour ceux qui ne l'ont pas lu, constitue en quelque sorte nos principes directeurs. Il a été rédigé il y a une quinzaine d'années. Nous venons tout juste de le mettre à jour en y apportant un ensemble d'ajouts pour répondre à la situation d'aujourd'hui.

Nous croyons effectivement que cet équilibre est vraiment important. Pour ma part, je pense que les entreprises doivent réfléchir aux conséquences de ce qu'elles construisent. Je pense aussi que le gouvernement doit baliser tout cela parce que, nous l'avons vu, ce ne sont pas toutes les entreprises qui vont le faire. Certaines ont besoin d'être guidées.

Mme Sun Xueling: De plus, il me semble que le Bulletin de santé d'Internet a été publié par la Fondation Mozilla, et j'aimerais remercier votre organisme, qui est sans but lucratif et qui travaille dans l'intérêt public. Je pense que votre bulletin a traité du scandale impliquant Cambridge Analytica et a fait remarquer qu'il était un symptôme d'un problème systémique beaucoup plus vaste, que, de nos jours, le modèle d'affaires dominant et les activités courantes du monde numérique sont, en fait, fondés sur la collecte et la vente de données au sujet des utilisateurs.

Seriez-vous alors d'accord pour dire que le scandale impliquant Cambridge Analytica illustre en quelque sorte une attitude mentale qui priorise la quête du gain et de la croissance de l'entreprise au détriment de sa responsabilité civique?

● (0925)

M. Alan Davidson: Oui, mais nous gardons espoir qu'il s'agit de cas isolés. Je dirais simplement que ce ne sont pas toutes les entreprises qui fonctionnent de cette façon. Il y a, je crois, des entreprises qui tâchent de faire ce qu'il faut pour servir l'utilisateur, qui tentent de faire passer leurs utilisateurs en premier, et non uniquement à des fins altruistes. Je pense que c'est plutôt parce que nous sommes nombreux à croire que c'est dans l'intérêt de l'entreprise et que, sur le long terme, le marché récompensera les entreprises qui accordent la priorité aux utilisateurs.

Mme Sun Xueling: Nous avons entendu des témoignages hier également. Je pense que bon nombre des membres du grand comité ont parlé avec des entreprises qui avaient fait état d'exemples concernant le Sri Lanka ou Nancy Pelosi. Il m'a semblé qu'il s'agissait davantage de diffuser de l'information, d'assurer la liberté d'extension de l'information, plutôt que de protéger réellement la liberté d'expression, puisqu'il qu'il n'y a pas de véritable liberté d'expression si elle est fondée sur une information fausse ou trompeuse.

Même si nous aimons croire que le scandale impliquant Cambridge Analytica est un cas unique, ce qui nous préoccupe, je pense, c'est que les modèles d'affaires existants de ces entreprises ne semblent pas devoir nous assurer que la responsabilité civique est perçue sous le même jour que la marge bénéficiaire des entreprises. Je pense que c'est à cela que je voulais en venir.

M. Alan Davidson: Étant dans ce domaine depuis longtemps, je peux dire qu'il est vraiment désolant de voir certains de ces comportements en ligne. Je pense que c'est en partie à cause de l'évolution des modèles d'affaires, surtout ceux qui font de l'engagement la mesure prépondérante. Nous espérons que les entreprises feront plus et mieux.

Il y a un risque à une trop grande intervention gouvernementale dans ce domaine, du fait que nous tenons à respecter la liberté d'expression. Lorsque les gouvernements font des choix tranchés sur ce qui est vrai et ce qui est faux dans l'information diffusée en ligne, il y a beaucoup de risques. Je pense qu'il faut trouver un juste équilibre. Pour commencer, il me semble qu'il faudrait utiliser notre tribune exceptionnelle pour vraiment pousser les entreprises à faire mieux. C'est le bon point de départ. Espérons qu'il aura des suites utiles.

Mme Sun Xueling: Oui. Merci.

Le président: Nous allons maintenant passer à la délégation irlandaise et à Mme Naughton.

Mme Hildegarde Naughton (présidente, Comité mixte sur les communications, l'action sur le climat et l'environnement, Parlement de la République d'Irlande): Je vous remercie, monsieur le président. Merci à tous d'être venus ce matin.

Ma première question s'adresse au porte-parole d'Amazon. En novembre dernier, le vendredi noir, je crois savoir qu'il y a eu des problèmes techniques. Beaucoup de noms et de courriels de clients ont paru sur votre site Web. Est-ce exact?

M. Mark Ryland: Non, ce n'est pas exact.

Mme Hildegarde Naughton: Non? D'accord. Je croyais qu'il y avait eu des reportages à ce sujet. Y a-t-il eu des problèmes techniques en novembre dernier?

M. Mark Ryland: Cela ne me dit rien du tout, mais je me ferai un plaisir de vérifier. Non, je ne suis pas au courant.

Mme Hildegarde Naughton: En ce qui concerne le RGPD et la protection des données, d'après ce que mes collègues vous ont demandé tout à l'heure, vous dites que vous seriez en faveur d'une forme quelconque de RGPD à l'échelle mondiale.

M. Mark Ryland: Encore une fois, nous croyons que les principes de la confiance des consommateurs — accorder la priorité aux clients, leur donner le contrôle de leurs données, obtenir leur consentement à l'utilisation des données — ont du sens. Les moyens précis de le faire, la tenue de dossiers et la charge administrative que cela suppose semblent parfois l'emporter sur les avantages pour les consommateurs, alors nous pensons vraiment que nous devons travailler en collectivité pour trouver un juste équilibre qui ne soit pas trop onéreux.

Par exemple, une grande entreprise comme la nôtre serait capable de se conformer à un règlement très coûteux à appliquer, mais pas nécessairement une petite entreprise. Nous devons trouver des moyens d'appliquer ces principes de façon efficace, relativement simple et directe.

Bien sûr, nous appuyons les principes qui sous-tendent le RGPD. Nous pensons que la loi comme telle n'est pas encore tout à fait au point, en ce sens que nous ne savons pas exactement comment certaines dispositions seront interprétées une fois rendues au niveau réglementaire ou judiciaire — ce qu'on entend au juste par diligence raisonnable, par exemple, de la part d'une entreprise.

Mme Hildegarde Naughton: D'accord, alors êtes-vous ouvert à cela, ou peut-être à une version différente à travers le monde?

M. Mark Ryland: Oui.

Mme Hildegarde Naughton: Comme vous le savez, dans le RGPD tel qu'il s'applique actuellement, il y a de ces obstacles pour certaines entreprises, mais on les a aplanis dans l'ensemble de l'Union européenne.

M. Mark Ryland: Oui.

Mme Hildegarde Naughton: Je suppose que vous attendez de voir la suite des choses...

M. Mark Ryland: Nous pensons qu'il y aura beaucoup de bonnes leçons à tirer de cette expérience. Nous pourrons faire mieux à l'avenir, que ce soit en Europe ou ailleurs, mais encore une fois, les principes ont du sens.

● (0930)

Mme Hildegarde Naughton: D'accord.

Ma question s'adresse à Microsoft. Plus tôt cette année, je crois savoir qu'un pirate a compromis le compte d'un agent de soutien de Microsoft. Est-ce exact?

M. John Weigelt: C'est exact. Il y a eu divulgation de justificatifs d'identité.

Mme Hildegarde Naughton: Microsoft disait alors qu'il se pouvait que le pirate ait eu accès au contenu de certains utilisateurs d'Outlook. Est-ce que cela est vraiment arrivé? A-t-il pu accéder au contenu d'utilisateurs de Microsoft?

M. John Weigelt: Cet accès du côté du soutien leur en donnait la possibilité, oui.

Mme Hildegarde Naughton: Comment un pirate a-t-il pu, je suppose, déjouer votre propre sécurité ou votre dispositif de sécurité des données?

M. John Weigelt: Tout cet environnement repose sur un modèle de confiance de bout en bout, alors il suffit de trouver le maillon le plus faible dans la chaîne. Dans ce cas-ci, malheureusement, l'employé de soutien avait un mot de passe que les pirates pouvaient deviner pour entrer dans ce système.

Mme Hildegarde Naughton: Qu'avez-vous fait pour que cela ne se reproduise plus? Cela me paraît être une atteinte fondamentale à la sécurité des données de vos utilisateurs.

M. John Weigelt: Tout à fait. Chaque fois qu'il se produit un incident dans notre environnement, nous réunissons notre équipe d'intervention de sécurité avec nos techniciens pour voir comment nous améliorer. Nous avons examiné ce qui s'était passé et nous nous sommes assurés de pouvoir mettre en place des protections comme le contrôle multifactoriel, qui exige deux choses pour se connecter: quelque chose que vous savez, quelque chose que vous avez. Nous avons envisagé des choses comme le contrôle à deux personnes et des outils de ce genre, afin de nous assurer de préserver la confiance de nos clients.

Mme Hildegarde Naughton: Nous savons que vous avez apporté ces changements. Avez-vous eu un rapport? Avez-vous fait un rapport sur le nombre d'utilisateurs dont les renseignements ou le contenu ont été compromis?

M. John Weigelt: Il faudrait que nous revenions devant le Comité pour en discuter. Je ne suis pas au courant de ce rapport. Je n'avais pas moi-même cherché à savoir.

Mme Hildegarde Naughton: D'accord.

En ce qui concerne les mesures prises par la suite... Là encore, il s'agit de la confiance des utilisateurs en ligne et de ce que votre entreprise a fait. Pourriez-vous nous revenir à ce sujet?

M. John Weigelt: Absolument.

Mme Hildegarde Naughton: Merci.

Le vice-président (M. Nathaniel Erskine-Smith (Beaches—East York, Lib.)): Il vous reste une minute.

M. James Lawless (membre, Comité mixte sur les communications, l'action sur le climat et l'environnement, Parlement de la République d'Irlande): Merci, monsieur le président.

Je m'adresse d'abord à Amazon. Est-ce qu'Alexa nous écoute? Je suppose que oui. Que fait-elle de cette information?

M. Mark Ryland: Alexa est à l'affût d'un mot-clé, le mot qui l'active, qui avertit le système que vous voulez interagir avec lui d'une façon ou d'une autre. Cette information n'est pas stockée localement. Rien n'est stocké localement sur l'appareil. Une fois que le mot-clé est reconnu, il suit le flux de données. Un témoin lumineux vous indique que l'appareil est maintenant actif, et le son suivant qui se produit dans la pièce est alors envoyé dans le nuage.

La première chose que fait le nuage, c'est de revérifier le mot-clé. Souvent, le logiciel de l'appareil n'est pas évolué, alors il fait parfois des erreurs. Si le nuage reconnaît que ce n'était pas un mot-clé, il interrompt le flux. Par contre, si le nuage confirme que le mot-clé a été prononcé, le flux est ensuite acheminé par un système de traitement du langage naturel, qui produit essentiellement un texte. À partir de là, les systèmes prennent le relais pour répondre à la demande de l'utilisateur.

M. James Lawless: D'accord.

Est-ce qu'Amazon se sert de cette information à des fins de profilage ou de marketing?

M. Mark Ryland: L'information est versée dans les renseignements sur votre compte, tout comme si vous achetiez des livres sur notre site Web. Elle pourrait donc influencer ce que nous vous présentons comme autres choses susceptibles de vous intéresser.

M. James Lawless: D'accord.

M. Mark Ryland: Elle n'est transmise à aucun tiers. Elle ne sert pas à des fins publicitaires et ainsi de suite.

M. James Lawless: D'accord, mais si vous avez demandé le temps qu'il fait aux Bermudes et que vous allez ensuite sur le site Web d'Amazon, vous pourriez tomber sur un guide de vacances aux Bermudes, n'est-ce pas?

M. Mark Ryland: C'est théoriquement possible, oui. Je ne sais pas si cet algorithme existe.

M. James Lawless: Est-ce probable?

M. Mark Ryland: Je ne sais pas. Il faudrait que je vous revienne là-dessus.

M. James Lawless: D'accord, mais on utilise tout de même les questions posées, qui sont traitées par Alexa, pour offrir quelque chose à l'utilisateur. On pourrait s'en servir pour lui faire une présentation de marketing intelligent sur la plateforme, non?

M. Mark Ryland: C'est parce que l'utilisateur lie directement l'appareil à son compte et que tous ses énoncés deviennent visibles. Vous pouvez voir une liste complète de ce que vous avez dit et vous pouvez supprimer n'importe quel énoncé. Il sera aussitôt retiré de la base de données et ne pourra plus servir à vous faire une recommandation.

M. James Lawless: Est-ce que l'utilisateur consent à cela lorsqu'il s'inscrit? Est-ce que cela fait partie des modalités?

M. Mark Ryland: Je pense que c'est très clair. Le consentement fait partie de l'expérience. Pour prendre un exemple familier, je n'ai pas explicitement consenti à ce que ma voix et mon image soient enregistrées ici aujourd'hui, mais le contexte me dit que c'est probablement ce qui se passe. Nous croyons que les expériences simples pour le consommateur sont les meilleures. Nous pensons que nos clients comprennent que, si nous accumulons des données à leur sujet, c'est justement pour que le service fonctionne comme il est censé fonctionner...

Le vice-président (M. Nathaniel Erskine-Smith): Merci.

M. Mark Ryland: ... et nous facilitons vraiment, vraiment, la suppression et le contrôle de ces données.

● (0935)

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup, même si vous comprenez peut-être mieux ce qui se passe aujourd'hui que la plupart des utilisateurs d'Alexa.

M. Charlie Angus: Excusez-moi, monsieur le président, mais puis-je invoquer le Règlement?

Je veux que ce soit bien clair. Quand on s'adresse à un comité, c'est comme s'adresser à un tribunal. Il ne s'agit pas de savoir si vous consentez à être enregistré ou si vous pensez que vous l'êtes. Il s'agit d'un processus parlementaire prévu par la loi, alors, bien sûr, vous êtes enregistré. Il est ridicule de comparer cela avec Alexa qui vous vend quelque chose à la Barbade, cela mine les fondements de notre Parlement.

Je rappellerais simplement aux témoins que nous sommes ici pour recueillir de l'information au profit de la communauté internationale des législateurs, et que tout est consigné officiellement.

Le vice-président (M. Nathaniel Erskine-Smith): Merci, monsieur Angus.

Monsieur de Burgh Graham, vous avez cinq minutes.

M. David de Burgh Graham (Laurentides—Labelle, Lib.): Merci. Je vais commencer par Microsoft.

L'écosystème de Microsoft est assez vaste, comme vous le savez. Vous avez la majorité des ordinateurs de bureau du monde, avec Office 365, LinkedIn, Bing, Skype, MSN, Live.com, Hotmail, etc. De toute évidence, vous avez la capacité de recueillir une énorme quantité de données sur un nombre immense de personnes. Pouvez-vous m'assurer qu'il n'y a pas de données personnelles échangées entre ces différentes plateformes?

M. John Weigelt: Parlez-vous de données échangées entre, disons, un utilisateur de Xbox et un utilisateur d'Office 365? Est-ce là votre question?

M. David de Burgh Graham: Oui, ou entre LinkedIn et Bing. Pendant nos premiers jours de séance sur cette question, nous avons beaucoup entendu parler de la création d'avatars des utilisateurs de différentes entreprises. Est-ce que Microsoft crée un avatar de ses utilisateurs? Est-ce qu'elle crée une image de qui utilise ses services?

M. John Weigelt: Si vous avez un compte Microsoft commun, vous pouvez conserver et gérer vos données de l'une à l'autre de ces plateformes. L'équipe de produits de Bing ne ferait pas nécessairement l'aller-retour entre elle et l'équipe de Xbox pour obtenir les données requises. C'est vous qui contrôlez les données qui se trouvent au centre.

M. David de Burgh Graham: Je voulais savoir s'il y avait un échange de données entre les services. Vous avez votre connexion commune, mais une fois que vous l'avez passée, vous pouvez aller dans différentes bases de données. Les bases de données interagissent-elles?

M. John Weigelt: Là encore, à travers toutes les différentes plateformes, il faudrait que j'examine chaque scénario particulier pour dire généralement qu'il n'y a pas d'échange de données entre...

M. David de Burgh Graham: D'accord.

Vous avez récemment acheté GitHub, une entreprise à code source ouvert, ce que j'ai trouvé très intéressant. Pourquoi?

M. John Weigelt: Nous trouvons que la communauté des partisans du code source ouvert est très dynamique et qu'elle offre un excellent modèle de développement. Ce libre dialogue entre eux, cette discussion libre, va au-delà de la simple conversation sur les logiciels pour englober des projets plus vastes. Nous y avons vu une occasion de collaboration.

Par le passé, vous savez qu'il y avait presque de l'animosité entre nous et les partisans du code source ouvert. Nous avons vraiment adhéré aux concepts du logiciel libre et des données ouvertes pour être en mesure de mieux innover dans le marché.

M. David de Burgh Graham: Je viens moi-même de cette communauté, alors je peux comprendre ce que vous dites.

J'aimerais m'adresser un instant à Mozilla.

Vous avez parlé de meilleures protections contre le pistage en ligne. Diriez-vous qu'il y a une sorte de course aux armements entre pisteurs et contre-pisteurs?

M. Alan Davidson: Malheureusement, oui. Nous sommes très lucides en nous apprêtant à construire cet ensemble de protections contre le pistage en ligne. Nous pensons qu'elles offrent une réelle valeur. Et je lève mon chapeau à nos amis d'Apple. Ils font quelque chose de semblable avec Safari qui est vraiment bon.

Les pisteurs vont trouver d'autres façons de déjouer nos protections, et nous allons devoir en construire de nouvelles. Je pense que cela va durer un certain temps, ce qui est malheureux pour les utilisateurs, mais c'est un exemple de ce que nous pouvons faire pour les protéger.

M. David de Burgh Graham: Compris.

Pour passer à Apple un instant, il y a eu récemment le piratage d'identifiant de capteur qui a été corrigé dans la version 12.2 d'iOS — je ne la connais pas —, qui permettait à n'importe quel site Web dans le monde de suivre n'importe quel iPhone et la plupart des appareils Android en se servant des données de calibrage sensoriel. Vous êtes probablement au courant de cela.

M. Erik Neuenschwander: Oui, c'est l'affaire du pistage par empreinte numérique.

M. David de Burgh Graham: Oui, le pistage par empreinte numérique. Pouvez-vous nous en dire davantage à ce sujet, nous dire comment il a été utilisé et si c'est vraiment corrigé maintenant dans iOS 12.2?

M. Erik Neuenschwander: Je vais commencer par expliquer un peu le contexte. Lorsque nous parlons, disons, de pistage en ligne, il peut y avoir des technologies qui servent expressément à cela, comme les témoins communément appelés *cookies*. Une des évolutions que nous avons observées est la mise au point de ce que nous appelons une empreinte synthétique. Il s'agit simplement d'un numéro unique qui est synthétisé par un tiers, probablement pour essayer de faire du pistage. On s'en sert aussi dans la lutte anti-fraude et pour d'autres usages, mais chose certaine, cela se prête très bien au pistage en ligne.

Vous avez raison. Certains chercheurs, en examinant les variations dans la fabrication des capteurs, ont déterminé qu'il était possible de synthétiser un de ces identifiants uniques. Le pistage par empreinte numérique, tout comme le contre-pistage, va évoluer continuellement et nous sommes déterminés à rester à l'avant-garde. Quant à savoir comment il a été utilisé, je n'ai aucune donnée indiquant qu'il ait même été utilisé, mais je ne peux pas non plus vous assurer qu'il ne l'a pas été.

Nous avons mis en place des mesures d'atténuation dans notre dernière mise à jour, et les chercheurs ont confirmé qu'elles ont bloqué leur version de l'attaque en ligne, mais je répète que c'est une technique qui continue d'évoluer, alors je pèse soigneusement mes mots « mesures d'atténuation ». À moins de retirer les capteurs de l'appareil, il y aura toujours un risque. Nous allons aussi continuer de travailler pour réduire ce risque et garder le dessus.

● (0940)

M. David de Burgh Graham: Il me reste environ 20 secondes. J'ai une autre question pour Apple.

Sur iOS, lorsque vous passez d'une application à l'autre, une application se met en suspens et l'autre s'ouvre. Lorsque vous revenez à l'application originale, si cela fait plus de quelques secondes, elle recharge les données. Est-ce que cela ne donne pas amplement l'occasion de pister vers n'importe quel site Web que vous consultez, en disant que c'est l'usage de l'appareil? Je trouve curieux de faire cela, au lieu de stocker le contenu que vous utilisez.

M. Erik Neuenschwander: Je vais diviser cela en deux parties, je crois bien.

Premièrement, lorsque l'application passe à l'avant-plan et qu'elle peut s'exécuter, elle peut recharger le contenu, si elle juge bon de le faire. À ce moment-là, vous lui avez remis les commandes et elle peut s'exécuter et recharger, si vous voulez.

Notre objectif, en fait, est de réduire au minimum ces recharges dans le cadre de l'expérience utilisateur. Nous voulons aussi que l'application qui se trouve à l'avant-plan obtienne, dans un bac à sable, dans un ensemble de limites que nous avons, le maximum des moyens d'exécution et des autres ressources de l'appareil. Cela peut vouloir dire que le système d'exploitation enlève des ressources aux applications qui se trouvent en arrière-plan.

Pour ce qui est du rechargement que vous voyez, iOS, notre système d'exploitation, pourrait y contribuer, mais au fond, peu importe les ressources qu'on préserve pour celle qui se trouve en arrière-plan, lorsque vous retournez à une application, elle a le contrôle de l'exécution et elle peut recharger si elle le juge bon.

M. David de Burgh Graham: Merci.

Le président: Merci, monsieur Graham.

Nous passons maintenant à mon coprésident, M. Collins.

Allez-y de vos remarques préliminaires. C'est bon de vous revoir.

M. Damian Collins (président, Comité sur le numérique, la culture, les médias et le sport, Chambre des communes du Royaume-Uni): Merci.

Mes excuses, puisque les autres représentants du Royaume-Uni et moi-même n'étions pas ici au début de la séance, mais nous sommes ravis de voir tous les témoins ici présents.

Hier, nous nous sommes concentrés sur certaines plateformes de médias sociaux, mais je pense que notre champ d'intérêt est beaucoup plus vaste et qu'il englobe tout un éventail d'entreprises de technologie.

J'aurais d'abord quelques questions pour Apple.

Lorsque je suis entré, il était question des données recueillies sur la voix. Pourriez-vous me parler un peu du genre de données qu'Apple recueille en ce qui concerne le son capté par ses appareils? Dans le cas des appareils intelligents, est-ce qu'ils captent le son ambiant pour se faire une idée des utilisateurs — peut-être le milieu dans lequel ils se trouvent ou ce qu'ils sont en train de faire lorsqu'ils utilisent l'appareil?

M. Erik Neuenschwander: Pour ce qui est de l'information sur nos appareils qui supportent Siri, il y a une partie de l'appareil qui est toujours à l'écoute. Sur certains de nos appareils, nous l'avons isolée même d'iOS, même de notre système d'exploitation, dans un coprocesseur dédié, essentiellement une pièce de matériel spécialisée, qui n'enregistre ni ne stocke l'information, mais qui est seulement à l'écoute du mot-clé pour activer notre assistant personnel, alors l'information n'est pas conservée dans l'appareil.

Toujours en réponse à votre question, elle n'est pas non plus versée dans un quelconque profil dérivé pour identifier quelque chose en rapport avec le comportement ou les centres d'intérêt de l'utilisateur. Non.

M. Damian Collins: Est-ce que l'appareil recueille de l'information sur l'environnement où on se trouve en ce moment? Disons, par exemple, que je suis dans l'autobus pour me rendre au travail. Est-ce qu'il capterait ce genre de bruit ambiant?

M. Erik Neuenschwander: Elle n'enregistre pas tout. Il y a ce que nous appelons une « période tampon ». Il s'agit essentiellement d'une courte période qui est enregistrée de façon transitoire pour analyser le mot-clé, et qui est ensuite continuellement effacée à mesure que le temps avance. Rien n'est enregistré, sauf les quelques millisecondes éphémères qui permettent d'entendre ce mot-clé.

M. Damian Collins: L'écoute ne sert qu'à passer une commande à Siri.

M. Erik Neuenschwander: C'est exact.

M. Damian Collins: À des fins de développement de produits ou de formation, l'entreprise conserve-t-elle certains de ces renseignements?

M. Erik Neuenschwander: Encore une fois, l'appareil ne conserve même pas ces renseignements. Comme il écoute de façon passagère, ces renseignements sont continuellement effacés. Lorsque l'utilisateur utilise un mot-clé, un apprentissage automatique se fait sur l'appareil en adaptant le modèle audio à l'interlocuteur pour réduire le nombre de faux positifs ou de faux négatifs de ce mot-clé. Ensuite, si l'utilisateur fait appel à Siri, au moment où Siri est interrogée et où l'on communique avec elle débute l'envoi de données à Apple.

M. Damian Collins: Quelle est la portée des données ainsi envoyées?

M. Erik Neuenschwander: La portée des données n'englobe que l'énoncé jusqu'à ce qu'il atteigne un point de terminaison et que Siri estime que l'utilisateur a cessé de parler, ainsi que des renseignements comme le modèle de l'appareil, pour adapter la réponse à l'appareil et un identificateur aléatoire généré par l'appareil, qui est la clé des données détenues par Siri aux fins de vos interactions avec elle. Il s'agit d'un identificateur qui est distinct de votre identificateur Apple et qui n'est associé à aucun autre compte ou service chez Apple.

M. Damian Collins: Est-ce qu'Apple tient un registre de mes demandes à Siri, de mes commandes?

M. Erik Neuenschwander: Oui.

● (0945)

M. Damian Collins: Est-ce que l'entreprise utilise ce registre ou est-il seulement utilisé pour faciliter la réponse à mon appareil?

M. Erik Neuenschwander: Je suppose, en réponse à la deuxième partie de votre question, que cela donne lieu à une certaine forme d'utilisation par l'entreprise. Oui, nous utilisons ces données pour Siri, mais pour Siri seulement.

M. Damian Collins: Pour comprendre ce que sont les objectifs de Siri, ne s'agit-il que de rendre Siri plus sensible à ma voix...

M. Erik Neuenschwander: Oui.

M. Damian Collins: ... ou les données sont-elles conservées par l'entreprise pour établir un profil des demandes des utilisateurs? Conservez-vous des profils de métadonnées des gens selon l'utilisation qu'ils font de Siri?

M. Erik Neuenschwander: Le seul profil de métadonnées que nous avons est celui qui est utilisé pour adapter vos interactions réelles avec Siri. Par exemple, nous formons nos modèles de voix pour qu'ils puissent reconnaître le langage naturel sur le profil sonore. Cela ne sert que pour le volet ou l'expérience Siri. Si vous demandez si les renseignements recueillis permettent d'établir un profil plus large utilisé par l'entreprise pour commercialiser des produits et des services, la réponse est non.

M. Damian Collins: Monsieur Ryland, est-ce qu'Amazon fait cela?

J'aimerais savoir quelle est la différence entre la façon dont Amazon utilise les données recueillies à partir de la voix et la façon dont Apple les utilise. Récemment, un utilisateur a présenté une demande de données qu'Amazon détenait. Cela comprenait une série d'enregistrements de la parole à domicile que l'entreprise utilisait apparemment à des fins de formation. J'aimerais savoir comment Amazon recueille les données vocales et comment elle les utilise.

M. Mark Ryland: L'appareil attend aussi un mot-clé. Il ne stocke aucune donnée ambiante. Une fois interpellé, il commence à acheminer des données vers le nuage pour analyser ce que l'utilisateur demande réellement. Ces données sont stockées; tout cela est expliqué dans le profil de l'utilisateur, qui peut voir tous les énoncés. Il peut voir ce qu'Alexa a cru entendre, le texte de l'interprétation qu'en a fait Alexa. Cela lui permet également de comprendre l'origine des problèmes de communication, et ainsi de suite.

L'utilisateur peut supprimer ces données, individuellement ou collectivement. Nous utilisons les données tout comme nous utilisons les données d'autres interactions concernant le compte de l'utilisateur. Cela fait partie du compte de l'utilisateur Amazon. Cela fait partie de la façon dont il interagit avec notre plateforme globale.

M. Damian Collins: Le représentant d'Apple a dit que l'appareil écoute constamment, mais attend seulement la commande Siri. Il semble que ce soit différent avec Alexa. L'appareil est toujours à l'écoute et il conserve dans le nuage ce qu'il a entendu.

M. Mark Ryland: Non, c'est plutôt très semblable. Nous conservons les énoncés entendus après le mot-clé, tout comme Siri.

M. Damian Collins: Je sais d'expérience qu'Alexa répond à des commandes autres que le mot-clé. Il pourrait être déclenché par quelque chose qu'il a entendu dans la salle et qui n'est pas nécessairement le mot-clé.

M. Mark Ryland: Cela me semble être une défaillance. Alexa n'est pas censée réagir de façon aléatoire aux sons ambiants.

M. Damian Collins: Roger McNamee, qui est venu témoigner devant nous hier, nous a expliqué comment il avait placé Alexa dans une boîte dès le premier jour parce qu'Alexa avait commencé à interagir avec une publicité d'Amazon qui passait à la télévision. Je pense que la plupart des gens qui ont ces appareils savent que toutes sortes de choses peuvent les déclencher, et pas seulement la commande ou le mot-clé d'Alexa.

M. Mark Ryland: Eh bien, nous travaillons sans cesse à raffiner la technologie et à nous assurer que le mot-clé constitue la seule façon dont les gens peuvent interagir avec l'appareil.

M. Damian Collins: Si vous conserviez dans l'appareil les données qu'il entend et les gardiez ensuite dans le nuage — ce qui semble être différent de ce que fait Apple —, vous nous dites que ce ne sont que des données sonores qui sont fondées sur les commandes reçues par Alexa?

M. Mark Ryland: Oui. Ce ne sont que les données créées en réponse à la tentative de l'utilisateur d'interagir avec Alexa, qui est déclenchée par le mot-clé.

M. Damian Collins: Est-ce qu'Amazon serait en mesure de répondre à une demande de données ou de renseignements de la police au sujet d'un crime qui a peut-être été commis à l'intérieur du pays en fonction de paroles captées par Alexa?

M. Mark Ryland: Nous observons évidemment les lois de tous les pays dans lesquels nous opérons. S'il y a une ordonnance exécutoire d'une portée raisonnable et ainsi de suite, nous y donnerons suite comme il se doit.

M. Damian Collins: Cela donne à penser que vous conservez plus de données que de simples commandes à Alexa.

M. Mark Ryland: Non, la seule chose à laquelle nous pourrions répondre, c'est l'information que je viens de décrire, c'est-à-dire les réponses qui viennent de l'utilisateur une fois qu'il a interpellé l'appareil. Il n'y a pas de stockage des données ambiantes.

M. Damian Collins: Vous dites que lorsque quelqu'un interpelle l'appareil, la commande reçue — son dialogue avec Alexa, si vous voulez — est conservée?

M. Mark Ryland: C'est exact.

M. Damian Collins: Vous dites qu'à moins que le mot-clé ne soit prononcé, l'appareil n'est pas déclenché et il ne recueille pas de données ambiantes.

M. Mark Ryland: C'est exact.

M. Damian Collins: D'accord.

Je m'intéresse au cas des données dont j'ai parlé plus tôt. On semblait craindre que le son ambiant soit conservé et enregistré et que l'entreprise l'utilise à des fins de formation.

M. Mark Ryland: Non. Quand j'ai parlé de formation, c'est simplement que nous améliorons nos modèles de traitement du langage naturel en utilisant les données que les clients nous donnent dans le cadre de leur interaction avec l'appareil. Ce n'est pas du tout basé sur le son ambiant.

● (0950)

M. Damian Collins: Tous les commandements d'Alexa qui sont déclenchés par le mot-clé sont donc conservés par l'entreprise dans le nuage. Pensez-vous que vos utilisateurs le savent?

M. Mark Ryland: Je pense que oui. D'après mon expérience de l'utilisation d'un appareil mobile pour configurer l'appareil à la maison, j'ai immédiatement remarqué qu'il y a une icône d'historique, où je peux essentiellement aller prendre connaissance de toutes mes interactions avec le système.

M. Damian Collins: Je ne me souviens pas d'avoir lu cela nulle part. C'est peut-être en raison du feuillet de l'épaisseur de *Guerre et paix*, des instructions qui sont rattachées à l'appareil.

Je pense que même si c'est peut-être la même chose que d'utiliser n'importe quelle autre fonction de recherche, le fait est qu'il parlait à un ordinateur, et je ne suis pas sûr que les utilisateurs savent que cette information est stockée indéfiniment. Je ne savais pas que cela se faisait. Je n'avais aucune idée de la façon dont on s'y prendrait pour le savoir. Je suis également un peu intrigué par le fait qu'il est possible, en fait, de voir la transcription de ce que vous avez demandé à Alexa.

M. Mark Ryland: Oui, c'est exact. C'est dans l'application mobile, sur le site Web et sur la page de confidentialité d'Alexa que vous pouvez voir toutes vos interactions. Vous pouvez voir ce que le système de transcription a cru entendre, et ainsi de suite.

M. Damian Collins: Je présume que tout cela est regroupé dans un ensemble de données qu'Amazon détient à mon sujet en ce qui concerne mes habitudes d'achat et d'autres choses également.

M. Mark Ryland: Cela fait partie des données de votre compte.

M. Damian Collins: Cela représente beaucoup de données.

Le président: M. Davidson veut répondre.

M. Alan Davidson: Je voulais simplement dire que je pense que cela met également en évidence le problème dont nous avons parlé au sujet du consentement.

Je suis un fidèle utilisateur d'Amazon Echo. L'entreprise a conçu un outil formidable. Il y a quelques semaines, je suis allé avec ma famille et nous avons vu les données qui étaient stockées, mais je dois dire que c'est...

La protection de la vie privée est un sujet qui me passionne. J'ai lu tout ce que vous recevez, et j'ai été stupéfait, honnêtement, et ma famille a été étonnée de voir ces données enregistrées de nous et de nos jeunes enfants qui remontent à plusieurs années et qui sont stockées dans le nuage. Cela ne veut pas dire que cela a été fait à tort ou illégalement. Je pense que c'est merveilleux de voir ce genre de transparence, mais les utilisateurs n'en ont aucune idée. Je pense que beaucoup d'utilisateurs ne savent tout simplement pas que ces données existent et ne savent pas non plus comment elles seront utilisées à l'avenir.

Comme industrie, nous devons faire un bien meilleur travail pour ce qui est de demander aux gens un consentement plus précis, ou fournir une meilleure information à ce sujet.

Le président: Oui.

M. Alan Davidson: Je ne veux pas m'en prendre à Amazon; c'est un produit merveilleux.

Le président: Nous passons maintenant à M. Gourde.

Je vois beaucoup de mains se lever. Tout le monde aura beaucoup de temps aujourd'hui.

Monsieur Gourde, vous avez cinq minutes.

[*Français*]

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

Ma question va toucher un sujet d'ordre un peu plus technique.

Vous possédez, surtout Amazon et les autres organisations semblables, beaucoup de renseignements et de données personnelles concernant vos clients.

Je suis convaincu que vous faites l'impossible pour sécuriser toutes ces données. Par contre, compte tenu de l'avènement de l'intelligence artificielle, vous avez peut-être eu des offres de service afin de vous aider à prévoir le marché dans l'avenir.

Cela pourrait être très utile — surtout pour Amazon — d'être capable de prévoir, supposons pour l'été prochain, quel article parmi ceux qui ont été commandés pourrait faire l'objet d'un rabais, être mis en solde.

Il y a peut-être des sous-traitants ou des personnes qui vous ont offert des services en ce qui a trait aux nouveaux systèmes d'algorithmes. Au fond, ils vous auraient vendu cela pour vous aider.

Est-ce que ces sous-traitants, si vous y faites appel — bien sûr, vous n'êtes pas obligé de nous le dire —, peuvent garantir que, en utilisant les données détenues par votre entreprise pour offrir ce genre de service, ils ne vont pas vendre ces renseignements personnels à d'autres personnes ou à des organisations plus importantes? Ces dernières seraient très heureuses d'obtenir ces informations, que ce soit pour vendre de la publicité ou à d'autres fins.

Y a-t-il des organisations qui vous offrent ce genre de service?

[*Traduction*]

M. Mark Ryland: Nous concluons des marchés avec des tiers pour la prestation de certains services et, dans des conditions très prudemment contrôlées, nous partageons des données personnelles.

Par exemple, si nous concluons un marché avec un service de livraison, nous communiquons le nom et l'adresse du client où le colis doit être livré, mais je pense que pour tous ces cas d'apprentissage automatique de base du genre dont vous parlez, tout cela ne concerne que notre entreprise. Nous ne vendons pas l'accès aux données de base aux entreprises avec lesquelles nous traitons aux fins des services que nous offrons. Ce partage de données ne se fait que dans des cas d'utilisation périphérique, et même dans ces cas, nous conservons des droits de vérification et nous contrôlons soigneusement, par l'entremise de contrats et de vérifications, l'utilisation que font nos sous-traitants des données de nos clients que nous partageons avec eux à ces fins très limitées.

● (0955)

[*Français*]

M. Jacques Gourde: Y a-t-il d'autres organisations qui utilisent des stratégies d'algorithmes pour mousser vos produits?

[*Traduction*]

M. John Weigelt: Nous appliquons chez Microsoft un très solide modèle de gouvernance des données qui nous permet de reconnaître et de marquer les données et de les protéger comme il se doit. Dans les secteurs où nous avons besoin de sous-traitants, leur nombre demeure très limité.

Il y a beaucoup de décisions à prendre avant que nous choisissions nos sous-traitants, et ils doivent conclure des ententes avec nous pour assurer la confidentialité des données qu'ils sauvegardent. Nous avons des règles strictes concernant la façon dont ils utilisent ces données et les conditions dans lesquelles ils doivent nous les renvoyer. Nous avons un programme très solide de politiques, de procédures et de mesures de sécurité techniques concernant l'utilisation des données par les sous-traitants pour veiller à ce qu'elles ne soient pas utilisées à mauvais escient.

L'intelligence artificielle est un domaine qui nous intéresse au plus haut point, et Satya Nadella, dans son livre intitulé *Hit Refresh*, a certes établi des principes d'utilisation judicieuse de l'intelligence artificielle afin de responsabiliser les gens. C'est vraiment le premier principe. Nous avons adopté ces principes au sein de notre organisation, en veillant à établir une structure de gouvernance robuste en matière d'intelligence artificielle. Nous avons mis sur pied un comité qui examine l'application de l'IA à l'intérieur et à l'extérieur de l'organisation pour s'assurer que nous l'utilisons de façon responsable.

La mise en place de ces éléments dans l'organisation nous aide à mieux gérer et comprendre la façon dont ces outils sont utilisés et à les mettre en place dans un cadre conforme à l'éthique. Nous sommes très heureux de collaborer avec des gouvernements partout dans le monde, que ce soit l'Union européenne avec ses travaux dans le domaine de l'éthique de l'intelligence artificielle ou les récentes lignes directrices de l'OCDE, ou même ici au Canada avec les travaux du Conseil stratégique des DPI, le CSDPI, sur un cadre déontologique de l'intelligence artificielle, afin que nous puissions aider les gens et d'autres organisations à mieux comprendre certaines de ces techniques, des processus et des modèles de gouvernance responsables qui doivent être mis en place.

M. Erik Neuenschwander: Je ne sais pas si Apple fait le genre de modélisation dont vous parlez. Au lieu de cela, notre apprentissage automatique a tendance à être basé sur l'intelligence des appareils.

Par exemple, à mesure que le clavier apprend à connaître l'utilisateur, l'appareil lui-même recueille et utilise cette information pour s'entraîner à reconnaître cet utilisateur sans que l'information ne quitte l'appareil. Lorsque nous recueillons des données pour aider à éclairer les modèles communautaires, nous appliquons des critères comme la protection de la vie privée différentielle locale, qui applique la randomisation aux données avant qu'elles quittent l'appareil de l'utilisateur, de sorte que nous ne sommes pas en mesure de revenir en arrière et de relier les données de l'utilisateur et leur contenu à un utilisateur. Pour nous, tout est centré sur l'appareil.

[*Français*]

M. Jacques Gourde: Monsieur Davidson, voulez-vous ajouter quelque chose?

[*Traduction*]

M. Alan Davidson: Nous ne déployons aucun de ces systèmes. Dans le cadre de certaines de nos recherches, nous avons également examiné la possibilité de faire des expériences sur des appareils. Je pense que c'est une approche très solide pour protéger la vie privée des gens.

Le président: Merci, monsieur Gourde.

Nous allons maintenant entendre M. Ian Lucas, du Royaume-Uni.

M. Ian Lucas (membre, Comité sur le numérique, la culture, les médias et le sport, Chambre des communes du Royaume-Uni): Si je peux revenir à la question de M. Collins, j'ai été intrigué par le téléphone Apple et l'appareil Alexa. Y a-t-il eu des tentatives de piratage de vos systèmes et d'accès à l'information que vous conservez?

M. Erik Neuenschwander: Les systèmes d'Apple sont constamment attaqués. Je ne sais pas exactement si l'application Siri en soi a été l'objet d'attaques ou non, mais on peut supposer qu'elle l'a été. Cependant, étant donné que les données de Siri ne sont pas associées à l'ensemble du compte Apple, même si nous les considérons comme très sensibles et que nous nous efforçons de les protéger, il serait très difficile pour une personne mal intentionnée de recueillir les données d'un utilisateur individuel à partir du système Siri.

M. Ian Lucas: A-t-on déjà réussi à pirater le système en ce qui concerne une personne en particulier?

M. Erik Neuenschwander: Pas à ma connaissance, non.

M. Mark Ryland: De même, nous protégeons les données des clients avec beaucoup de succès depuis plus de 20 ans. Il s'agit d'un nouveau type de données, de toute évidence d'un type très sensible, mais nous conservons un dossier très positif à cet égard, et rien n'indique qu'il y ait eu quelque violation que ce soit à l'égard des données liées à Alexa.

Le président: Nous cédons maintenant la parole à M. Lawless, pour cinq minutes.

M. James Lawless: Merci.

Pour revenir à la sécurité, à la confidentialité des données et au cryptage, je crois qu'Apple a parlé du Key Store sur l'iPhone et l'iPad, et Mozilla, je crois, offre aussi une fonction de type Key Store dans son navigateur.

L'une des difficultés en matière de sécurité, c'est que nos mots de passe, selon moi, sont devenus tellement sûrs que personne ne les retient, sauf les appareils eux-mêmes. Sur le Key Store d'Apple — je crois qu'on l'appelle l'application Key Store —, vous pouvez demander à l'application de générer un mot de passe pour vous, puis lui demander de s'en souvenir pour vous. Vous ne savez pas ce que c'est, mais l'application et l'appareil le savent, et je suppose que cette information est stockée dans le nuage quelque part. Je sais que vous en avez présenté un aperçu au début.

Je suppose que Mozilla a une fonction semblable qui permet de demander à la plateforme de se souvenir du mot de passe pour vous, donc vous avez plusieurs mots de passe, et je pense que Microsoft offre aussi probablement cette fonction dans ses navigateurs. Encore une fois, si vous ouvrez une session dans Mozilla, Edge ou n'importe quel navigateur, vous pouvez remplir automatiquement tous vos champs de mot de passe. Nous nous retrouvons dans une situation comme celle du *Seigneur des anneaux*, où il n'existe qu'« un anneau pour tous ». Dans nos tentatives pour améliorer la sécurité, nous nous sommes retrouvés avec un seul maillon dans la chaîne, et ce maillon est assez vulnérable.

Peut-être, pourrais-je obtenir des commentaires sur ce problème particulier de toutes les plateformes.

● (1000)

M. Erik Neuenschwander: Je crois que l'application dont vous parlez est l'application Keychain Access sur les appareils Mac et iOS. Dans les « réglages », « mots de passe » et « comptes », vous pouvez voir les mots de passe. Comme vous le dites, ils sont générés automatiquement par la plateforme. La plupart des utilisateurs en font l'expérience grâce à notre navigateur Safari, qui offre une fonction de connexion à Keychain. Comme vous le dites, l'information est stockée dans le nuage.

Elle est sauvegardée dans le nuage et cryptée de bout en bout — je tiens à le préciser — au moyen d'une clé qu'Apple n'a jamais en sa possession. Même si nous plaçons cette information dans le nuage, à la fois pour vous permettre de récupérer les mots de passe et de les synchroniser entre tous les appareils que vous avez connectés à iCloud, nous le faisons d'une manière qui n'expose pas vos mots de passe à Apple.

Vous avez raison de dire que les mots de passe continuent de poser un défi en ce qui concerne la protection des comptes d'utilisateur. On voit beaucoup d'entreprises, notamment Apple, passer à ce qu'on appelle l'authentification à deux facteurs, où le simple mot de passe n'est pas suffisant pour accéder au compte. Nous sommes très favorables à cela. Nous avons pris un certain nombre de mesures au fil des ans pour faire passer nos comptes iCloud à ce niveau de sécurité, et nous estimons que c'est un bon progrès pour l'industrie.

La dernière chose que j'aimerais préciser, c'est que les données des mots de passe sont extrêmement délicates et méritent notre plus haut niveau de protection. C'est pourquoi, à part l'application Keychain Access dont vous parlez sur le Mac, sur nos dispositifs iOS et maintenant sur notre T2 — c'est le nom de la puce de sécurité dans certains de nos plus récents appareils Mac —, nous utilisons la technologie de l'enclave sécurisée pour protéger ces mots de passe et les séparer du système d'exploitation. Comme la surface d'attaque est plus petite, même si c'est un risque auquel nous sommes très attentifs, nous avons pris des mesures, à l'étape de la conception matérielle, pour protéger les données entourant les mots de passe des utilisateurs.

M. Alan Davidson: C'est une excellente question. J'ajouterais simplement que cela semble contre-intuitif, n'est-ce pas? Il y a à peine 10 ans, nous aurions dit: « C'est fou. Vous allez mettre tous vos mots de passe au même endroit? » Nous offrons un produit semblable — Lockwise — sur notre navigateur.

Aujourd'hui, les experts en sécurité vous diront que c'est une bien meilleure solution pour la plupart des gens parce que le plus gros problème que nous avons tous est que nous ne pouvons pas nous souvenir de nos mots de passe, alors nous finissons par utiliser le même mot de passe partout, ou nous finissons par utiliser des mots de passe idiots partout, et c'est là que débutent nos problèmes.

Nos propres sondages d'experts en sécurité et nos propres experts internes ont dit qu'il est en fait beaucoup plus intelligent d'utiliser un gestionnaire de mots de passe. Pour la plupart d'entre nous, cela réduit sensiblement la menace de cette vulnérabilité centrale. Je vous encourage donc tous à utiliser des gestionnaires de mots de passe.

Je viens d'envoyer une note à tous nos employés pour leur dire qu'ils devraient le faire. Nous prenons tous cela très au sérieux. L'authentification à deux facteurs est un élément important, et c'est un élément important du fonctionnement de ces gestionnaires. Nous prenons très au sérieux la responsabilité de protéger nos informations, mais il s'avère qu'il s'agit d'une bien meilleure solution pour la plupart des consommateurs aujourd'hui.

M. John Weigelt: J'aimerais ajouter que nous constatons que les protections matérielles locales fondées sur le cryptage sont importantes pour appuyer la protection des mots de passe. Jumelez ces protections à l'authentification multifactorielle, en utilisant peut-être quelque chose que vous possédez déjà.

Je pense qu'un contrepoint intéressant à cela et un ajout intéressant est la capacité de prendre des décisions très solides au sujet des personnes, au sujet de leur utilisation d'un système en particulier. Nous utilisons des données anonymes et pseudonymes pour aider les organisations à reconnaître que « Jean-Pierre se connecte à partir d'Ottawa, et il semble y avoir au même moment une ouverture de session à partir de Vancouver. Il ne peut pas voyager aussi vite. Avertissons Jean-Pierre qu'il est peut-être temps de rafraîchir son mot de passe. »

Il y a une autre chose que nous pouvons faire, compte tenu de la portée mondiale de notre vision de l'environnement des cybermenaces. Souvent, les utilisateurs malveillants partagent des dictionnaires de noms d'utilisateur et de mots de passe. Nous consultons ces dictionnaires, et nous sommes en mesure d'éclairer nos outils de sorte que si les organisations — par exemple, food.com — découvrent qu'un de leurs noms d'utilisateurs y figure, elles peuvent aussi s'en occuper.

Dans le cas des données associées à l'utilisation d'un ensemble d'outils particulier, l'anonymat et le pseudonymat fournissent une plus grande assurance de protection de la vie privée et de sécurité également. Assurons-nous de reconnaître qu'il y a un équilibre à trouver pour nous assurer de préserver la vie privée tout en protégeant ces utilisateurs.

● (1005)

M. James Lawless: C'est un domaine très intéressant, et les défis y demeurent nombreux. Il y a un compromis à faire entre la convivialité et la sécurité.

Je me souviens qu'un gestionnaire de la sécurité des TI d'une grande société m'a parlé d'une politique qu'il avait mise en œuvre avant l'avènement des gestionnaires de mots de passe, il y a peut-être une décennie. Il avait mis en place une politique de mots de passe robustes afin que tout le monde ne puisse pas utiliser son animal domestique ou son lieu de naissance, et ainsi de suite. Il a ensuite constaté que, même si cette politique était appliquée, tout le monde écrivait ses mots de passe sur papier parce qu'il n'y avait aucun moyen de s'en souvenir, ce qui était contre-productif.

J'ai une dernière question, puis je vais ensuite partager mon temps avec ma collègue. Je pense qu'il y a un site Web appelé haveyoubeenhacked.com ou haveibeenhacked — quelque chose du genre — qui enregistre essentiellement les atteintes connues. Si vos données, vos plateformes ou d'autres applications ou sites de tiers se trouvent dans le nuage et sont compromis, vous pouvez faire une recherche pour vous-même ou pour obtenir vos détails et les retirer.

Y a-t-il moyen de remédier à cela? J'ai fait le test récemment, et je crois qu'il y avait quatre sites différents sur lesquels mes détails avaient été divulgués. Si cela se produit sur vos plateformes, comment allez-vous procéder? Comment pouvez-vous atténuer cela? Vous contentez-vous simplement d'informer les utilisateurs? Faites-vous de la sensibilisation ou essayez-vous d'effacer cet ensemble de données et de recommencer? Que se passe-t-il dans un tel cas?

M. John Weigelt: Nous avons des exigences et des obligations en matière de notification des atteintes, et nous avisons nos utilisateurs s'il y a un soupçon d'atteinte à leur information et nous leur recommandons de changer leur mot de passe.

Pour ce qui est de l'ensemble organisationnel, comme la trousse d'outils dont j'ai parlé — je pense que c'est « Have I been pwned »...

M. James Lawless: C'est bien cela.

M. John Weigelt: ... ce site a des dictionnaires facilement accessibles, alors nous les transmettons également aux utilisateurs organisationnels. Il y a la notification des utilisateurs individuels, et nous aidons également les entreprises à comprendre ce qui se passe.

M. Alan Davidson: Nous faisons la même chose en ce sens que nous avons tous des obligations en matière d'atteinte à la protection des données et nous nous en acquittons dans de tels cas. Nous avons également mis au point notre propre version Firefox de ce surveillant « Have I been hacked ». Les titulaires de compte Firefox qui choisissent d'y adhérer seront avisés des autres attaques dont nous sommes informés, pas seulement de n'importe quelle atteinte à notre système, mais à d'autres également. Ce sera un service que les gens trouveront fort utile.

M. James Lawless: C'est bien.

M. Erik Neuenschwander: Si les équipes de sécurité d'Apple, en plus des étapes dont il a été question ici, apprennent qu'il y a probablement eu violation d'un compte, alors nous pouvons prendre une mesure qu'on appelle la « réinitialisation automatisée » du compte. Nous obligerons en fait l'utilisateur à réinitialiser son mot de passe et lui poserons des défis supplémentaires s'il a une authentification à deux facteurs à l'aide de ses dispositifs de confiance existants pour rétablir l'accès à ce compte.

M. James Lawless: Oui, il est très difficile de revenir à notre compte une fois qu'on en est évincé, et je le sais pour l'avoir vécu.

Des voix: Oh, oh!

M. Erik Neuenschwander: Vous avez parlé d'équilibre entre la convivialité et la sécurité.

M. James Lawless: Oui.

M. Erik Neuenschwander: Nous essayons de trouver un équilibre entre la possibilité que vous soyez la bonne personne qui essaie de récupérer son compte, auquel cas il ne faut pas exagérément vous compliquer la vie, ou nous essayons de garder un utilisateur malveillant définitivement à l'écart. C'est un domaine en évolution.

Mme Hildegarde Naughton: Puis-je intervenir, s'il vous plaît?

Le président: Nous avons en fait largement dépassé le temps prévu. Le président passera au deuxième tour, et vous êtes déjà inscrite en premier au deuxième tour, Hildegarde. Lorsque tout le monde aura pris la parole, nous passerons à la prochaine série de questions. Cela ne devrait pas être très long.

Nous passons maintenant à Mme Vandenbeld, pour cinq minutes.

Mme Anita Vandenbeld (Ottawa-Ouest—Nepean, Lib.): Merci beaucoup.

J'aimerais d'abord parler de la désuétude du consentement. Quand on veut utiliser une application ou autre chose, il y a de bonnes et de mauvaises fins. Disons, par exemple, que j'utilise mon iPhone et que je quitte le Parlement à 9 h. Mon iPhone me dit exactement quelle route prendre pour me rendre à la maison. Il sait où je vis parce qu'il a vu que j'emprunte cette voie tous les jours, et si je commence soudainement à emprunter une voie différente pour me rendre à un autre endroit, il le saura aussi.

Bien, c'est parfait quand je veux savoir si je devrais ou non prendre l'autoroute 417, mais le fait que mon téléphone sache exactement où je dors tous les soirs pourrait aussi être très troublant pour beaucoup de gens.

Nous n'avons pas vraiment le choix. Si nous voulons utiliser certains services, si nous voulons avoir accès à Google Maps ou à autre chose du genre, nous devons accepter, mais il y a alors d'autres utilisations de ces données.

Soit dit en passant, en ce qui concerne le fait qu'il s'agit d'une audience publique, il y a une enseigne sur le mur qui le précise. J'aimerais bien qu'il y ait une telle enseigne lorsqu'on effectue des recherches sur Internet pour savoir si ce qu'on fait sera enregistré ou rendu public.

Ma question, qui s'adresse particulièrement à Apple, porte sur les données que vous recueillez sur mes allées et venues. Il ne s'agit pas seulement de savoir où je vais ce jour-là. Le problème ne réside pas dans le fait de savoir si je veux aller du point A au point B et de savoir quel autobus je dois prendre; le problème, c'est que mon appareil sait exactement où je me trouve sur le plan géographique.

Lesquelles de ces données sont sauvegardées et à quelles autres fins pourraient-elles être utilisées?

● (1010)

M. Erik Neuenschwander: J'aimerais avoir plus de précisions, madame, à savoir de qui et de quoi vous parlez, parce qu'il y a des nuances à faire ici. « L'appareil » — votre téléphone — sait effectivement tout cela. Votre téléphone recueille des données de capteurs et des tendances comportementales et il essaie de déterminer où se trouve votre maison — et c'est votre iPhone. Quand vous dites « vous » en parlant d'Apple, sachez que nous n'avons pas cette information, ou du moins pas par ce processus. Si vous nous laissez une adresse de facturation pour des achats ou autre chose du genre, c'est différent, mais l'information qui améliore l'intelligence de votre iPhone demeure sur votre téléphone et Apple ne la connaît pas.

Lorsque vous demandez dans quelle mesure ces données sont recueillies, sachez qu'elles sont recueillies par le téléphone. Elles sont recueillies sous la fonction « lieux importants ». Les utilisateurs peuvent aller les chercher et les supprimer, mais la collecte ne concerne que l'appareil. Ce n'est pas Apple qui recueille cette information.

Pour ce qui est des fins auxquelles elle peut être utilisée, d'une version à l'autre du système d'exploitation, nous essayons d'utiliser cette information pour fournir de bonnes expériences locales sur l'appareil, comme les avis de moment du départ ou les avis d'accidents de la circulation sur votre trajet vers le domicile, mais cela ne va pas s'étendre à des fins auxquelles Apple, l'entreprise, pourrait utiliser ces données, parce que ces données ne sont jamais en notre possession.

Mme Anita Vandenbeld: Je pense que cela revient à ce que Microsoft a commencé à dire dans sa déclaration préliminaire, c'est-à-dire la capacité des pirates informatiques d'accéder aux données. Apple n'utilise pas ces données, mais est-il possible, grâce aux cybermenaces, que d'autres utilisateurs malveillants puissent accéder à ces données?

Je vais en fait poser la question à Microsoft.

Vous avez parlé d'investir 1 milliard de dollars par année dans la recherche et le développement en matière de sécurité, et vous avez utilisé l'expression « démantèlements coopératifs de réseaux de zombies ». Pouvez-vous m'en dire plus à ce sujet, et aussi parler de votre travail en matière de cybercriminalité?

Nous savons qu'une fois que les données sont divulguées, il est impossible de revenir en arrière, et puisque bon nombre de ces Cambridge Analytica et autres agrégateurs de données les utilisent, que faites-vous pour vous assurer que ces données ne sont pas diffusées au départ?

M. John Weigelt: Lorsque nous examinons le marché, nous constatons qu'il évolue continuellement, n'est-ce pas? Ce qui a été mis en place pour les contrôles de sécurité il y a 10 ans est différent aujourd'hui, et cela fait partie des efforts déployés par la collectivité pour protéger l'environnement des TI.

Dans notre cas, nous analysons ces techniques courantes. Nous essayons ensuite de nous assurer que ces techniques disparaissent. Nous n'essayons pas seulement de suivre; nous essayons de devancer les utilisateurs malveillants afin qu'ils ne puissent pas répéter leurs exploits antérieurs et qu'ils doivent trouver de nouvelles façons de faire.

Nous examinons des outils comme le cryptage, le renforcement du fonctionnement du système d'exploitation, pour que les choses ne se passent pas toujours au même endroit. C'est un peu comme si vous changiez d'itinéraire lorsque vous rentrez chez vous du Parlement le soir, de sorte que si des malfaiteurs vous attendent à l'angle de Sparks et Bank, ils ne vous auront pas parce que vous avez changé d'itinéraire. Nous faisons la même chose au sein du système interne, et cela rompt avec tout un tas de choses que fait la communauté des pirates traditionnels. Comme nous incluons également la protection de la vie privée et l'accessibilité, notre travail porte sur la confiance, la sécurité, la protection des renseignements personnels et l'accessibilité.

Parallèlement, comme il existe une plus vaste communauté Internet dans son ensemble, ce n'est pas quelque chose que nous pouvons faire seuls. Il y a des fournisseurs de services Internet, des sites Web et même des ordinateurs à domicile qui sont contrôlés par ces réseaux de zombies. Les pirates informatiques ont commencé à créer des réseaux d'ordinateurs qu'ils partagent pour commettre leurs méfaits. Ils peuvent avoir jusqu'à un million d'ordinateurs zombies qui attaquent différentes communautés. Cela ralentit vraiment l'Internet, embourbe le trafic sur la Toile et ainsi de suite.

Pour démanteler ces réseaux, il faut un savoir-faire technique pour en prendre le contrôle, mais il faut aussi l'appui des entités juridiques dans les régions. Ce qui est unique pour nous, c'est que notre centre de cybercriminalité a collaboré avec les autorités gouvernementales pour trouver de nouveaux précédents juridiques qui permettent de supprimer ces réseaux. Ainsi, en plus de l'aspect technologique, nous nous assurons d'être en règle sur le plan juridique pour mener nos activités.

Enfin, ce que nous avons fait pour les réseaux Zeus et Citadel, d'importants réseaux de zombies qui s'étaient installés dans les systèmes d'entreprises canadiennes, c'est collaborer avec le Centre canadien de réponse aux incidents cybernétiques ainsi qu'avec les entreprises pour désinfecter ces appareils afin qu'ils puissent redémarrer sans problème.

Mme Anita Vandenbeld: Monsieur Davidson, avez-vous quelque chose à ajouter?

M. Alan Davidson: J'ai deux points à soulever rapidement.

Premièrement, nous travaillons à ce que nous appelons l'« allègement des données ». Cette idée part du principe que nous ne devrions pas conserver les données dont nous n'avons pas besoin. La meilleure façon de protéger les données est de ne pas les conserver. Parfois, c'est nécessaire, mais parfois ce ne l'est pas. L'industrie pourrait faire un meilleur travail et les consommateurs pourraient en apprendre davantage sur l'importance d'insister pour que les données ne soient pas conservées si elles ne sont pas nécessaires.

Deuxièmement, l'emplacement est un aspect particulièrement délicat. C'est probablement un aspect qui, au bout du compte, exigera davantage d'attention de la part du gouvernement. De nombreux utilisateurs se sentiraient probablement très à l'aise qu'une société comme Apple ou Microsoft détienne ces données, parce qu'ils ont d'excellents experts en sécurité et ce genre de choses. Nous nous inquiétons beaucoup des petites entreprises et des tierces parties qui détiennent certaines de ces données et qui ne travaillent peut-être pas de façon aussi sûre.

● (1015)

Le président: Nous allons passer à Mme Jo Stevens, du Royaume-Uni.

Mme Jo Stevens (membre, Comité sur le numérique, la culture, les médias et le sport, Chambre des communes du Royaume-Uni): Merci, monsieur le président.

J'aimerais aborder un sujet tout à fait différent, celui de la concurrence et des marchés. J'aimerais demander à messieurs Ryland et Neuenschwander s'ils pensent que des règles en matière de concurrence et des règles antitrust différentes devraient s'appliquer aux géants de la technologie, compte tenu de leur influence et de leur pouvoir sans précédent sur le marché.

M. Erik Neuenschwander: En ce qui concerne les règlements antitrust, comme je travaille au sein d'une organisation d'ingénierie, je ne peux pas dire que j'ai beaucoup réfléchi à cette question. Je serai heureux de répondre à vos questions et de les soumettre à nos équipes des affaires juridiques ou gouvernementales.

Mme Jo Stevens: Comme consommateur, pensez-vous que les grands géants technologiques mondiaux ont trop d'influence et de pouvoir sur le marché?

M. Erik Neuenschwander: Mon objectif, en ce qui concerne nos plateformes, est de permettre à l'utilisateur de contrôler les données et de laisser le plus de contrôle possible aux utilisateurs.

M. Mark Ryland: Nous sommes une entreprise relativement importante, mais bien sûr, c'est en grande partie le résultat de nos activités à l'échelle mondiale. Nous évoluons dans beaucoup de marchés différents. Dans un segment de marché donné, nous pouvons souvent être un très petit joueur ou un joueur de taille moyenne.

Encore une fois, je ne vais pas me prononcer en profondeur au sujet des lois sur la concurrence. Ce n'est pas mon domaine d'expertise, mais nous estimons que la loi actuelle sur la concurrence est suffisante en ce qui a trait aux sociétés de technologie.

Mme Jo Stevens: Monsieur Weigelt, qu'en pensez-vous?

M. John Weigelt: Nous sommes sur le marché depuis pas mal de temps, depuis les années 1970, en fait, nous avons donc eu le temps de réfléchir à l'organisation et la manière dont nous exerçons nos activités. Je pense que nous avons apporté les correctifs nécessaires, en nous appuyant sur les commentaires et les points de vue des gouvernements étrangers.

Une chose qui me semble importante à signaler, en tant que Canadien travaillant pour Microsoft ici au Canada, c'est cet écosystème de partenaires qui stimule l'innovation canadienne et les entreprises canadiennes. Plus de 12 000 partenaires tirent leurs revenus grâce à l'ensemble d'outils à leur disposition et ont accès à une plateforme cohérente, ce qui leur permet de vendre leurs innovations dans le monde entier grâce à ces outils et de multiplier les revenus qu'ils génèrent ici au pays.

Les progiciels permettent parfois de multiplier les revenus par huit. Pour l'infonuagique, le facteur de multiplication peut être aussi élevé que 20 pour l'utilisation de ces ensembles d'outils. Il s'agit donc d'un moteur économique fantastique. Cet accès au marché mondial est un atout important pour nos partenaires.

Mme Jo Stevens: Cela m'amène à ma prochaine question. Je pense que c'est une idée largement répandue que les géants mondiaux de la technologie sont un peu comme un service public et qu'ils devraient être traités à ce titre en raison du pouvoir qu'ils détiennent.

Compte tenu de ce que vous venez de dire au sujet de l'innovation, croyez-vous que, si c'était le cas et si la pression antitrust était plus forte, cela pourrait nuire à l'innovation? Est-ce la principale raison que vous invoquez?

M. John Weigelt: Je faisais un lien entre ces deux sujets. Ce que je voulais dire, c'est que nous démocratisons la technologie. Nous la simplifions grandement pour les pays émergents et les entreprises émergentes et nous leur donnons des idées fantastiques pour tirer parti d'une technologie très avancée. Quand on pense à l'intelligence artificielle et au travail qui se fait à Montréal, à Toronto et ailleurs dans le monde, il est essentiel que nous puissions utiliser ces outils pour créer un nouveau marché.

Je vois cela comme un catalyseur pour le milieu de l'innovation. Nous collaborons avec cinq supergrappes canadiennes, qui sont le moteur de l'innovation du Canada dans les domaines de l'agriculture, des océans, de la fabrication de pointe, pour créer de nouveaux ensembles d'outils. Notre capacité d'interagir avec ces différents secteurs, d'adopter des approches multiplateformes et d'optimiser notre expérience sur une plateforme leur permet de s'engager dans des activités qui sont dans le meilleur intérêt du milieu.

Par exemple, dans la supergrappe de l'économie océanique, utiliser et obtenir des données sur nos océans et partager ce produit commun avec l'ensemble du secteur, c'est une pratique que nous encourageons afin de stimuler la croissance du secteur. Faciliter l'accès à cette plateforme est un moyen de stimuler l'innovation.

● (1020)

Mme Jo Stevens: Pourriez-vous nous parler de l'innovation du point de vue de votre entreprise? Ma question s'adresse à vous deux.

M. Mark Ryland: Oui, avec plaisir.

La concurrence est très forte sur tous les marchés où nous sommes présents. L'infonuagique est un excellent exemple. Les joueurs ne sont pas très nombreux sur ce marché, mais la concurrence est très forte et les prix sont en baisse, ce qui facilite, comme l'a dit mon collègue, l'émergence de nouveaux modèles d'affaires qui étaient auparavant impensables.

J'ai travaillé quelques années à la division des organismes du secteur public chez Amazon Web Services. Ce que j'y ai constaté, c'est que de très petites entreprises, disons de 10, 20 ou 30 employés, étaient en concurrence pour l'obtention de gros contrats gouvernementaux, ce qui aurait été impensable pour elles avant l'existence de l'infonuagique. Seule une très grande entreprise spécialisée dans les contrats gouvernementaux aurait pu soumissionner pour ces gros contrats, parce qu'il fallait qu'elle soit dotée d'une solide infrastructure et qu'elle soit en mesure de faire d'importants investissements en capital.

Comme il est maintenant possible d'obtenir de nombreux services de TI à partir du nuage, nous assistons à une fantastique démocratisation, pour reprendre ce mot, de l'accès au marché international, de l'accès des petits commerces au marché international, que ce soit en vendant sur le site de vente au détail d'Amazon ou au moyen de notre plateforme infonuagique. Je pense que la concurrence est vraiment renforcée parce que certains de ces joueurs de grande envergure permettent aux consommateurs d'avoir accès à une gamme plus vaste de marchés.

Mme Jo Stevens: Mais ils doivent passer par vous, n'est-ce pas? Autrement, comment feraient-ils?

M. Mark Ryland: Non, ils peuvent y accéder par notre entremise ou celle de nos concurrents.

Mme Jo Stevens: Mais les concurrents ne sont pas si nombreux, n'est-ce pas?

M. Mark Ryland: Ils ne sont pas nombreux, mais la concurrence est féroce.

Mme Jo Stevens: Il me semble un peu bizarre que vous ayez si peu de concurrents, même si la concurrence est féroce. Ce n'est pas ce que j'aurais normalement imaginé.

Et vous, monsieur Neuenschwander?

M. Erik Neuenschwander: Je ne m'y connais pas beaucoup en matière de législation, mais il semble très difficile de légiférer dans ce domaine. Je suppose que l'objectif d'une loi n'est pas de freiner l'innovation ni d'imposer une limite à ce que les entreprises peuvent faire, mais plutôt d'encourager les bons comportements.

Mme Jo Stevens: D'accord, merci.

Le président: Merci, madame Stevens.

Monsieur Saini, c'est maintenant à vous. Vous avez cinq minutes.

M. Raj Saini (Kitchener-Centre, Lib.): Bonjour à tous.

Vous connaissez tous, j'en suis certain, l'expression « monopole de données ». Nous avons devant nous Apple, qui contrôle un logiciel populaire d'exploitation mobile. Nous avons Amazon, qui contrôle la plus importante plateforme commerciale en ligne. Nous avons également Microsoft, qui a la capacité d'acquérir une foule de données et de les utiliser pour s'imposer sur les marchés.

Au sujet de la concurrence, je veux aller plus loin que Mme Stevens. Si nous regardons du côté de l'Union européenne, nous voyons qu'Apple a violé les règles de l'UE relatives aux aides d'État lorsque l'Irlande lui a accordé des avantages fiscaux indus de 13 milliards d'euros. Dans certains cas, vous avez payé beaucoup moins d'impôts, ce qui vous donnait un avantage.

Dans le cas d'Amazon, la Commission européenne a jugé anti-concurrentielle la clause de la nation la plus favorisée des contrats d'Amazon et le Luxembourg a accordé à Amazon des avantages fiscaux illégaux d'une valeur d'environ 250 000 millions d'euros.

Mon intention n'est pas de vous mettre dans l'embarras, mais il y a manifestement un problème de concurrence. Ce problème est attribuable à l'existence d'une diversité de régimes ou de lois en matière de concurrence, que ce soit en Europe, à la FTC des États-Unis, ou au Canada. La loi européenne sur la concurrence prévoit l'imposition d'un droit spécial aux acteurs dominants du marché. La situation est différente aux États-Unis parce que les mêmes infractions n'ont pas été sanctionnées. Selon vous, est-ce une mesure qui devrait être envisagée, étant donné que vous êtes en position dominante sur le marché?

M. Mark Ryland: Je le répète, je ne suis pas un expert en droit de la concurrence, mais je vous assure que nous nous conformons aux lois des pays et des régions où nous exerçons nos activités et que nous continuerons à le faire.

M. Raj Saini: Si la Commission européenne a imposé une amende à Amazon, c'est donc que vous n'avez pas vraiment respecté la loi.

Ma question porte sur le droit spécial imposé en vertu de la loi européenne sur la concurrence aux entreprises en position dominante sur le marché. Selon vous, les États-Unis et le Canada devraient-ils faire la même chose?

M. Mark Ryland: Je vais devoir vous revenir sur ce point. Je ne suis pas un expert en la matière. Je serai heureux de faire le suivi avec nos experts dans ce domaine.

M. Raj Saini: Parfait.

Des commentaires du côté d'Apple?

M. Erik Neuenschwander: Je sais que l'affaire des aides publiques a fait beaucoup de bruit dans la presse, mais tout ce que je sais de cette affaire, je l'ai appris par les nouvelles. Je n'ai pas beaucoup lu sur le droit européen de la concurrence. Comme mon travail porte essentiellement sur la protection intégrée de la vie privée du point de vue technologique, je vais devoir demander à nos spécialistes de répondre à vos questions.

M. Raj Saini: D'accord.

Amazon est probablement la librairie dominante sur le marché. Êtes-vous d'accord?

M. Mark Ryland: Non, je ne suis pas d'accord.

M. Raj Saini: Ah non? Qui occupe une place plus importante que vous?

M. Mark Ryland: Le marché du livre est énorme et de nombreux acteurs vendent des livres, de Walmart à...

● (1025)

M. Raj Saini: Qui vend plus de livres que vous?

M. Mark Ryland: Je ne connais pas la réponse, mais je serai heureux de faire une recherche pour vous.

M. Raj Saini: D'accord.

L'une des méthodes que vous utilisez lorsque vous mettez des livres en vente — j'ai lu cela quelque part, corrigez-moi si je fais erreur —, c'est que vous approchez de petites librairies et leur imposez un droit appréciable pour inscrire leurs livres sur votre site. Vous ne payez pas les auteurs en fonction du nombre de copies numériques vendues, mais vous les payez en fonction du nombre de pages lues. Si le lecteur ne le lit pas le livre jusqu'au bout, vous empochez la différence. Vous enregistrez les préférences des lecteurs. S'ils lisent des auteurs populaires, vous n'offrez pas de rabais sur ces livres, parce que vous savez qu'ils les achèteront de toute façon.

Pensez-vous que cette pratique est équitable, ou est-ce que j'ai tout faux?

M. Mark Ryland: Je ne connais pas les faits que vous évoquez, je ne peux donc pas répondre. Je serai heureux de vous revenir là-dessus.

M. Raj Saini: D'accord.

Une dernière question. Laissons de côté l'animation un instant et imaginons qu'Amazon est un grand centre commercial. Vous en êtes le propriétaire. Vous louez des espaces aux détaillants. Vous leur donnez accès à votre plateforme. Vous contrôlez l'accès aux consommateurs et vous recueillez des données sur chaque site. Vous exploitez le plus grand centre commercial au monde.

Lorsque de petits commerçants connaissent un certain succès, vous avez tendance à utiliser cette information pour réduire la concurrence. Comme vous avez accès à toutes les tierces parties qui vendent des produits sur votre site, croyez-vous que ce soit une pratique équitable?

M. Mark Ryland: Nous n'utilisons pas les données que nous recueillons pour soutenir le marché de nos fournisseurs tiers. Nous n'utilisons pas ces données pour promouvoir nos propres ventes ou les produits que nous lançons en ligne.

M. Raj Saini: Vous en êtes certain?

M. Mark Ryland: Oui.

M. Raj Saini: Vous dites que si quelqu'un annonce un produit sur votre site Web, vous ne faites pas le suivi des ventes de ce produit pour savoir s'il est populaire ou non.

M. Mark Ryland: Nous recueillons les données pour soutenir l'entreprise et ses clients. Nous ne les utilisons pas pour nos propres activités de vente au détail.

M. Raj Saini: Vous ne cherchez pas à savoir quel produit se vend bien ou lequel se vend moins bien et vous n'essayez pas de concurrencer l'entreprise d'aucune manière.

M. Mark Ryland: Le volet de notre entreprise qui soutient ce vaste marché de fournisseurs tiers et qui a contribué au succès de milliers d'entreprises et de petits commerces dans le monde entier utilise certainement les données pour maximiser leur succès sur le marché. Nous ne les utilisons pas pour nos activités commerciales.

M. Raj Saini: L'une des plaintes que nous entendons dans le domaine de l'innovation, c'est que certains acteurs dominent le marché parce qu'ils ont accès à des données et parce qu'ils peuvent les conserver et les utiliser. Dans bien des cas, les petites entreprises ou les joueurs de moindre importance n'ont pas accès aux données ni au marché. De surcroît, il arrive parfois, lorsque des entreprises émergentes ont le vent dans les voiles, que les grandes compagnies leur achètent leur technologie pour la détruire et empêcher ainsi l'entreprise de leur faire concurrence.

Est-ce là une pratique utilisée par Amazon, Apple ou Microsoft?

M. Mark Ryland: Si vous regardez l'historique de nos acquisitions, vous constaterez que nous avons tendance à acquérir de très petites entreprises très ciblées. En gros, la réponse serait donc non.

M. Erik Neuenschwander: C'est la même réponse du côté d'Apple.

M. Raj Saini: Je parle de toute technologie émergente, de toute entreprise émergente susceptible de faire concurrence à n'importe laquelle de vos plateformes. Vous ne faites pas cela, ou seulement...? Je ne comprends pas ce que vous voulez dire.

M. Erik Neuenschwander: Les acquisitions dont je suis au courant visaient des entreprises comme AuthenTec, dont nous avons utilisé la technologie pour créer la première version de notre système Touch ID dans nos téléphones. Nous recherchons des innovations technologiques que nous pouvons intégrer à nos produits. Je ne pense pas que la technologie de lecture d'empreintes numériques de cette entreprise en faisait une concurrente directe d'Apple.

M. John Weigelt: Nous travaillons activement avec les jeunes entreprises du monde entier. Des programmes comme BizSpark et Microsoft Ventures aident nos partenaires et les entreprises en démarrage à progresser et à vendre leur produit. Nous sommes un fournisseur de logiciels génériques; nous offrons une plateforme commune à partir de laquelle les entreprises du monde entier créent leurs innovations. Une plateforme de ce genre a été construite à Montréal, Privacy Analytics, c'est une jeune entreprise qui se spécialisait dans la technologie de confidentialité persistante appelée Perfect Forward Privacy. Nous n'avions pas cette technologie et nous avons pensé qu'elle pourrait servir de catalyseur pour nos activités. Nous avons donc fait l'acquisition de cette entreprise dans le but d'intégrer sa technologie à nos produits.

Nos décisions en matière de création ou d'acquisition s'appuient sur les ressources dont nous disposons; dans certains cas, nous avons fait l'acquisition d'innovations fantastiques que nous avons intégrées à nos produits. Voilà en quoi consiste notre stratégie d'acquisition.

M. Raj Saini: Je vous remercie.

Le président: Monsieur Saini, je vous remercie.

Le dernier intervenant sera M. Baylis.

Quand M. Baylis aura terminé, nous procéderons à une autre série de questions. Pour que les choses soient claires, nous recommencerons à poser des questions aux délégations en suivant l'ordre de la liste.

Monsieur Baylis, vous avez cinq minutes.

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

Je remercie également nos témoins. Vous êtes tous deux très bien informés et disposés à répondre à nos questions, ce qui n'a pas été le cas hier. Je vous en suis reconnaissant.

Monsieur Davidson, dans vos observations préliminaires, vous avez dit que Google et Facebook doivent saisir l'occasion d'accroître leur transparence. Pouvez-vous nous en dire plus à ce sujet?

● (1030)

M. Alan Davidson: Bien sûr.

Nous pensons que la transparence publicitaire est un précieux outil à envisager pour lutter contre la désinformation, surtout dans un contexte électoral. Nous avons collaboré avec certains autres acteurs de premier plan à l'élaboration du Code de bonnes pratiques contre la désinformation de l'UE, afin d'améliorer les outils de transparence qui permettront aux consommateurs d'avoir plus de discernement face aux annonces qu'ils voient, tout en aidant les chercheurs et les journalistes à comprendre comment se produisent des vastes campagnes de désinformation. À la Fondation Mozilla, nous avons quelqu'un qui travaille là-dessus. Notre grande source de frustration, pour être honnête, c'est qu'il est très difficile d'avoir accès aux archives publicitaires, même si certains de nos collègues se sont engagés à en faciliter l'accès.

Nous avons récemment fait une analyse. Les experts ont établi cinq critères distincts — par exemple, est-ce une donnée historique? Est-elle publique? Est-ce une information difficile à obtenir? Ce genre de choses.

Sur notre blogue, nous publions des billets indiquant, par exemple, que Facebook n'a respecté que deux des cinq critères, soit le nombre minimal établi par les experts pour garantir un accès raisonnable à une publicité archivée. Sans vouloir critiquer ces entreprises — nous l'avons déjà fait publiquement —, je dirais que nous espérons aller plus loin, parce que si la transparence n'est pas au rendez-vous, je pense que...

Google a obtenu une meilleure note. Elle a obtenu quatre sur cinq sur la fiche des experts, sans toutefois être plus transparente concernant les annonces publicitaires. Nous n'arrivons toujours pas à comprendre comment sont orchestrées les campagnes de désinformation.

M. Frank Baylis: Vous avez dit que ces entreprises ne sont pas disposées à s'autoréglementer et que, à votre avis, elles devraient être réglementées. Vous ai-je bien compris?

M. Alan Davidson: Je voulais dire que si nous ne pouvons obtenir de meilleurs renseignements... La transparence est la première étape et elle peut être un outil vraiment puissant. Si nous arrivions à assurer la transparence et à mieux informer les gens sur la publicité partisane qu'ils voient, cela pourrait contribuer grandement à contrer ces campagnes de désinformation et la manipulation des élections. Si cette transparence n'est pas assurée, il serait alors plus raisonnable que les gouvernements interviennent et imposent plus de restrictions. Selon nous, c'est la deuxième meilleure solution, c'est certain. C'est ce que nous essayons de faire.

M. Frank Baylis: Mon collègue M. Angus ou, si vous le permettez, Charlie, mon collègue aîné...

M. Charlie Angus: Votre frère aîné.

M. Frank Baylis: Mon grand frère Charlie a soutenu que certaines activités devraient nécessiter le consentement — vous avez parlé de consentement granulaire ou distinct — et que d'autres devraient être carrément interdites. Êtes-vous d'accord avec cette ligne de pensée?

M. Alan Davidson: Nous avons dit que nous l'étions. Nous pensons qu'il est important de reconnaître que ces différents outils apportent de grands avantages aux utilisateurs, même dans des domaines comme la santé, les finances ou la localisation, nous voulons donc leur donner ces moyens. Si on parle des enfants ou de certaines informations du domaine de la santé, il faut probablement placer la barre très haut, voire interdire cette pratique.

M. Frank Baylis: Mon jeune collègue, M. Erskine-Smith, a dit que certaines pratiques fondées sur l'âge... Par exemple, nous interdisons aux personnes d'un certain âge de conduire et nous interdisons la consommation d'alcool sous un certain âge. Les témoins ont-ils des idées sur cette possibilité d'interdire carrément la collecte de certaines données, qu'elles soient ou non liées à l'âge, ou d'autres types de données? Avez-vous des commentaires à faire à ce sujet?

M. Erik Neuenschwander: Dans mes réponses précédentes, j'ai expliqué que nous cherchions à laisser les données sur l'appareil de l'utilisateur et sous son contrôle. Je ferais une distinction entre les données recueillies par une entreprise et celles recueillies par un appareil sous le contrôle de l'utilisateur. Dans la mesure du possible, nous voulons laisser les utilisateurs contrôler leurs données, par consentement explicite, et les laisser dans leur appareil.

M. Frank Baylis: Si l'information est recueillie, mais qu'elle n'est pas utilisée ou vue par une entreprise comme la vôtre... Si l'entreprise l'a recueillie et simplement conservée et que j'ai ensuite le choix de la supprimer ou non, vous estimez que c'est différent d'une collecte destinée à une utilisation ailleurs. C'est bien ce que vous dites?

M. Erik Neuenschwander: Je crois effectivement que la collecte effectuée par une entreprise est différente de la collecte effectuée sur l'appareil de l'utilisateur. À la limite, je n'emploierais pas le mot « collecte ». On devrait peut-être dire « stockage » ou quelque chose de ce genre.

M. John Weigelt: Je prends mon temps pour répondre à cette question parce que je réfléchis aux différentes situations possibles. J'essaie de me mettre à la place d'un parent et je me demande comment j'utiliserais ces outils. Je suis convaincu que cela dépend du contexte dans lequel s'inscrit cette interaction. Un environnement médical sera radicalement différent d'un environnement de divertissement en ligne.

La gestion des données dépend énormément du contexte, qu'il s'agisse des garanties de protection ou même de l'interdiction de recueillir ces données.

M. Frank Baylis: Est-ce que j'ai le temps de poser une autre question, monsieur le président?

Le président: Si vous faites vite, oui; vous avez 30 secondes.

M. Frank Baylis: Parlons de l'infonuagique. On dirait un beau nuage, mais ce n'est pas là que cela se passe. Il y a un serveur physique quelque part. C'est de cela qu'il est question. Oublions le nuage; c'est un serveur physique. Les lois applicables dépendent de l'endroit où se trouve le serveur.

On parle d'Apple, de Microsoft ou d'Amazon — et Amazon, c'est une grande partie de vos activités. Si nous, législateurs canadiens, adoptons une série de lois protégeant le Canada, mais que le serveur se trouve à l'étranger, nos lois n'auront aucun effet.

Est-ce que vous prenez des mesures pour vous aligner sur les lois gouvernementales en veillant à ce que ces serveurs se trouvent dans les limites territoriales du pays qui les réglemente?

● (1035)

M. Mark Ryland: Nous avons des centres de données dans de nombreux pays, y compris au Canada. Il y a un contrôle juridique, mais nous devons respecter les lois de tous les pays où nous fonctionnons. Ces lois peuvent aussi avoir une incidence extraterritoriale.

M. John Weigelt: Nous avons créé des centres de données dans 54 régions du monde et nous en avons installé ici au Canada, à Toronto et à Québec. Il se trouve que j'ai la responsabilité de veiller à ce qu'ils respectent les lois et règlements canadiens, qu'il s'agisse des normes du Bureau du surintendant des institutions financières ou des lois fédérales ou provinciales sur la protection des renseignements personnels. Nous accordons la plus grande importance au respect du cadre juridique local. Nous traitons les données stockées dans ces centres de données comme des documents imprimés. Nous voulons que les lois fassent en sorte que ces renseignements électroniques soient traités comme des documents imprimés.

Nous sommes d'ardents défenseurs de la CLOUD Act, qui permet de clarifier les conflits de lois qui posent des problèmes aux entreprises multinationales comme la nôtre. Nous respectons les lois régionales, mais elles sont parfois contradictoires. Avec la CLOUD Act, on espère créer une plateforme commune pour comprendre les traités d'entraide juridique ou pour y donner suite — car nous savons tous que l'application des traités d'entraide juridique est plutôt lente et que ces traités s'appuient sur des documents imprimés —, qui fournira de nouveaux instruments juridiques pour donner aux gouvernements la garantie que les renseignements de leurs résidants sont protégés de la même façon qu'ils le seraient dans des centres de données locaux.

Le président: Merci.

Merci, monsieur Baylis.

On n'en a pas encore parlé, et c'est pourquoi je vais poser la question.

Nous sommes ici à cause d'un scandale appelé Cambridge Analytica et d'une entreprise de médias sociaux appelée Facebook. Nous voulions vous différencier. Vous n'êtes pas dans les médias sociaux; les médias sociaux étaient représentés ici hier. Vous vous occupez de mégadonnées, etc.

J'ai un commentaire qui concerne plus précisément Apple. C'est pourquoi nous voulions que Tim Cook soit ici. Il a fait des observations très intéressantes. Je vais lire exactement ce qu'il a dit:

> Il y a d'abord le droit d'avoir des données personnelles réduites au minimum. Les entreprises devraient se faire un devoir de supprimer les renseignements signalétiques dans les données sur les clients ou d'éviter de les recueillir. Il y a ensuite le droit de savoir — c'est-à-dire de savoir quelles données sont recueillies et pourquoi. En troisième lieu, il y a le droit d'accès. Les entreprises devraient faire en sorte qu'il soit facile pour vous de consulter, de corriger et de supprimer vos données personnelles. Enfin, il y a le droit à la protection des données, sans quoi la confiance est impossible.

C'est une déclaration très forte. Dans la perspective d'Apple — et je poserai aussi la question à Mozilla —, que feriez-vous pour régler le problème de Facebook?

M. Erik Neuenschwander: Je ne suis même pas sûr de comprendre suffisamment tous les aspects du problème de Facebook pour pouvoir le régler.

Mais je sais qu'on peut se concentrer sur deux moyens. J'accorde toujours la priorité aux solutions technologiques. Ce que nous voulons, c'est placer l'utilisateur au contrôle des données et de l'accès aux données sur son appareil. Nous avons pris l'initiative, dans le cadre de notre plateforme, de dresser la barrière du système d'exploitation entre les applications et les données de l'utilisateur et d'exiger le consentement de l'utilisateur, par la médiation du système d'exploitation, entre ces applications et ses données. C'est un ensemble de mesures que nous avons fait évoluer au fil du temps.

On vous a dit aussi aujourd'hui qu'il fallait également songer à la convivialité, et c'est pourquoi nous essayons de garder les choses claires et simples pour les utilisateurs. Ce faisant, nous avons apporté à notre plateforme technologique des améliorations qui nous permettent d'élargir cet ensemble de données que le système d'exploitation... Je rappelle que c'est distinct d'Apple, distinct de l'entreprise. Le système d'exploitation peut prendre de l'avance et permettre à l'utilisateur de contrôler cet accès.

C'est un processus auquel nous resterons fidèles.

Le président: À mon avis, il est très difficile de modifier la loi à cet égard, étant donné tous les paramètres qui entrent en ligne compte. Ce serait peut-être plus simple pour quelqu'un comme Tim Cook et dans le cadre d'une idéologie qui considère que les utilisateurs sont primordiaux. Il serait peut-être plus simple pour Apple de s'en charger que pour les législateurs du monde entier d'essayer de régler cette question. Nous faisons cependant tout notre possible. Nous essayons vraiment.

Monsieur Davidson, est-ce que vous avez quelque chose à dire sur la façon de régler le problème de Facebook?

● (1040)

M. Alan Davidson: Vu de l'extérieur, il est très difficile d'imaginer comment régler le problème d'une autre entreprise. À mon avis, nous sommes nombreux à être déçus des choix qu'elle a faits et qui ont suscité l'inquiétude de beaucoup de gens et de nombreux organismes de réglementation.

Notre espoir est qu'elle garantisse la protection de la vie privée et permette aux utilisateurs d'exercer plus de contrôle. C'est un point de départ extrêmement important.

Si je devais dire quelque chose à mes collègues, je les inviterais à réfléchir un peu moins à court terme au sujet des moyens de répondre à certaines de ces préoccupations. Je pense qu'ils ont beaucoup d'outils à leur disposition pour donner aux gens beaucoup plus de contrôle sur leurs renseignements personnels.

À l'heure actuelle, les organismes de réglementation disposent de nombreux outils pour bien encadrer ce que les entreprises peuvent se permettre ou non. Malheureusement, quand les gens ne respectent pas de bonnes pratiques en matière de protection de la vie privée, ils donnent le mauvais exemple.

Nous pouvons tous faire quelque chose. C'est pourquoi nous avons intégré l'extension Facebook Container dans nos outils de suivi: pour essayer de donner plus de contrôle aux gens.

Le président: Merci de votre réponse.

Il y a encore des questions. Nous allons commencer par mon coprésident, puis nous suivrons l'ordre habituel. Vous aurez du temps. Ne vous inquiétez pas.

Commençons par M. Collins.

M. Damian Collins: Merci.

Je vais m'adresser d'abord à M. Ryland et à Amazon.

Pour faire suite aux commentaires du président au sujet de Facebook, si je relie mon compte Amazon à Facebook, quelles sont les données qui sont partagées entre les deux plateformes?

M. Mark Ryland: Je ne sais pas comment on relie un compte Facebook à Amazon. Je sais qu'Amazon peut servir de service de connexion vers d'autres sites Web, mais Facebook n'en fait pas partie. Je ne connais aucun autre modèle de connexion.

M. Damian Collins: Vous dites qu'on ne peut pas le faire. On ne peut pas connecter un compte Facebook et un compte Amazon.

M. Mark Ryland: Pas à ma connaissance. Je ferai un suivi pour m'en assurer.

M. Damian Collins: Il y a eu le Digital, Culture, Media and Sport Committee à Londres, que j'ai présidé avec mes collègues ici présents. En décembre dernier, nous avons publié des documents concernant l'affaire Six4Three.

Au même moment, une enquête du *New York Times* donnait à penser qu'un certain nombre de grandes entreprises avaient conclu avec Facebook des accords spéciaux de réciprocité leur permettant d'avoir accès aux données de leurs utilisateurs sur Facebook et à celles de leurs amis. Amazon figurait parmi ces entreprises.

Pourriez-vous nous dire quel genre de protocoles d'entente vous avez avec Facebook et si cela vous donne accès non seulement aux données de vos clients ou des titulaires de comptes Facebook, mais aussi à celles de leurs amis?

M. Mark Ryland: Je vais devoir vous revenir à ce sujet. Je ne sais pas du tout.

M. Damian Collins: Cet article du *New York Times* a fait des vagues l'année dernière. Je suis étonné qu'on ne vous en ait pas parlé.

Je vais poser la même question à Microsoft également.

On peut se connecter à Skype à partir de son compte Facebook. Je vous le demande également: si on relie son compte Skype et son compte Facebook, quelles sont les données qui sont partagées entre les deux?

M. John Weigelt: Si je comprends bien, il s'agit d'une connexion simplifiée à votre compte Skype à partir de Facebook. Quand on se connecte, une fenêtre contextuelle devrait s'ouvrir pour donner une idée de ce que Facebook fournit à l'environnement Skype.

C'est un modèle de connexion simplifié.

M. Damian Collins: Quelles sont les données qui sont partagées entre les comptes? Pour les utilisateurs qui utilisent ce moyen, quelles sont les données d'utilisation de Skype qui sont communiquées à Facebook?

M. John Weigelt: C'est simplement une connexion.

M. Damian Collins: Oui, mais toutes ces connexions sur Facebook comportent également des accords de réciprocité. La question est de savoir si...

M. John Weigelt: C'est seulement une façon simplifiée de partager une preuve d'identité, si on veut, et c'est ce qui vous permet de vous connecter à Skype.

M. Damian Collins: Je sais comment fonctionne la connexion de base, mais ces dispositions de connexion à partir de Facebook donnent un accès réciproque aux données des deux. C'est effectivement une connexion.

M. John Weigelt: Ce n'est rien qui n'aurait pas été divulgué dans le cadre de la connexion initiale; donc, quand vous vous connectez, quand vous utilisez cette passerelle, une fenêtre contextuelle indique les données qui interagissent ou sont échangées.

M. Damian Collins: Et puis c'est dans les conditions et modalités.

M. John Weigelt: C'est dans la fenêtre contextuelle par laquelle vous devez passer. C'est une modalité simplifiée et, si j'ai bien compris; c'est un avis à plusieurs niveaux. On vous donne un aperçu de la catégorie de données; puis, en cliquant dessus, vous pouvez aller plus loin pour voir de quoi il s'agit.

M. Damian Collins: En termes simples, est-ce que Facebook saurait avec qui j'ai communiqué sur Skype?

M. John Weigelt: Je ne crois pas, mais je vais devoir vous revenir à ce sujet. Mais, vraiment, je ne crois pas.

M. Damian Collins: D'accord.

Je voudrais revenir à Amazon. Rapidement.

Voici comment Amazon.com prévoit la connexion entre un compte Facebook et un compte Amazon:

> Aller dans réglages, sélectionner son compte, puis choisir la fonction de connexion aux réseaux sociaux.
>
> Sélectionner ensuite son compte Facebook.
>
> Fournir ses données de connexion et cliquer sur Se connecter.

C'est une façon très simple de connecter son compte Facebook à son compte Amazon. Je vais donc vous reposer la question: quand on fait cela, quelles sont les données qui sont partagées entre les deux plateformes?

● (1045)

M. Mark Ryland: Je vais devoir vous revenir à ce sujet. Je ne sais pas du tout.

M. Damian Collins: Je vois. C'est pourtant assez élémentaire. Ce qui m'inquiète, c'est que des données soient partagées entre les deux plateformes.

Je rappelle que l'enquête du *New York Times* a révélé l'existence d'accords de réciprocité préférentiels entre Amazon et Facebook, entre Microsoft et Facebook, pour que ces entreprises aient accès non seulement aux données de leurs utilisateurs sur Facebook, mais aussi à celles de leurs amis, alors que ce réglage avait été éliminé d'autres applications. Il reste que les principaux partenaires de Facebook ont un accès préférentiel compte tenu de l'argent qu'ils dépensent ensemble ou de la valeur des données.

Je voudrais savoir, encore une fois, si Amazon ou Microsoft peut nous parler de la nature des données, de ce qu'elles englobent, et si ces arrangements sont toujours en vigueur.

M. John Weigelt: Je ne peux rien dire de...

M. Damian Collins: Je ne sais pas si cela veut dire que vous ne savez pas ou que vous ne savez pas quoi dire. Quoi qu'il en soit, si vous pouviez nous écrire, nous vous en serions reconnaissants.

M. Mark Ryland: D'accord.

M. John Weigelt: Sans faute.

M. Mark Ryland: Nous ferons un suivi.

Le président: Passons à M. Erskine-Smith. Vous avez cinq minutes.

M. Nathaniel Erskine-Smith: Merci beaucoup.

Je voudrais d'abord parler d'éthique et d'intelligence artificielle. Le Comité a entrepris une étude à ce sujet, et le gouvernement du Canada exige désormais des évaluations algorithmiques d'impact sur les ministères quand ceux-ci emploient un algorithme pour la première fois, à titre d'évaluation du risque dans l'intérêt public. D'après vous, est-ce qu'on devrait l'exiger des grandes entreprises de mégadonnées du secteur public comme la vôtre?

Je vais commencer par Amazon, puis je ferai le tour de la table.

M. Mark Ryland: Nous faisons le maximum pour garantir l'impartialité des algorithmes, et c'est l'un de nos principes fondamentaux. Nous avons des ensembles de données d'essai pour veiller à toujours respecter la norme à cet égard.

M. Nathaniel Erskine-Smith: Selon vous, est-ce qu'il devrait y avoir transparence pour le public afin de garantir une reddition des comptes suffisante concernant les algorithmes que vous appliquez à ces trésors considérables de données et de renseignements personnels?

M. Mark Ryland: Je pense que le marché arrive très bien à faire en sorte que les entreprises se dotent de bonnes normes à cet égard.

M. Nathaniel Erskine-Smith: Voyez-vous, ce qui est frustrant, c'est que vous avez dit être d'accord avec les principes du RGPD, et le droit à l'explication des algorithmes est justement un principe du RGPD.

Apple, qu'en pensez-vous?

M. Erik Neuenschwander: Dans le modèle d'apprentissage machine que nous employons, nous voulons effectivement que les utilisateurs comprennent que nous le faisons principalement en le plaçant sur leurs appareils et en le développant à partir de leurs données. Quand nous développons des modèles généralisés, nous nous appuyons sur des ensembles de données publiques. Nous ne le faisons surtout pas à partir de données personnelles.

Si l'apprentissage machine se fait à partir de données personnelles, nous tenons absolument à ce que le processus puisse être expliqué aux utilisateurs et que ceux-ci puissent le comprendre.

M. Nathaniel Erskine-Smith: Vous croyez donc à cette transparence publique.

M. Erik Neuenschwander: Nous croyons en la transparence à bien des égards.

M. Nathaniel Erskine-Smith: Microsoft, quel est votre avis?

M. John Weigelt: Nous participons et nous contribuons au travail qui se fait ici, au Canada, et notamment au règlement des difficultés liées aux définitions. Dans le cas des systèmes d'intervention artificielle à grande échelle, il faut pouvoir expliquer à l'utilisateur ce qui se passe dans les coulisses.

C'est un sujet très controversé, un large domaine de recherche sur le droit à l'explication, sur la généralisabilité et sur la façon dont nous examinons les résultats.

D'après la documentation actuelle, tout se passe pour ainsi dire comme si l'évaluation des risques algorithmiques et un avis au public étaient obligatoires à partir du moment où on a la localisation du site Web — par exemple, si je viens du Québec et que je présente un site Web en français pour cette raison.

M. Nathaniel Erskine-Smith: Vous vous inquiétez de la définition, mais vous êtes d'accord sur le principe.

M. John Weigelt: Nous sommes d'accord sur le principe et nous félicitons le gouvernement du Canada d'avoir mis cela en place dès maintenant; d'autres devraient envisager des possibilités semblables.

M. Nathaniel Erskine-Smith: Notamment le secteur privé et Microsoft.

Concernant la réglementation de la concurrence, j'ai lu hier une citation de l'organisme de réglementation allemand, qui souligne la position dominante de Facebook sur le marché et estime que « le seul choix donné à l'utilisateur est d'accepter de fournir une combinaison complète de données ou de s'abstenir d'utiliser le réseau social. En tout état de cause, on ne peut pas parler de consentement volontaire ».

Est-ce que le même principe s'applique à vos entreprises?

M. Mark Ryland: Nous faisons face à une concurrence féroce sur les marchés où nous exploitons. Dans le domaine de l'infonuagique, par exemple, notre principal concurrent est l'ancien modèle d'exploitation des entreprises informatiques, et il y a un vaste éventail de concurrents.

M. Nathaniel Erskine-Smith: Je vois. Changeons un peu de sujet. Est-ce qu'on devrait tenir compte de l'incidence sur la vie privée des consommateurs dans la réglementation de la concurrence?

M. Mark Ryland: C'est un domaine qui n'est pas non plus de mon ressort. Je déteste donner cette réponse.

M. Nathaniel Erskine-Smith: Dommage, parce que j'avais précisé à Amazon que nous discuterions justement de concurrence aujourd'hui.

Je pose la question aux autres entreprises: pensez-vous qu'on devrait tenir compte de l'incidence sur la vie privée des consommateurs dans la réglementation de la concurrence?

M. Erik Neuenschwander: Vous laissez entendre qu'on exige, du moins dans certains cas, un consentement unique, du genre tout ou rien, et nous le savons très bien. Nous proposons, en fait, un consentement très nuancé et détaillé. Il est possible d'utiliser un appareil Apple sans s'inscrire ni créer de compte Apple. Nous essayons donc de différencier et de séparer ces choses.

● (1050)

M. Nathaniel Erskine-Smith: Je vois.

Est-ce que Microsoft a un point de vue sur cette question?

M. John Weigelt: C'est une question de données et plus particulièrement de protection et d'utilisation des données. Je crois que nous devons examiner l'utilisation des données de façon plus générale. À ce chapitre, des fiches de données pourraient être utiles puisque, selon moi, la protection des renseignements personnels est une question de sécurité et d'accessibilité des données.

M. Nathaniel Erskine-Smith: J'ai hâte de savoir ce que l'avocat général associé aura à dire demain au forum des données du commissaire à la concurrence.

J'ai une autre question au sujet du droit de la concurrence.

Dans les années 1990, Explorer était gratuit, et pourtant, on a empêché Microsoft d'être en situation de monopole avec son navigateur. Il ne s'agissait pas de protéger les consommateurs contre une hausse des prix. Il s'agissait de protéger l'innovation.

Je vais lancer quelques flèches en direction d'Amazon. Tout à l'heure, vous avez dit que les renseignements que je verse dans Alexa font partie de mon profil d'utilisateur. J'en déduis que ce que je regarde sur Prime, ce que j'achète de n'importe quel vendeur et ce que je recherche sur Amazon ou ailleurs sur Internet, tout cela est agrégé en un profil unique aux fins des publicités ciblées, je présume.

J'aimerais aussi savoir si mon profil d'utilisateur, combiné au profil des autres utilisateurs, oriente vos décisions en matière de nouveaux produits. Est-ce une question légitime?

M. Mark Ryland: Nous examinons les tendances, les achats et le comportement de nos clients pour déterminer quels seront les prochains...

M. Nathaniel Erskine-Smith: Au contraire, en réponse aux questions de M. Saini, vous avez dit ne pas faire le pistage en ligne des renseignements des vendeurs tiers sur vos sites Web. Si l'on regarde les choses sous un autre angle, on constate que vous faites le pistage de toutes les décisions d'achat individuelles sur Amazon et que vous combinez ces données pour faire concurrence aux vendeurs tiers sur votre plateforme de commerce. N'exploitez-vous pas ainsi votre position hégémonique?

M. Mark Ryland: Je pense que le fait que le marché des vendeurs tiers est si prospère — on y retrouve un très grand nombre d'entreprises prospères — montre très clairement que ce n'est pas un problème.

M. Nathaniel Erskine-Smith: Vous n'estimez pas détenir un avantage indu sur le marché.

M. Mark Ryland: Non.

M. Nathaniel Erskine-Smith: Ma dernière question a été soulevée par...

Le président: Faites vite, je vous prie. Nous essayons de donner la parole à tout le monde.

M. Nathaniel Erskine-Smith: En ce qui concerne la monétisation des données personnelles, comme je l'ai dit hier aux experts, le problème tient au modèle d'affaires. Cette proposition a été formulée par un certain nombre de personnes. Je crois que Tim Cook d'Apple a fait valoir le même argument en ce qui a trait au complexe industriel de données.

J'aimerais que les témoins de Microsoft et d'Amazon me disent s'ils pensent que le modèle d'affaires est problématique en soi. Vous voulez recueillir de plus en plus de renseignements à notre sujet. Quelle est l'utilité, pour nous, de cette collecte massive de renseignements à notre sujet? Le modèle d'affaires pose-t-il problème?

M. John Weigelt: Je tiens à préciser que les renseignements que nous recueillons ne concernent que les produits. Nous ne cherchons pas à personnaliser les choses pour cibler une personne en particulier.

Lorsque nous nous rendons compte que les gens n'utilisent pas une fonctionnalité, grosso modo, nous faisons usage de l'anonymat et du pseudonymat; c'est une excellente fonctionnalité. Nous essayons de faire ressortir cette fonctionnalité dans les versions subséquentes. C'est simplement pour nous aider à améliorer notre entreprise. Nous sommes une société de logiciels et de services. C'est notre secteur d'activité.

M. Mark Ryland: Notre modèle d'affaires est tout à fait conforme à la protection de la vie privée des consommateurs, car il s'agit de respecter les choix de ceux-ci grâce à un modèle traditionnel d'achat et de vente de ressources et de produits et de services.

M. Nathaniel Erskine-Smith: Merci.

Le président: Nous passons maintenant à M. Angus. Vous avez cinq minutes.

M. Charlie Angus: Merci beaucoup.

Diapers.com était une entreprise en ligne qui vendait des couches dans ce « marché concurrentiel » dont parle Amazon. Jeff Bezos voulait l'acheter. L'entreprise a refusé l'offre, alors Amazon a fixé des prix d'éviction. Amazon perdait 100 millions de dollars en couches tous les trois mois, et ce, afin de pousser un concurrent à la vente ou à la faillite. Finalement, Diapers.com a accepté l'offre. On craignait qu'Amazon ne baisse les prix encore plus.

Nous parlons d'antitrust en raison de ce qu'on appelle, dans The Economist, la « zone de destruction » de l'innovation. Or, dans le cas d'Amazon, il s'agit d'une zone de destruction de la concurrence fondée sur le pouvoir que vous avez, sur toutes vos plateformes, de baisser les prix et de pousser les gens à la faillite. Selon Shaoul Sussman, les pratiques de prix d'éviction d'Amazon relèvent de l'antitrust et réclament une mesure législative.

Que répondez-vous à cela?

M. Mark Ryland: Je me dois de répéter que je ne suis pas un expert en droit de la concurrence et que je ne connais pas l'historique ou les détails de certains éléments dont vous faites mention.

Dans notre secteur d'activité en général, nous constatons une forte concurrence entre toutes ces entreprises. Il y a beaucoup d'entreprises en démarrage et un grand nombre de concurrents qui utilisent notre plateforme Amazon Web Services — soit AWS. Certaines des plus grandes plateformes de commerce en ligne en Allemagne et en Amérique latine, par exemple, nous font confiance et utilisent AWS. Nous pensons donc que la concurrence fonctionne bien.

M. Charlie Angus: Oui, vous avez tous ces gens qui utilisent vos services infonuagiques, puis vous pouvez baisser les prix dans une attaque contre les petites entreprises familiales. Lena Kahn, de Open Markets, dit que, étant donné que vous dominez le marché dans un si grand nombre de secteurs, vous pouvez utiliser les profits que vous tirez des services infonuagiques pour imposer des prix d'éviction et réduire la concurrence. Elle dit que la « structure et la conduite [de votre entreprise] soulèvent des préoccupations d'ordre anticoncurrentiel, et pourtant, [la société] échappe au contrôle antitrust ».

Les législateurs doivent se pencher sur cette question, selon moi. Nous constatons que, au Canada, vous jouissez de l'avantage de ne pas payer des impôts au même titre que nos entreprises les plus pauvres. Au Royaume-Uni, vous avez gagné 3,35 milliards de livres et vous n'avez payé que 1,8 million de livres sur des revenus imposables. Si vous obtenez ce genre de traitement, on peut dire que vous êtes le plus grand assisté social de la terre entière.

Aux États-Unis, les choses vont encore plus rondement. Vous avez réalisé des profits de 11 milliards de dollars et vous avez obtenu un remboursement de 129 millions de dollars. De fait, vous avez eu droit à un taux d'imposition négatif de 1 %. Voilà un avantage extraordinaire. Quelle entreprise ou quel particulier ne voudrait obtenir un remboursement au lieu de payer des impôts?

Comment justifier l'existence d'un marché où Amazon peut couper l'herbe sous le pied de n'importe quel concurrent ou éditeur de livres sans même payer sa juste part d'impôts? Ne croyez-vous pas qu'il nous incombe de vous rappeler à l'ordre et de veiller à ce que le marché soit gouverné par des règles équitables?

● (1055)

M. Mark Ryland: Mes excuses. Comme je vous l'ai déjà dit, je ne suis pas un expert en droit de la concurrence. La discussion devait porter sur la sécurité, la protection des consommateurs et la protection de la vie privée, un domaine dans lequel j'ai une certaine expertise. Je ne suis pas en mesure de répondre à vos questions sur les sujets dont vous parlez.

M. Charlie Angus: Oui, c'est malheureux. C'est pourquoi le président du Comité a demandé que nous invitions des gens qui soient à même de répondre aux questions, parce que ce sont là les questions qui, pour nous, les législateurs, exigent des réponses. Nous sommes dans une nouvelle ère et en raison de Facebook, nous nous trouvons dans la situation actuelle. Si les pratiques d'entreprise de Facebook étaient meilleures, nous ne serions peut-être pas tenus de nous pencher là-dessus. Or, nous y sommes tenus. Si Amazon ne se livrait pas à de telles pratiques anticoncurrentielles, nous pourrions penser que le libre marché fonctionne parfaitement, mais ce n'est pas le cas actuellement, et vous n'arrivez pas à nous donner des réponses.

Voilà qui nous place dans une situation difficile. À titre de législateurs, nous demandons des réponses. Qu'est-ce qu'un taux d'imposition équitable? Comment assurer la concurrence sur le marché? Comment pouvons-nous nous assurer qu'il n'y a pas de pratique de prix d'éviction acculant les entreprises — nos entreprises — à la faillite en raison de votre hégémonie sur le marché? Pourtant, vous n'arrivez pas à répondre à nos questions. Tout cela nous laisse très perplexes. Devrions-nous demander l'aide d'Alexa ou de Siri?

Des voix: Oh, oh!

M. Mark Ryland: Je m'excuse, mais je n'ai pas l'expertise nécessaire pour répondre à ces questions.

M. Charlie Angus: Merci.

Le président: J'aimerais revenir sur ce qu'a dit M. Angus. C'est la raison pour laquelle nous avons demandé à M. Bezos de venir. Il peut répondre à ce genre de questions devant notre grand Comité. C'est lui qui aurait été à même de répondre à toutes nos questions. Nous n'aurions exclu aucun témoin du Comité, mais nous voulions entendre des gens capables de nous donner des réponses complètes au sujet de l'ensemble du dossier.

Je donne maintenant la parole à M. Lucas, du Royaume-Uni.

M. Ian Lucas: Monsieur Weigelt, puis-je revenir à la question du transfert de données au sein de Microsoft? Vous avez dit que Microsoft avait acquis un certain nombre d'entreprises, dont LinkedIn. Pouvez-vous apporter des éclaircissements? Si je confie des renseignements à LinkedIn, ceux-ci sont-ils ensuite communiqués à d'autres entreprises au sein de Microsoft?

M. John Weigelt: Pas du tout. LinkedIn conserve une certaine indépendance par rapport à la société Microsoft.

M. Ian Lucas: Vous dites donc que l'information recueillie par LinkedIn est isolée et qu'elle n'est pas communiquée au sein de la société Microsoft.

M. John Weigelt: Tout transfert de... Excusez-moi. Permettez-moi de revenir en arrière. Toute connexion entre votre profil LinkedIn et, par exemple, votre suite Office est effectuée par vous-même, l'utilisateur. C'est une connexion qui est établie sciemment. Par exemple, vous pouvez choisir de tirer parti d'une connexion à LinkedIn dans vos clients de messagerie. Alors, l'utilisateur accomplit une action dans son profil LinkedIn. C'est sa suite Office...

M. Ian Lucas: Ce qui m'intéresse, c'est le fonctionnement par défaut. Si je m'inscris à LinkedIn, j'omets de lire les modalités d'utilisation et je donne des renseignements, est-il possible que ceux-ci soient transférés vers d'autres entreprises de la famille Microsoft, pour reprendre votre appellation?

M. John Weigelt: LinkedIn ne partage pas de tels renseignements à l'échelle de l'entreprise à partir du système informatique dorsal.

M. Ian Lucas: En règle générale, les renseignements sont-ils transférés à travers les différentes entreprises faisant partie de la société Microsoft?

M. John Weigelt: En règle générale, chaque secteur d'activité est indépendant.

● (1100)

M. Ian Lucas: Y a-t-il un transfert d'informations entre les différentes entreprises?

M. John Weigelt: Les renseignements personnels sont conservés dans chaque secteur d'activité.

M. Ian Lucas: Je viens de poser une question très précise. La politique de la société Microsoft permet-elle le transfert de données personnelles entre les différentes entreprises appartenant à Microsoft?

M. John Weigelt: C'est une question d'usage compatible...

M. Ian Lucas: Pouvez-vous répondre par un oui ou par un non?

M. John Weigelt: C'est une question d'usage compatible, n'est-ce pas? Donc, nous, à titre de...

M. Ian Lucas: La réponse à cette question est soit oui, soit non.

M. John Weigelt: Je dois répondre que je ne peux ni affirmer ni nier qu'il y ait... Je ne suis pas au courant.

M. Ian Lucas: Bon, d'accord. Voilà qui ne nous avance pas beaucoup.

Pourriez-vous me revenir là-dessus?

M. John Weigelt: Certainement.

M. Ian Lucas: Merci.

Monsieur Neuenschwander, j'ai devant moi deux appareils Apple très impressionnants, quoique mes collègues technophiles me disent que mon iPhone est complètement dépassé.

Le problème, c'est que bien souvent, les gens accèdent à Facebook, par exemple, au moyen d'un appareil Apple. Vous avez dit qu'une grande quantité de renseignements se retrouvent dans le téléphone ou dans l'iPad d'Apple. Vous avez aussi dit que ces renseignements ne sont pas transférés ailleurs et qu'il ne vous appartient pas de les transférer. Je n'accepte pas vraiment cet argument, parce que les gens ont accès à d'autres plateformes au moyen de vos appareils.

Votre entreprise est l'une des plus grandes sociétés du monde. Vous pouvez choisir avez qui vous faites affaire. Pourquoi permettre aux entreprises qui ne partagent pas votre approche en matière de protection de la vie privée d'utiliser votre matériel pour faire des affaires?

M. Erik Neuenschwander: Je ne sais pas si les entreprises sont d'accord ou non avec notre approche. Je pense que nous encouragerions... Nous essayons de donner l'exemple dans notre approche en matière de protection de la vie privée.

Comme je l'ai dit, l'objectif de mon équipe est, je crois, de mettre les renseignements sur l'appareil, mais je pense que nous avons une responsabilité à l'égard du déplacement de ces renseignements. C'est pourquoi nous avons pris des mesures pour que notre système d'exploitation s'interpose entre les applications et certaines données présentes sur l'appareil.

Il y a des données présentes sur l'appareil que nous n'avons jamais rendues accessibles. Il en restera ainsi, je crois. Par exemple, le numéro de téléphone de l'utilisateur ou les identificateurs du matériel qui pourraient être utilisés pour le pistage n'ont jamais été rendus accessibles sur notre plateforme.

Il s'agit d'un concept technologique du type « vase clos », selon lequel chaque application est séparée à la fois des autres applications et des données présentes dans le système d'exploitation.

M. Ian Lucas: Là où je veux en venir, c'est que vous établissez les principes. Le président les a énoncés. C'est vraiment complexe et difficile pour nous de légiférer sur ces questions. Nous nous en rendons tous compte.

Vous pouvez décider si vous faites affaire avec Facebook. Si vous le vouliez, vous pourriez refuser à Facebook l'accès à votre matériel en cas de non-respect des principes. Facebook a causé beaucoup de tort à votre secteur. Pourquoi continuez-vous de faire affaire avec cette entreprise?

M. Erik Neuenschwander: Si vous parlez de la disponibilité de l'application sur l'App Store, je crois qu'il y a deux...

M. Ian Lucas: On ne peut nier qu'énormément de gens accèdent à Facebook au moyen de vos appareils.

M. Erik Neuenschwander: D'accord. D'un côté, supposons que l'application Facebook ne soit pas offerte. Facebook a un site Web auquel les gens pourraient toujours avoir accès au moyen de notre navigateur ou d'un navigateur concurrent.

Si nous allons plus loin et disons que nous devrions commencer à imposer ce que j'appellerais...

M. Ian Lucas: Il ne s'agit pas d'imposer quelque chose. C'est une question d'accord. Si vous croyez en vos principes et si vous êtes une entreprise éthique, vous devriez faire affaire avec des gens qui respectent vos principes. Vous avez le pouvoir de faire cela.

M. Erik Neuenschwander: Ce qui est en mon pouvoir, je suppose, ce sont les mesures techniques. Mon approche consiste à dire que toute application ou tout service passant par le téléphone devrait comprendre des mesures techniques permettant à l'utilisateur de garder la maîtrise de ses données.

M. Ian Lucas: Vous pourriez décider de ne pas faire affaire avec Facebook. Vous pourriez établir vos propres principes et les appliquer en choisissant avec qui vous faites affaire. Pourquoi ne faites-vous pas cela?

M. Erik Neuenschwander: Si vous parlez de la disponibilité de Facebook sur l'App Store, le retrait de cette application n'aurait pas une incidence mesurable sur la protection de la vie privée.

M. Ian Lucas: Vraiment?

M. Erik Neuenschwander: Je pense que les utilisateurs...

M. Ian Lucas: Vous feriez les manchettes, ne croyez-vous pas?

● (1105)

M. Erik Neuenschwander: Bien sûr, nous ferions les manchettes. Avec tout le respect que je vous dois, je ne crois pas que les manchettes aient nécessairement une incidence sur la protection de la vie privée. Je pense que les utilisateurs...

M. Ian Lucas: Ne pensez-vous pas que cela aurait une incidence importante sur l'approche adoptée par Facebook?

M. Erik Neuenschwander: Comme vous l'avez souligné, Facebook est un service extrêmement populaire. Les utilisateurs se tourneraient vers les technologies Web pour trouver d'autres façons de continuer à accéder à Facebook. Personnellement, je ne vois pas comment Apple pourrait... ou comment je pourrais, par respect pour la vie privée d'une personne...

M. Ian Lucas: Ce qui me préoccupe, c'est que vous vous présentez comme les bons tout en facilitant les choses pour les méchants par l'entremise de votre matériel.

M. Erik Neuenschwander: Au fil des ans, nous avons adopté de nombreuses mesures pour établir des limitations et pour en faire plus que toute autre plateforme en matière de protection de la vie privée et de maîtrise des utilisateurs sur les données présentes sur nos appareils. C'est précisément grâce à l'intégration de notre matériel informatique que nous avons pu prendre tant de mesures positives et proactives pour encourager la minimisation des données et pour permettre aux utilisateurs d'avoir une maîtrise sur leurs données.

M. Ian Lucas: Cependant, vous voulez tout de même faire affaire avec les méchants.

Le président: Merci, monsieur Lucas. Nous devons poursuivre.

Nous passons maintenant à Mme Naughton, de l'Irlande.

Mme Hildegarde Naughton: Merci.

J'aimerais revenir à M. Ryland et à la question que j'ai posée plus tôt au sujet de l'affichage des noms et des adresses électroniques des clients par Amazon. Êtes-vous absolument certain que cela ne s'est pas produit?

M. Mark Ryland: Chose certaine, je ne suis pas au courant de l'incident. Je ne crois pas que cela se soit produit, mais nous vous reviendrons là-dessus.

Mme Hildegarde Naughton: Le 21 novembre 2018, deux articles ont paru dans *The Guardian* et dans *The Telegraph*. Dans les deux cas, on faisait état d'une importante atteinte à la protection des données chez Amazon, si bien que les noms et adresses électroniques des clients avaient été divulgués sur le site Web de l'entreprise.

M. Mark Ryland: Je me ferai un plaisir de vous revenir là-dessus.

Mme Hildegarde Naughton: Merci. Je voulais simplement tirer cela au clair. C'est consigné au compte rendu.

Le président: Monsieur Lawless, vous avez la parole.

M. James Lawless: J'ai une question au sujet de la transférabilité des données et du principe du RGPD. Cela m'a semblé poser problème.

Pour ce qui est des mégadonnées, il s'agit de savoir où elles se trouvent, comment elles sont stockées, sous quelle forme elles sont conservées, etc. Acceptez-vous cela? Souhaitez-vous conserver des données qui soient exclusives à votre société ou êtes-vous à l'aise avec l'utilisation de formats ouverts qui permettent le partage? J'aimerais savoir quelle est la position actuelle de chacun d'entre vous au sujet de la transférabilité des données.

M. Alan Davidson: Nous pensons que l'accès et la transférabilité des données sont des éléments extrêmement importants du RGPD. En fait, ce sont des piliers de toute bonne réglementation en matière de protection de la vie privée. C'est sans parler de l'effet positif que cela pourrait avoir sur la concurrence. Nous pensons qu'il y a beaucoup de travail prometteur à accomplir pour faire en sorte que les gens sachent ce qui se trouve à tel endroit et pour que cette information — laquelle nous fournissons, d'ailleurs, lorsque nous détenons des données — soit utilisable.

Il ne s'agit pas seulement de savoir que l'on peut télécharger tout son corpus de données Facebook — je l'ai fait et j'encourage les gens à le faire, c'est très intéressant. Il s'agit aussi de rendre ces données utilisables, de telle sorte que l'utilisateur puisse les transporter ailleurs s'il le souhaite.

M. John Weigelt: Nous nous sommes engagés à respecter le RGPD et les principes de la transférabilité des données. La grande question porte sur l'interopérabilité des profils ou des données et sur la possibilité de les déplacer dans un format approprié. Pour l'heure, on ignore encore où les gens veulent transférer leurs données et dans quels formats ils veulent le faire.

M. James Lawless: Microsoft a fait des progrès à ce chapitre. Je sais que, par le passé, on alléguait qu'il y avait chez Microsoft un problème qui tenait aux formats exclusifs, mais aujourd'hui, on offre toujours l'option de « sauvegarder sous » un format plus ouvert. Est-ce là ce que vous avez fait?

M. John Weigelt: Tout à fait. Même que dans le secteur, dans le domaine de l'infonuagique, des activités arbitraires ont été déplacées d'un endroit à l'autre. Nous avons adopté cette approche. De plus, nous nous sommes tournés vers la communauté des codes sources ouverts et des données ouvertes pour obtenir des conseils.

M. Erik Neuenschwander: Anticipant le RGPD, Apple a lancé un portail de données et de renseignements personnels. Les utilisateurs peuvent télécharger leurs renseignements personnels, au titre de l'accès à l'information comme au titre de la transférabilité, en formats lisibles par des humains et par des machines.

M. Mark Ryland: Au nom d'Amazon Web Services, où je travaille, je dirai que l'importation et l'exportation sont des fonctionnalités fondamentales de notre plateforme. Chez nous, toute fonction d'importation se double d'une fonction d'exportation dans des formats lisibles par des machines virtuelles ou dans d'autres types de formats de données d'importation ou d'exportation. Nos outils sont toujours bidirectionnels.

Nous collaborons aussi beaucoup avec la communauté des codes sources ouverts en vue de la transférabilité des codes des applications, entre autres. Par exemple, bon nombre de nos plateformes sont compatibles avec les formats pour le débardage des conteneurs, tel Kubernetes pour la gestion de grappes de serveurs. Les utilisateurs peuvent très facilement créer des systèmes caractérisés par une très grande transférabilité des données entre les plateformes. Telles sont les attentes de nos clients, attentes auxquelles nous souhaitons répondre.

● (1110)

M. James Lawless: Vous dites que c'est comme Apache, suivant les lignes directrices des fondations du code source ouvert. Les normes du code source ouvert sont en train d'être consolidées et acceptées, je suppose, dans une certaine mesure. Peut-être s'agissait-il de concepts communautaires antérieurs au RGPD, mais ces concepts sont maintenant assez généralisés, n'est-ce pas?

M. John Weigelt: Tout à fait.

M. James Lawless: Oui, d'accord. C'est très bien. Merci.

Merci, monsieur le président.

Le président: Nous passons maintenant à Mme Xueling, de Singapour. Vous avez cinq minutes.

Mme Sun Xueling: Monsieur Davidson, vous avez dit tout à l'heure, en réponse à une question de M. Baylis, qu'en ce qui concerne les publicités politiques, vous aimeriez voir les entreprises adopter des mesures pour promouvoir la transparence. J'aimerais donner deux exemples dans lesquels les mesures prises par les entreprises n'ont pas été suffisantes.

En avril 2018, Facebook a mis en œuvre de nouvelles règles pour la transparence en matière de publicité politique. Chez Facebook, on a admis avoir pris beaucoup de temps pour déceler l'ingérence étrangère dans les élections américaines de 2016. On a dit avoir amélioré la transparence en matière de publicité et on a argué que, par conséquent, il y aurait une meilleure reddition de comptes. Pourtant, à la fin d'octobre 2018, Vice News a publié un rapport montrant à quel point il était facile de contourner les barrières que Facebook avait prétendu avoir mises en place. Les journalistes ont dû se soumettre à une vérification d'identité avant de pouvoir acheter des annonces publicitaires, mais une fois cette étape franchie, ils ont été capables de publier des annonces semant la discorde et de mentir au sujet de ceux qui les avaient payées.

Voilà pour Facebook.

Par ailleurs, en août 2018, Google a déclaré avoir investi dans des systèmes robustes visant à identifier les opérations d'influence lancées par des gouvernements étrangers. Cependant, peu de temps après, un organisme sans but lucratif nommé Campaign for Accountability a mené une expérience qui a été décrite en détail: des chercheurs de l'organisme ont prétendu travailler pour un organisme de recherche Internet, puis ils ont acheté des publicités politiques ciblant les internautes américains. Selon Campaign for Accountability, chez Google, on n'a pas tenté de vérifier l'identité du compte et on a approuvé les annonces en moins de 48 heures. Les publicités ont été diffusées sur un large éventail de sites Web et de chaînes YouTube, générant plus de 20 000 visionnements, et ce, pour un coût inférieur à 100 $.

Ainsi, il ne semble pas que les plateformes soient sur le point de remplir leur promesse de protection contre l'ingérence étrangère.

Êtes-vous d'accord avec ce que je viens de dire?

M. Alan Davidson: Manifestement, il nous reste beaucoup de travail à faire. Tout à fait. Nous qui travaillons dans ce domaine avons ressenti une frustration, car nous pensons que la transparence de la publicité est un outil extrêmement important pour accomplir cela. Les autres outils ne sont pas aussi efficaces.

Mme Sun Xueling: Oui. Il ne semble pas qu'il s'agisse d'un problème technique à proprement parler, puisque les chercheurs ont indiqué avoir utilisé l'adresse IP russe pour accéder aux plateformes de publicité russe de Google et fournir les détails de l'organisme de recherche Internet. Ils sont allés jusqu'à payer les publicités en roubles.

Voilà qui semble indiquer que le désir de vendre des publicités est plus fort que l'intention de réduire l'ingérence étrangère.

M. Alan Davidson: Je mettrais un bémol. Il est encore trop tôt pour dire ce qu'il en est. Il reste beaucoup à faire, à mon avis. L'expérience des élections en Inde et au Parlement européen sera peut-être instructive. Là-bas, les gens ont tenté d'adopter des mesures de manière beaucoup plus proactive. Nous devons être à même d'évaluer cela, je crois. C'est pourquoi, entre autres raisons, la transparence est importante.

Les plateformes doivent en faire plus, mais comme l'un de vos collègues l'a souligné, nous devrions aussi nous pencher sur les auteurs de ces actes...

Mme Sun Xueling: Tout à fait, oui.

M. Alan Davidson: ... et lorsque des États-nations s'en prennent à nos entreprises, nous avons besoin de l'aide du gouvernement.

Mme Sun Xueling: Plus tôt, vous avez parlé de garde-fous.

M. Alan Davidson: Oui.

Mme Sun Xueling: Je crois que c'est important pour que nous évitions de plonger dans l'abîme de la désinformation.

M. Alan Davidson: Je suis d'accord.

Mme Sun Xueling: Merci.

Merci, monsieur le président.

Le président: Merci.

Nous passons maintenant à Mme Vandenbeld. C'est à vous.

Mme Anita Vandenbeld: Je vais changer un peu le sujet de la conversation. Monsieur Davidson, dans votre déclaration préliminaire, vous avez mentionné le fait que votre entreprise met davantage l'accent sur la diversité de la main-d'œuvre. Nous savons — des témoins entendus ici l'ont aussi dit — que les algorithmes sont influencés par les préjugés sociaux de ceux qui en écrivent le code, de sorte que si la plupart des programmeurs sont des hommes dans la vingtaine, leurs préjugés sociaux seront reconduits par les algorithmes.

Dans quelle mesure est-il important de diversifier la main-d'œuvre? Comment vous y prenez-vous? Quelles sont les répercussions?

M. Alan Davidson: Selon nous, c'est extrêmement important. Non seulement est-ce la bonne chose à faire, mais nous soutenons aussi que les produits que nous créerons seront meilleurs si nous disposons d'une main-d'œuvre plus diversifiée qui reflète l'ensemble des communautés que nous desservons.

C'est un grand problème dans la Silicon Valley et dans le secteur de la technologie en général. Je pense que nous devrions tous l'admettre. Nous devons travailler là-dessus sans relâche.

Dans notre entreprise, nous en avons fait une très grande priorité. Par exemple, chaque année, tous les cadres de notre entreprise ont des objectifs. Nous parlons d'objectifs et de résultats clés. Chacun établit ses propres critères, mais il y a un critère qui est obligatoire pour tout le monde. La question se pose comme suit: dans quelle mesure avez-vous réussi à assurer la diversité dans votre processus d'embauche? Lorsque l'on se sait évalué, on a tendance à fournir un effort quelque peu accru.

Nous devons en faire plus à ce chapitre. Nous sommes les premiers à reconnaître qu'il nous reste du chemin à faire. Je pense que nous avons fait beaucoup de progrès en matière de diversité des genres, surtout parmi les membres de la communauté du domaine technique. Dans d'autres aspects de la diversité ethnique, nos résultats sont moins bons, il nous reste beaucoup à faire. Nous y travaillons vraiment.

● (1115)

Mme Anita Vandenbeld: Merci.

M. Alan Davidson: Merci d'avoir soulevé la question.

Mme Anita Vandenbeld: Pourrais-je demander à chacun des autres témoins de s'exprimer à ce sujet?

M. John Weigelt: Chez Microsoft, Satya Nadella en a fait une priorité absolue. Nous reconnaissons que nos décisions et nos produits sont meilleurs si notre entreprise reflète mieux les communautés que nous desservons.

Ici, au Canada, nous travaillons à faire en sorte que Microsoft Canada reflète la mosaïque culturelle du Canada, ce qui comprend non seulement le sexe, mais aussi les origines ethniques et l'orientation. De plus, pour les personnes qui ont des exigences d'adaptation et des méthodes de travail uniques, comme des problèmes de vision, d'ouïe ou d'attention...

Nous travaillons vraiment à forger une telle communauté en intégrant cet effort au sein de notre programme d'éthique de l'IA. Nous avons un comité de gouvernance qui se penche sur les utilisations délicates de l'IA. Ensuite, nous réunissons un groupe de personnes très diversifié pour examiner toutes les facettes de cette utilisation délicate. Nous voulons expressément obtenir le point de vue intersectionnel de toute personne de l'entreprise souhaitant émettre un commentaire afin de refléter cette mosaïque culturelle dont j'ai parlé. De cette façon, nous pensons être à même de tuer dans l'œuf certains effets imprévus potentiels, de manière à pouvoir donner des conseils et une orientation à l'avenir.

Mme Anita Vandenbeld: Allez-y.

M. Erik Neuenschwander: En plus de la protection des renseignements personnels, la diversité constitue l'une des quatre valeurs d'entreprise de notre PDG Tim Cook. Les deux valeurs sont très importantes. Cela va bien au-delà de l'IA. La protection de la vie privée relève surtout de la condition humaine. Pour ce qui est de la diversité des points de vue, elle nous aidera à faire de bons choix.

En matière de diversité dans notre entreprise, je n'ai pas les chiffres sous la main. Je suis sûr qu'il nous reste encore beaucoup de travail à faire. Nous avons adopté des mesures d'amélioration non seulement en matière de recrutement et de rayonnement visant à attirer des personnes de la diversité, mais aussi en matière de roulement ou de longévité de la carrière. Faire entrer une personne dans l'entreprise est une chose, s'assurer qu'elle a une expérience de carrière productive et enrichissante pour qu'elle reste dans l'entreprise et continue d'y contribuer en est une autre.

Comme je l'ai dit, nous avons encore du travail à faire sur ces deux aspects.

Mme Anita Vandenbeld: Merci.

M. Mark Ryland: La situation est similaire chez Amazon. Nous mettons beaucoup l'accent sur la diversité. Parmi nos objectifs d'entreprise, cet enjeu occupe une grande place. Les gestionnaires d'embauche et les cadres supérieurs sont tenus d'atteindre des objectifs précis à cet égard.

Bien entendu, ce n'est pas seulement une question d'embauche. C'est aussi une question de longévité de carrière, de gestion de carrière et de création de communautés d'intérêts au sein de notre entreprise. Ainsi, les gens sentent qu'ils font partie à la fois de l'entreprise dans son ensemble et de communautés d'intérêts qui leur ressemblent vraiment.

Nous travaillons très fort dans tous ces domaines pour accroître la diversité de l'entreprise. Encore une fois, nous pensons que c'est ce qu'il y a de mieux pour les affaires. Non seulement est-ce la bonne chose à faire, mais c'est aussi ce qui nous aidera à créer de meilleurs produits, parce que les origines diverses de nos employés correspondent aux clients que nous essayons de rejoindre.

Mme Anita Vandenbeld: Merci.

Le président: Merci, madame Vandenbeld.

J'aimerais expliquer le déroulement des choses. Nous aurons encore quelques interventions, puis nous entendrons les derniers commentaires des vice-présidents, du coprésident et de moi-même. Ensuite, ce sera terminé. Si nous dépassons les 11 h 30, ce sera de peu.

Monsieur Kent, vous avez cinq minutes.

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

J'aimerais revenir à la question de la concurrence, de l'antitrust et des monopoles dans le nouveau marché. On a beaucoup parlé récemment, particulièrement aux États-Unis, des nouveaux monopoles numériques et du fait qu'ils sont peut-être beaucoup plus durables que les monopoles du passé — les chemins de fer, les compagnies de téléphone, etc. Ces monopoles peuvent vaincre leurs concurrents en les achetant ou en les détruisant.

Hier, j'ai cité, à l'intention du représentant de Facebook qui comparaissait au Comité, les écrits de Chris Hughes, le cofondateur de Facebook, désormais désillusionné. Certains de nos témoins d'aujourd'hui ont laissé entendre que leurs entreprises seraient peut-être prêtes à accepter des déclinaisons de la loi européenne. Toutefois, M. Hughes a fait les manchettes en laissant entendre que Facebook devrait être démantelée et faire l'objet d'une démarche antitrust. Il a dit ceci: « Ce qui effraie chez Facebook, ce n'est pas quelques règles de plus. C'est une poursuite antitrust ».

Je sais que la défense contre les poursuites antitrust peut poser problème. En situation de monopole en matière de mégadonnées, vous invoquez l'excuse suivante: votre service est gratuit, il n'y a pas de coûts tangibles associés aux achats des consommateurs.

C'est peut-être une question trop vaste pour le poste que vous détenez, comme on l'a déjà dit. C'est pourquoi nous avions demandé que les PDG soient présents aujourd'hui. Je me demande tout de même, particulièrement dans le cas d'Amazon et de Microsoft, si vous pourriez nous parler du point de vue de vos entreprises visant à contrer ces discussions antitrust et les appels au démantèlement dans l'intérêt d'une plus grande concurrence et d'une plus grande protection des consommateurs.

Je pose d'abord la question à M. Ryland.

● (1120)

M. Mark Ryland: Je dirai volontiers quelques mots à ce sujet.

Comme je l'ai déjà dit, notre modèle d'affaires est très traditionnel. Nous vendons des biens et des services — lesquels ont une valeur pécuniaire — tant dans notre commerce de détail Amazon.com que dans notre entreprise d'infonuagique, et nous faisons face à une concurrence féroce pour toutes sortes de services et de plateformes qui ne se limitent pas à l'Internet. Les gens utilisent une grande variété de canaux et de mécanismes pour acquérir des services de TI, que ce soit pour l'infonuagique ou pour d'autres types de ressources. De notre point de vue, il s'agit tout simplement d'un modèle d'affaires très différent, et notre utilisation des données pour améliorer l'expérience des consommateurs est, à notre avis, très avantageuse pour les consommateurs. Ceux-ci apprécient vraiment l'expérience d'utilisation de ces technologies.

À mon avis, c'est une approche qui diffère beaucoup de certains enjeux que vous soulevez. Je m'en tiens à cette affirmation plutôt générale. En ce qui concerne les détails du droit de la concurrence, comme je l'ai déjà dit, je ne suis pas un expert.

Je pense vraiment que notre modèle d'affaires est très traditionnel à cet égard. C'est un peu différent, à mon avis.

L'hon. Peter Kent: Merci.

Je vais passer au témoin de Microsoft.

M. John Weigelt: Au vu de la longévité de notre entreprise, qui existe depuis les années 1970, nous avons connu des fluctuations. Nous avons eu un téléphone par le passé. Nous avons un excellent navigateur, mais celui-ci a subi un certain nombre de modifications. Auparavant, on disait: un ordinateur sur chaque bureau. Aujourd'hui, on dit plutôt: un téléphone dans chaque poche. Ces fluctuations traversent le milieu qui est le nôtre.

Pour ce qui est de l'environnement des données, les consommateurs se tourneront vers les services qui leur plaisent. Il y aura des fluctuations. Si vous parlez aux milléniaux, ils vous diront qu'ils utilisent différents services. Par exemple, mes enfants — qui, s'ils ne se considèrent pas comme des milléniaux, occupent le même espace —, diront ceci: « Papa, ne me parle pas sur cette plateforme, je ne suis pas là. Parle-moi sur cette autre plateforme ». Ces choses-là fluctuent.

Des données, on passe ensuite aux algorithmes. Nous entrevoyons une ère algorithmique et une monétisation des algorithmes. Nous assistons à une transition des algorithmes aux API, les gens tirant un profit pécuniaire de ces API.

Nous voyons ce moteur d'innovation en marche, qui va continuellement de l'avant. Nous devons travailler ensemble pour essayer d'anticiper les conséquences imprévues et d'apprendre en cours de route des leçons en matière de désinformation. C'est comme le jeu de la taupe: on n'a pas plus tôt frappé une taupe qu'une autre resurgit à un endroit imprévu. On s'exclame alors: « Oh, nous n'avions pas pensé à cela. » En travaillant ensemble, nous pouvons mettre en place les instruments pour y arriver.

J'ai donné une réponse abstraite à votre question au sujet de l'anticoncurrence et de l'antitrust, je sais, mais j'aimerais aborder la question sous l'angle général et sur le plan des fluctuations. Comment pouvons-nous mettre en place des mécanismes de protection solides pour les entreprises et les particuliers? Grâce à des partenariats.

L'hon. Peter Kent: C'est au tour des témoins d'Apple et de Mozilla.

M. Erik Neuenschwander: Je ne crois pas avoir grand-chose à ajouter aux observations des autres témoins. Je pense que nous essayons à la fois d'offrir la diversité de l'App Store à nos utilisateurs et de favoriser une grande concurrence. De nombreuses entreprises ont connu une grande réussite dans cet espace.

En ce qui concerne les données personnelles, nous pratiquons la minimisation des données et nous essayons de donner le pouvoir non pas à Apple, mais bien aux utilisateurs.

M. Alan Davidson: Je dirai simplement que je travaille pour une entreprise qui, d'une certaine façon, a pris naissance en réaction à Internet Explorer, qui était un joueur dominant dans le marché à l'époque. Nous croyons que la loi antitrust constitue un garde-fou très important pour le marché. Comme tout le monde, nous voulons qu'il y ait des règles du jeu équitables sur le plan de la concurrence.

À notre avis, il y a beaucoup de préoccupations au sujet de la taille des entreprises. Plus grande est la taille, plus grande est la responsabilité. Nous pensons aussi que les organismes de réglementation antitrust disposent de beaucoup d'outils très puissants à l'heure actuelle. Nous devons, je crois, réfléchir à la façon de donner à ces organismes plus d'information, plus d'outils et une meilleure compréhension des API et de la puissance des données dans leur analyse, notamment. C'est d'abord là que nous devons effectuer une mise à niveau, tandis que nous réfléchissons à la façon d'élargir les rôles. C'est un domaine très important.

● (1125)

L'hon. Peter Kent: Pour moderniser numériquement...?

M. Alan Davidson: Nous avons besoin d'une application contemporaine et numérique de la loi antitrust.

L'hon. Peter Kent: Merci.

Le président: Merci, monsieur Kent.

Le dernier intervenant est M. Graham. C'est à vous.

M. David de Burgh Graham: Merci.

J'ai posé des questions à tout le monde un peu plus tôt. J'aimerais donc discuter un peu avec M. Ryland d'Amazon.

Plus tôt, vous avez discuté avec M. Lucas de la question de savoir si la sécurité d'Alexa avait déjà été compromise. Si je me souviens bien, vous avez dit que non. Est-ce exact?

M. Mark Ryland: C'est exact.

M. David de Burgh Graham: Vous n'êtes pas au courant du piratage de Checkmarx d'il y a à peine un an, qui a complètement compromis Alexa et qui pourrait causer la diffusion en direct d'innombrables enregistrements audio?

M. Mark Ryland: Je n'étais pas au courant de ce... Je vais vous revenir là-dessus.

M. David de Burgh Graham: N'êtes-vous pas le directeur de l'ingénierie de sécurité?

M. Mark Ryland: Qu'est-ce que c'est?

M. David de Burgh Graham: N'êtes-vous pas le directeur de l'ingénierie de sécurité?

M. Mark Ryland: Oui, chez Amazon Web Services.

M. David de Burgh Graham: Vous travaillez pour Amazon Web Services; on ne nous a donc pas envoyé quelqu'un de Amazon. Je voulais simplement que ce soit clair.

Amazon a un système de marketing intégré. Si je cherche une information sur Amazon et je vais ensuite sur un autre ordinateur et un autre site Web, il y aura des annonces de Amazon me demandant si je veux acheter l'article que j'avais cherché antérieurement sur un autre appareil et avec une adresse IP différente. Que fait Amazon pour savoir cela? Quel genre d'échange de données y a-t-il entre Amazon et des sites comme Facebook et autres? Par exemple, National Newswatch me fait le coup.

Comment se fait cet échange d'information? Comment savez-vous qui je suis quand j'utilise un autre appareil?

M. Mark Ryland: Nous faisons des échanges publicitaires. Nous avons tout un site consacré à la vie privée, qui vous permet de désactiver la publicité. Cela dit, il ne s'agit pas de renseignements personnels. Les données sont anonymisées. Le système se fonde sur un profilage démographique.

Je répète qu'il est très simple de désactiver la publicité sur notre site Web. On peut également se valoir d'outils commerciaux, comme AdChoices, pour éviter de participer aux réseaux publicitaires.

M. David de Burgh Graham: Ce sont des données soi-disant anonymes, mais le système sait exactement ce que j'ai cherché il y a trois heures.

M. Mark Ryland: Je ne sais quoi vous dire dans votre cas précis, mais nous n'utilisons pas vos renseignements personnels à de telles fins.

M. David de Burgh Graham: D'accord.

Au tout début de la réunion, vous avez présenté des points de vue intéressants sur le consentement à l'utilisation des données, ce qui a suscité une excellente intervention de M. Angus. Selon Amazon ou selon vous, quelle est la limite de consentement pour la divulgation de données? Est-ce explicite? Suffit-il que la boîte précise qu'il s'agit d'un appareil « intelligent » pour que le consentement à divulguer des données soit sous-entendu?

M. Mark Ryland: Nous pensons que le plus logique, c'est d'être sensible au contexte. Le consommateur averti aura sûrement une idée de ce qui est en jeu. Si ce n'est pas le cas, il faudra nous arranger pour que ce soit plus explicite. C'est très contextuel.

Cela dépend aussi, bien entendu, du type de données. Certaines sont beaucoup plus délicates que d'autres. Comme l'un des panélistes l'a mentionné, utiliser une plateforme de jeux en ligne et consulter un site sur les soins de santé sont deux choses entièrement différentes; il faut donc connaître le contexte et le contenu. Le consentement fondé sur le contexte est tout à fait logique.

M. David de Burgh Graham: D'accord.

Vous avez dit plus tôt que votre entreprise est axée sur la clientèle. Accordez-vous autant d'importance à vos travailleurs?

M. Mark Ryland: Oui. Nous nous efforçons de le faire.

M. David de Burgh Graham: Vous ne suivez pas des pratiques antisyndicales?

M. Mark Ryland: Ce n'est pas mon champ d'expertise, mais je dirais que nous traitons nos travailleurs avec respect et dignité. Nous nous efforçons de leur offrir de bons salaires et des conditions de travail raisonnables.

M. David de Burgh Graham: Obtenez-vous des données de vos propres employés?

M. Mark Ryland: Comme toutes les entreprises, nous recueillons des données sur des aspects comme l'accès à Internet et l'utilisation responsable de notre technologie pour protéger les autres travailleurs.

M. David de Burgh Graham: Alors Amazon n'aurait jamais distribué de matériel promotionnel antisyndical à des entreprises nouvellement acquises.

M. Mark Ryland: Je ne suis pas au courant de ce genre de scénario.

M. David de Burgh Graham: Eh bien, j'espère que lors de notre prochaine réunion, nous pourrons compter sur un représentant de Amazon qui en sache plus long sur les politiques de l'entreprise. Vous maîtrisez sans doute les services sans fil évolués, mais ce qu'il nous faut, c'est nous faire une idée globale du fonctionnement de Amazon.

Je pense que c'est tout pour l'instant. Merci.

Le président: Merci, monsieur de Burgh Graham.

Il semble que j'ai oublié Mme Stevens du Royaume-Uni, et...

M. James Lawless: Monsieur le président, avant que vous ne donniez la parole à Mme Stevens, je dois m'excuser, car nous devons prendre l'avion.

Je voudrais simplement remercier les membres de tout le travail qui a été fait ces derniers jours.

Le président: D'accord. Merci. Nous vous reverrons en novembre prochain.

M. James Lawless: Absolument.

Le président: Toutes nos salutations à Mme Naughton. Merci d'être venus.

M. James Lawless: Merci beaucoup.

Le président: Allez-y, madame Stevens.

Mme Jo Stevens: Merci beaucoup, monsieur le président.

J'aimerais revenir à quelque chose que vous avez dit tout à l'heure, monsieur Weigelt, au sujet d'un conseil ou d'un groupe qui doit se pencher sur l'utilisation judicieuse de l'intelligence artificielle. Pouvez-vous me donner un exemple du genre de déploiement qui serait « judicieux » d'après vous?

● (1130)

M. John Weigelt: Il y a d'abord l'utilisation de l'intelligence artificielle dans le diagnostic médical. Il y a trois critères à examiner: le système peut-il approuver ou refuser des services corrélatifs? Y a-t-il atteinte aux droits de la personne ou à la dignité humaine? Y a-t-il des problèmes de santé et de sécurité?

Dans un cas, des chercheurs ont établi des algorithmes d'intelligence artificielle sur les radiographies pulmonaires. Ils ont ensuite voulu les incorporer à la salle d'urgence, pour en constater le fonctionnement et les effets sur les patients. Notre comité s'est réuni. Nous avons examiné les ensembles de données. Nous avons étudié la validité de cet ensemble de données ouvertes et le nombre de personnes visées. Nous avons ensuite déconseillé leur usage clinique aux chercheurs en cause en leur précisant que tout logiciel utilisé comme instrument médical est un domaine complètement différent. Il faut des certifications et tout le reste.

Un usage judicieux serait d'évaluer si l'intelligence artificielle peut oui ou non tirer des leçons de ces examens. C'est l'optique que nous avons tendance à adopter en la matière.

Mme Jo Stevens: C'est un exemple très utile. Merci.

Nous savons, et ce ne sont pas les preuves qui manquent, qu'il y a des préjugés délibérés et inconscients inhérents à l'intelligence artificielle. Je pense qu'il y a un argument assez solide en faveur d'une approche réglementaire pour régir son déploiement, un peu comme ce que nous avons dans, disons, le secteur pharmaceutique. Avant de mettre un médicament sur le marché, il faut en examiner les effets secondaires indésirables.

Qu'en pensez-vous? Pensez-vous qu'il y a un argument en faveur d'une approche réglementaire, particulièrement parce que, comme nous le savons, le déploiement actuel de l'intelligence artificielle est discriminatoire envers les femmes, les Noirs et les minorités ethniques? Des gens perdent leur emploi et n'ont pas accès à des services comme des prêts et des hypothèques à cause de cela.

M. John Weigelt: Absolument. Je pense que vous avez raison de parler du parti pris involontaire en ce qui a trait aux décisions en matière d'intelligence artificielle; il s'agit donc de nous protéger contre cela. C'est l'un des principes techniques sur lesquels nous travaillons fort pour donner des conseils et des directives à nos équipes.

Il y a certains domaines où nous avons préconisé une action très rapide et directe pour agir plus prudemment et plus délibérément, comme dans le cas du logiciel de reconnaissance faciale. Pour revenir à ce que vous disiez, bon nombre de ces modèles ont été formés en fonction d'une communauté très homogène et ne tiennent donc pas compte de la diversité des gens qu'ils doivent servir.

Nous sommes d'ardents défenseurs de la mise en place de cadres législatifs pour certains régimes de consentement, par exemple s'il faut des bannières dans les rues, s'il faut des paramètres, s'il faut définir la différence entre l'espace public et l'espace privé, et ainsi de suite.

Mme Jo Stevens: Dans quelle mesure êtes-vous prêt à rendre public le travail que vous avez fait? Je vous en sais gré si vous le faites officieusement. C'est très bien, mais il serait utile de savoir ce que vous faites et ce que font vos collègues.

M. John Weigelt: Absolument. Il est clair que nous devons mieux renseigner la collectivité de l'excellent travail qui est en cours. Nous avons publié des lignes directrices sur les robots et sur la façon de s'assurer qu'ils se comportent correctement, car figurez-vous que nous avons eu nos propres ennuis avec un robot sectaire qui a semé la discorde pendant un certain temps. Nous en avons tiré des leçons. Notre PDG a appuyé notre équipe et nous avons progressé. Nous avons fourni des conseils, et ils sont accessibles au public.

Nous avons ce qu'on appelle la AI Business School, qui propose toute une série de cours à l'intention des chefs d'entreprise pour mettre en place un modèle de gouvernance de l'intelligence artificielle. Nous travaillons avec ce milieu pour l'aider. Nous nous efforçons de diffuser le travail que nous faisons à l'interne dans le cadre de notre examen de l'éthique de l'intelligence artificielle.

Enfin, je dirais que nous travaillons dans le cadre d'une soixantaine d'activités d'orientation en matière de réglementation qui se déroulent partout dans le monde afin de commencer à socialiser cet aspect du point de vue de l'expérience pratique. Ici, au Canada, on s'occupe de mettre au point les critères d'évaluation de l'impact de l'intelligence artificielle et la norme d'éthique correspondante.

Mme Jo Stevens: Ce serait vraiment bien de voir un assistant virtuel coupé sur un patron tout autre que celui d'une femme servile. J'ai hâte de voir quelque chose de différent.

Merci.

Le président: Merci, madame Stevens.

Nous allons maintenant entendre les observations finales de nos vice-présidents, puis du coprésident.

Monsieur Erskine-Smith, voulez-vous commencer par vos 60 secondes, s'il vous plaît?

M. Nathaniel Erskine-Smith: Je pense que si nous avons tiré des leçons des derniers jours, c'est que nous continuons de vivre dans une ère de capitalisme de surveillance qui pourrait avoir de graves conséquences sur nos élections, sur notre vie privée, voire sur notre envie d'innover.

Malgré certaines frustrations, je crois que nous avons fait des progrès. Toutes les plateformes et toutes les entreprises de mégadonnées nous ont dit ce qu'elles n'avaient pas dit auparavant, à savoir qu'elles allaient adopter des règles plus rigoureuses en matière de protection de la vie privée et des données.

Hier, les responsables des plateformes ont fait remarquer qu'ils doivent rendre des comptes au public lorsqu'ils prennent des décisions sur le contrôle du contenu, et ils ont reconnu la responsabilité des entreprises à l'égard des répercussions algorithmiques. Il y a donc des progrès, mais il reste encore beaucoup de travail à faire en ce qui concerne la concurrence et la protection des consommateurs, et la reconnaissance de la responsabilité des algorithmes qu'ils utilisent, pour passer à une responsabilisation et responsabilité réelles lorsque les décisions ont des conséquences négatives.

Je pense qu'il y a encore beaucoup de travail à faire, et cela dépendra d'une coopération mondiale suivie. Je pense que notre communauté canadienne a su transcender les lignes de parti. Ce comité international travaille maintenant efficacement dans plusieurs pays.

La dernière chose que je dirai, c'est qu'il ne s'agit pas seulement de s'attaquer à ces graves problèmes mondiaux au moyen d'une coopération mondiale sérieuse entre les parlementaires; il faut une coopération mondiale de la part des entreprises. S'il y a une dernière chose à retenir, c'est que les entreprises ne l'ont tout simplement pas pris assez au sérieux.

● (1135)

Le président: Merci, monsieur Erskine-Smith.

Nous passons maintenant à M. Angus.

M. Charlie Angus: Merci à nos deux excellents présidents. Merci à nos témoins.

Je pense que nous avons vu quelque chose d'extraordinaire. Je suis très fier du Parlement canadien et de notre volonté de participer à ce processus.

Il y a eu des témoignages extraordinaires en ce qui a trait à la qualité des questions, et j'ai été très fier d'en faire partie. Deux faits extraordinaires, c'est que, au cours de mes 15 années en fonction, nous n'avons jamais réussi à transcender les lignes de parti sur ainsi dire quoi que ce soit, et pourtant, nous voilà réunis. De plus, nous n'avons jamais travaillé au-delà des frontières internationales. Nous pouvons remercier un dénonciateur canadien, Christopher Wylie, qui a lancé l'alerte sur le Tchernobyl numérique qui sévissait autour de nous.

Les politiciens, nous ne nous occupons pas des aspects techniques complexes. Ils nous effraient. Nous n'avons pas l'expertise nécessaire, alors nous avons tendance à les éviter, ce qui a été un grand avantage pour la Silicon Valley pendant des années.

Ces choses ne sont pas tellement techniques. Je pense que ce que nous avons fait ces deux derniers jours avec nos collègues d'autres pays — et ce que nous continuerons de faire à l'échelle internationale — c'est de rendre les choses aussi simples et claires que possible pour rétablir la primauté de la personne humaine dans le domaine des mégadonnées. La vie privée est un droit fondamental qui sera protégé. Les législateurs ont l'obligation et le devoir de protéger les principes démocratiques de notre pays, comme la liberté d'expression et le droit de participer à l'univers numérique sans faire proliférer l'extrémisme. Ce sont là des principes fondamentaux sur lesquels reposent nos démocraties. Ce qui était vrai à l'ère des lettres manuscrites est tout aussi vrai à l'ère de la téléphonie.

Je tiens à remercier mes collègues de leur participation. Je pense que nous sortons de nos réunions beaucoup plus forts qu'avant et nous prendrons encore plus de force à l'avenir. Nous voulons travailler avec les entreprises de technologie pour faire en sorte que le monde numérique soit un monde démocratique au XXI^{e} siècle.

Merci à tous.

Le président: Merci, monsieur Angus.

C'est votre tour, monsieur Colllins.

M. Damian Collins: Merci beaucoup, monsieur le président.

J'aimerais commencer par vous féliciter, vous et les membres de votre comité, de l'excellent travail que vous avez fait en organisant et présidant ces séances. Je pense que cette rencontre a réussi à faire exactement ce que nous espérions. Elle s'appuie sur les travaux que nous avions entrepris à Londres. Je pense que c'est un modèle de coopération entre les comités parlementaires de différents pays qui travaillent sur les mêmes questions et profitent mutuellement de leurs expériences et connaissances connexes.

Les séances ont été divisées entre ce que nous appelons les entreprises de médias sociaux hier et d'autres entreprises de données ici. En réalité, ce dont nous parlons, c'est que même s'il y a différentes fonctions, ce sont toutes des entreprises de données énormes. Ce qui nous intéresse, c'est la façon dont elles recueillent leurs données, si elles ont le consentement des intéressés, et ce qu'elles font de ces données.

Au cours des séances, nous avons vu à maintes reprises des entreprises refuser de répondre à des questions directes sur la façon dont elles obtiennent des données et dont elles les utilisent. Qu'il s'agisse de savoir comment Amazon et Facebook échangent les données... Même si c'est amplement diffusé, il demeure que nous ne le savons pas. Mon collègue, M. Lucas, a posé une question au sujet de l'échange des données de LinkedIn et de Microsoft. Il est possible d'intégrer totalement vos données LinkedIn à vos outils Microsoft, et une recherche rapide sur Google vous dira exactement comment faire.

Je ne comprends pas pourquoi les entreprises ne veulent pas parler ouvertement des outils qu'elles mettent en place. Les gens peuvent consentir à utiliser ces outils, mais comprennent-ils la portée des données qu'ils divulguent ce faisant? Si c'est aussi simple et direct qu'il semble, je suis toujours surpris que les gens ne veuillent pas en parler. Pour moi, ces séances sont importantes parce que nous avons l'occasion de poser les questions que les gens ne poseront pas et de continuer à insister pour obtenir les réponses dont nous avons besoin.

Merci.

Le président: Je vais d'abord m'adresser aux panélistes, puis je ferai quelques observations finales.

Je tiens à vous encourager. Vous aviez promis, surtout M. Ryland, de nous donner beaucoup de documents que vous n'avez pas... Divers commentateurs n'avaient pas toute l'information que nous demandions. Je vous implore de fournir les renseignements que nous avons demandés au greffier à mes côtés afin que nous puissions obtenir une réponse complète pour le Comité. Nous la distribuerons ensuite à tous les délégués ici présents.

Ce que je ne risque pas d'oublier de sitôt, c'est le commentaire de Roger McNamee au sujet de l'expression « poupées vaudou ».

Je regarde mes enfants. J'en ai quatre, âgés de 21, 19, 17 et 15 ans, respectivement. Je les vois devenir de plus en plus dépendants de ces appareils téléphoniques. Je vois le travail effectué par nos collègues à Londres au sujet de la dépendance que ces appareils peuvent créer. Je me demandais où on voulait en venir. On voit clairement que le capitalisme de surveillance, tout le modèle des affaires, ne demandent qu'une chose: garder ces enfants, nos enfants, collés au téléphone, même si c'est au prix de leur santé. C'est une question d'argent, tout simplement. Nous avons la responsabilité de faire quelque chose à ce sujet. Nous nous soucions de nos enfants, et nous ne voulons pas qu'ils soient transformés en poupées vaudou contrôlées par le tout-puissant dollar et le capitalisme.

Comme nous aimons tellement les appareils, je pense qu'il nous reste du travail à faire pour nous assurer que nous continuons d'offrir l'accès. Nous aimons la technologie et nous l'avons déjà dit. La technologie n'est pas le problème; c'est le véhicule. Nous devons nous attaquer aux causes de ces pratiques qui créent une dépendance.

Je vais dire merci et faire quelques derniers commentaires.

Merci à notre greffier. Nous allons l'applaudir pour s'être si bien tiré d'affaire.

Il a ce regard sur son visage parce que des événements comme celui-ci ne se déroulent pas sans ses petits problèmes. Nous nous en occupons au fur et à mesure, alors c'est difficile. Encore une fois, un gros merci à Mike MacPherson, pour avoir tout si bien résolu.

Je remercie également mon équipe — à ma gauche, Kera, Cindy, Micah, Kaitlyn — de m'avoir aidé à régler les questions administratives. Je pense qu'ils ont hâte de décompresser.

Avant de terminer, je vais encore évoquer... Oh, j'ai oublié les analystes. Désolé. J'oublie toujours nos pauvres analystes. Veuillez vous lever.

Merci pour tout.

Merci également aux interprètes. Il y avait trois langues à traduire, alors je vous remercie de nous avoir accompagnés toute la semaine.

Je salue notre ami Christopher Wylie, même si les sandwichs ont fini par avoir la vedette. Je ne sais pas si quelqu'un a vu ses gazouillis, « En plus d'une occasion ratée de faire preuve de démocratie, Zuckerberg a manqué toute l'action autour des sandwichs. » Notre ami m'a suggéré d'envoyer les restes par la poste au siège social de Facebook. C'est peut-être ainsi que nous réussirons à remettre la convocation en bonnes mains.

Je tiens à remercier tous les médias d'avoir accordé à cette question l'attention qu'elle mérite. C'est notre avenir et celui de nos enfants qui sont en jeu.

Encore une fois, merci à tous les panélistes qui sont venus de si loin, en particulier nos membres du Royaume-Uni, qui sont nos frères et sœurs de l'autre côté de l'océan.

Singapour est toujours là aussi. Merci d'être venus.

Passez une bonne journée.

Nous nous reverrons en Irlande au mois de novembre.

La séance est levée.