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 027 • 2e SESSION • 41e LÉGISLATURE

**TÉMOIGNAGES**

## Le jeudi 5 juin 2014

---

## Président

**M. Pat Martin**

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

**Le jeudi 5 juin 2014**

● (1110)

[*Traduction*]

**Le président (M. Pat Martin (Winnipeg-Centre, NPD)):** Bonjour, mesdames et messieurs. Je déclare la séance ouverte.

Nous nous excusons auprès de nos témoins; nous avons été retardés en raison de circonstances inévitables.

Bienvenue au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Nous sommes ici aujourd'hui pour poursuivre notre étude du problème grandissant du vol d'identité et de ses répercussions économiques.

Nous sommes très ravis d'accueillir aujourd'hui, de Rogers Communications inc., M. Kenneth Engelhart, vice-président principal, Réglementation et chef de la protection des renseignements personnels, et M. Aaron Storr, directeur, Soutien de l'exécution de la loi.

Ensuite, de Google, nous sommes ravis de revoir et d'accueillir M. Colin McKay, chef, Politiques publiques et relations gouvernementales.

Encore une fois, nous présentons nos excuses aux témoins. Nous savons que le timbre se fera entendre de nouveau d'ici environ 25 minutes. Nous allons donc vous demander de faire vos exposés. S'il reste du temps, nous allons le diviser également entre les trois partis, s'ils sont d'accord. Chaque parti pourra peut-être poser une ou deux questions, puis nous devrons quitter lorsque le timbre se fera entendre.

Cela dit, je crois savoir que nous avons une question liée aux travaux du comité dont nous devons discuter avant d'inviter les témoins à prendre la parole.

Monsieur Calandra.

**M. Paul Calandra (Oak Ridges—Markham, PCC):** Brièvement, je demande le consentement unanime pour convoquer Mary Dawson mardi prochain pendant 90 minutes; nous pourrions discuter des travaux du comité par la suite.

**Le président:** M. Calandra a-t-il le consentement unanime du comité?

Monsieur Ravignat.

**M. Mathieu Ravignat (Pontiac, NPD):** Il l'a, en effet, et je crois qu'il s'agit d'une période de temps très raisonnable. Nous avons hâte.

**Le président:** Monsieur Andrews, du Parti libéral.

**M. Scott Andrews (Avalon, Lib.):** Oui, cela me convient.

**Le président:** Très bien, c'est donc convenu. Nous allons avertir le greffier d'inviter la commissaire à l'éthique, Mary Dawson, à venir témoigner devant le comité dans le cadre d'une séance de 90 minutes.

C'est excellent.

D'accord, messieurs, nous allons suivre l'ordre sur la liste des témoins. Monsieur Kenneth Engelhart, de Rogers Communications, vous pouvez faire votre exposé, si vous le voulez bien.

**M. Kenneth Engelhart (vice-président principal, Réglementation et chef de la protection des renseignements personnels, Rogers Communications inc.):** Je vous remercie d'avoir invité Rogers Communications à comparaître devant le comité.

Vous avez élargi la portée de vos audiences pour inclure l'examen des renseignements communiqués aux entreprises de télécommunications aux organismes chargés d'appliquer la loi, et c'est justement le sujet que j'aborderai dans mon intervention.

Cette question intéresse vivement le public et les médias, et nous félicitons votre comité de ses efforts en vue de nous permettre d'expliquer publiquement nos procédures.

Rogers est une société canadienne offrant divers services de communications et de médias qui privilégient, d'abord et avant tout, les besoins de ses clients. Nous voulons leur offrir les meilleurs services de communications possible et garantir que leurs renseignements personnels sont conservés en toute sécurité. Toutefois, en tant qu'entreprise responsable, nous avons le devoir de coopérer avec les organismes chargés d'appliquer la loi qui demandent l'aide de Rogers dans le but d'assurer la sécurité de notre pays.

Je suis heureux de présenter le *Rapport sur la transparence de 2013* à votre comité. Publié ce matin, ce rapport contient plus de détails sur le nombre et le type de demandes que nous avons reçues en 2013 de la part d'agences gouvernementales et d'organismes chargés d'appliquer la loi. Nous sommes fiers d'être la première entreprise de télécommunications au Canada à partager ces renseignements publiquement.

Tel qu'indiqué dans le rapport, Rogers a reçu 174 917 demandes de renseignements relatifs aux clients en 2013. Ces demandes sont regroupées dans les six catégories que je vous décrirai maintenant.

Premièrement, les corps policiers et d'autres agences semblables présentent des mandats ou des ordonnances d'un tribunal nous obligeant à leur communiquer des renseignements relatifs aux clients.

Deuxièmement, certaines agences gouvernementales sont légalement habilitées à demander des renseignements. Par exemple, Revenu Canada détient ce type de pouvoir en vertu de la Loi de l'impôt sur le revenu.

Troisièmement, nous recevons des demandes urgentes provenant de centres de réception des appels au 911 ou de la part des policiers dans les situations où il y a danger de mort. Il peut s'agir d'affaires de disparition de personnes ou de cas de personnes en détresse. Nous les aidons à retrouver une personne possédant un téléphone cellulaire et nous fournissons les coordonnées de personnes ayant composé le 911, mais qui pourraient être dans l'impossibilité de communiquer.

Quatrièmement, la police nous envoie parfois une lettre indiquant qu'elle fait enquête sur l'exploitation d'enfants et qu'elle pourrait devoir obtenir des renseignements tellement vite qu'elle n'a pas le temps de se procurer un mandat ou une ordonnance auprès d'un tribunal.

Cinquièmement, nous recevons parfois des ordonnances d'un tribunal conformément à la Loi sur l'entraide juridique en matière criminelle. Ces demandes proviennent de pays étrangers ayant contacté le ministère de la Justice. Comme nous avons signé un traité ou une convention avec ces pays, nos tribunaux traitent leurs demandes. Veuillez noter que nous ne répondons pas à toutes les demandes que nous recevons. Lorsque nous estimons que la portée d'une ordonnance est trop vaste, nous la refusons, et, si nécessaire, nous nous adressons aux tribunaux pour contester la demande.

Le dernier domaine est celui qui, à mon avis, suscite le plus d'intérêt. Il s'agit des demandes ayant trait à la vérification des noms et des adresses des clients. Souvent, la police ne sait pas à quel fournisseur elle doit s'adresser pour demander un mandat. Par conséquent, il arrive, par exemple, qu'elle nous demande si une personne demeurant à telle adresse ou possédant tel numéro de téléphone est un client ou une cliente de Rogers. Nous répondons par un oui ou par un non. D'autres demandes semblables sont faites dans cette catégorie.

Nous croyons que ces renseignements sont utiles pour la police, car ils lui évitent de demander un mandat ciblant le mauvais fournisseur ou la mauvaise personne. Les journalistes se sont vivement intéressés à ces perquisitions sans mandat, bien qu'il s'agisse de la façon pour la police d'identifier contre qui elle devrait obtenir un mandat ou une ordonnance.

Par ailleurs, certaines agences américaines ont manifesté un grand intérêt pour l'acquisition de métadonnées sans mandat de perquisition. Je peux assurer au comité que Rogers ne transmet pas de métadonnées à quelque organisme canadien d'application de la loi que ce soit sans mandat de perquisition, que nous ne l'avons jamais fait et que nous ne le ferons jamais.

En outre, comme je l'ai indiqué plus tôt, nous ne traiterions jamais une demande que l'on pourrait qualifier d'interrogatoire à l'aveuglette. La protection des renseignements personnels de nos clients nous tient à coeur. Nous croyons qu'il est utile de faire preuve de plus de transparence, et nous encourageons le gouvernement du Canada à soumettre son propre rapport afin de faire davantage la lumière sur ces demandes.

Je me ferai un plaisir de répondre à vos questions.

● (1115)

**Le président:** Merci beaucoup, monsieur Engelhart. Nous vous remercions de vos remarques.

Nous allons maintenant inviter le représentant de Google à faire son exposé.

Monsieur Colin McKay.

**M. Colin McKay (chef, Politiques publiques et relations gouvernementales, Google inc.):** Merci beaucoup, monsieur le président.

Je suis ravi de comparaître de nouveau devant votre comité, la première fois cette session, pour parler d'un sujet important, soit la sécurité de l'information et le vol d'identité.

Mes commentaires n'en tiennent pas compte, mais j'aimerais d'abord vous dire que je suis ravi que Rogers ait présenté un rapport sur la transparence. Une bonne partie de ce que Ken a décrit se trouve dans un rapport semblable que nous publions tous les six mois et qui est affiché sur le site www.google.com/transparencyreport.

Je vais commencer par vous énumérer une courte liste, J'en ai deux, mais je vais en sauter une pour épargner du temps. Il s'agit d'une série de locutions: 123456, motdepasse, bienvenu, ninja, abc123, 123456789, 12345678, soleil, princesse et qwerty. Il s'agit effectivement de mots de passe obtenus lors d'une atteinte récente. La deuxième liste que j'avais est très semblable.

Malheureusement, lorsqu'il est question de sécurité de l'information, l'expérience démontre que le maillon le plus faible de la chaîne est souvent l'utilisateur.

Il ne faut pas se leurrer. Personne n'aime mémoriser des mots de passe complexes composés de chaîne de lettres, de chiffres et de caractères spéciaux, surtout dans un monde où chaque site Web nous demande de se connecter. Malheureusement, nous sommes tous des cibles possibles. À chaque mois, on tente d'infiltrer des réseaux, de voler des mots de passe et d'accéder à nos comptes.

Des témoins précédents vous ont parlé de groupes qui tentent de pirater des systèmes de paiement, de recueillir des numéros d'assurance sociale, de voler furtivement des données financières et de manigancer socialement leur insertion dans des bureaux ou des réseaux. Il peut s'agir d'attaques criminelles concertées ou simplement de tentatives maladroites de jeunes programmeurs.

Bien souvent, les criminels exploitent nos habitudes et notre volonté de croire qu'un ami Facebook est réellement dans une impasse à l'étranger, nous demandent de répondre à un faux avertissement de sécurité d'un fournisseur de service de courriel, ou nous font croire que le soutien du réseau tente réellement de communiquer avec nous et n'a besoin que de notre mot de passe pour nous offrir le soutien qui facilite tant notre travail.

Chez Google, nous élaborons des systèmes et des outils pour alerter nos utilisateurs de tentatives possibles d'atteinte à leur compte et à leur information. Nous donnons aux utilisateurs de l'information sur les sites qui pourraient tenter d'injecter des logiciels malveillants et prendre le contrôle de leur ordinateur, et nous travaillons très fort pour avoir les réseaux les plus sécuritaires au monde.

À une réunion précédente, j'ai posé cette question à votre comité qui se sert de Gmail, tout comme mon collègue, et il y a consensus à la table.

Gmail traite des milliards de messages chaque jour. Gmail a un bilan exceptionnel en matière de protection des utilisateurs contre les pourriels. Les utilisateurs de Gmail n'ont pas vu de pourriels dans leur boîte de réception depuis des années. En fait, lorsqu'un polluposteur tente d'utiliser un nouveau type de pourriel, nos systèmes le détectent souvent et le bloquent des comptes Google en l'espace de quelques minutes, et si par hasard il apparaît dans votre boîte de réception, vous pouvez cliquer su un bouton pour envoyer un signal à nos systèmes pour nous indiquer qu'à l'avenir, les messages semblables devraient être considérés comme des pourriels.

Qu'en est-il des résultats de recherche? Nos technologies examinent des milliards d'adresses URL sur le Web, à la recherche de sites Web dangereux.

Qu'est-ce que j'entends par dangereux? Il peut s'agir de site qui injecte des codes malicieux. Il pourrait tenter de vous convaincre de télécharger un logiciel qui contient un virus. Il peut s'agir d'hameçonnage, où l'on essaie de faire passer un site pour un site financier légitime.

Nous tentons de donner aux utilisateurs des indices visuels, comme des avertissements ou d'immenses interstitielles rouges qui indiquent de ne pas cliquer sur les liens dangereux. Le résultat? Chaque jour, nous détectons plus de 7 500 sites non sécuritaires et envoyons des avertissements à plus de 6 millions de résultats de recherche Google et un million de téléchargements.

Plus d'un milliard de personnes reçoivent de la protection contre l'hameçonnage et les logiciels malveillants chaque jour en raison des avertissements que nous montrons aux utilisateurs relativement aux sites Web dangereux grâce à nos efforts de navigation sécuritaire. Nous partageons ces données avec d'autres navigateurs, Safari et Firefox, afin que leurs utilisateurs soient protégés également.

Après tout, le but est de protéger Internet contre les comportements illicites et les expériences extrêmement mauvaises pour les utilisateurs, le vol d'identité étant le pire résultat possible.

Chez Google, nous travaillons continuellement à la sécurité des réseaux et des données. La sécurité est une partie essentielle de notre culture en matière de génie. À nos bureaux en Californie, à New York, à Munich, à Zurich et à Montréal, nous avons une équipe de plus de 250 experts en génie de la sécurité dont le travail est d'aider l'entreprise à demeurer à la fine pointe de l'innovation en matière de sécurité de l'information.

Revenons aux mots de passe. Nous pouvons convenir que les mots de passe sont un compromis entre la sécurité et la commodité. À titre d'utilisateur, on laisse souvent tomber la sécurité pour favoriser la commodité.

Par curiosité, les gens dans la salle savent-ils pourquoi qwerty est un mot de passe populaire? Il s'agit des cinq lettres dans le coin supérieur gauche du clavier. C'est la même combinaison en Russie sur le clavier cyrillique.

● (1120)

La difficulté consiste à créer un processus de vérification qui soit suffisamment complexe pour freiner ou empêcher les tentatives d'accès aux comptes, mais qui reste suffisamment pratique pour l'utilisateur moyen. Pour ce faire, il faut souvent innover.

En 2011, nous avons lancé un processus de vérification en deux étapes des comptes Google. Pour procéder à cette vérification, vous devez confirmer votre identité au moyen d'un mot de passe et d'un autre code transmis à un dispositif différent, que ce soit un téléphone, un dispositif USB distinct sur votre ordinateur, quelque chose de bien précis. Cela ajoute un élément plus solide de sécurité pour l'ouverture d'une session. Même si un voleur ou un pirate arrive à voler votre mot de passe, il ne suffit pas pour accéder à votre compte. Nous offrons gratuitement cette protection aux détenteurs de comptes.

Qu'en est-il des réseaux? Depuis un an, nous avons élargi à l'ensemble de la séance le protocole de cryptage SSL, ou Secure Sockets Layer, pour qu'il s'ouvre par défaut quand vous ouvrez une session dans Gmail, Google Search, Google Docs et bien d'autres services. Cette mesure de protection empêche les curieux de s'immiscer dans votre activité quand vous êtes dans un réseau ouvert, par exemple quand vous utilisez votre ordinateur portatif dans un café.

Nous avons crypté les données qui circulent entre nos centres de données, et nos experts de la sécurité s'efforcent constamment d'élargir et de renforcer cette protection pour englober plus de services et de liens. Cette semaine, nous avons diffusé un outil pour aider nos utilisateurs à déterminer quelle part des courriels envoyés entre Gmail et les fournisseurs de services de courriels externes sont cryptés en cours de route. Après cela, on peut avoir un système de cryptage plus solide dans l'ordinateur personnel, mais quand on envoie des courriels à quelqu'un dont le système n'est pas sécurisé, cette partie de l'échange n'est pas protégée. C'est important, parce que les courriels ne sont pas cryptés en chemin à moins que les fournisseurs de courriels de l'expéditeur et du destinataire appuient ce système.

Pour terminer, nous réagissons rapidement aux menaces qui sont décelées. Nous avons les programmes Chromium et Web Vulnerability Reward, et nous payons généreusement des pirates et des chercheurs en matière de sécurité pour cerner les failles et les points faibles de nos programmes et services sur le plan de la sécurité. Depuis quatre ans, nous avons ainsi dépensé près de 3 millions de dollars.

Ce qui est important, c'est que quand un exploit de sécurité est recensé, on fait les ajustements nécessaires et on le diffuse à des centaines de millions d'utilisateurs en quelques heures. Je vous explique la séquence: un chercheur en matière de sécurité, qui travaille sur un point faible particulier de notre système trouve un moyen d'obtenir le contrôle du système en quelques mois, participe à un concours et nous en parle. Nous lui proposons une belle somme, et à la fin de la journée, ce n'est plus un point faible parce que nos ingénieurs s'en sont emparé et ont résolu le problème.

Google ne ménage pas ses efforts pour s'assurer que les renseignements de nos utilisateurs sont sûrs, protégés et toujours disponibles. Notre engagement à l'égard de la sécurité des données de nos utilisateurs est absolue, et nous allons continuer de lutter contre tous ceux qui tentent de la compromettre.

Je vous remercie.

**Le président:** Je vous remercie de cet excellent et très instructif exposé, comme toujours.

Par bonheur, il nous reste une vingtaine de minutes. À ce que nous avons compris, le timbre commencera à retentir aux environs de 11 h 45. Cela nous laisse, je pense, suffisamment de temps pour un tour d'interventions de cinq minutes pour chaque parti. Si les membres du comité en conviennent, c'est ainsi que nous allons procéder.

Nous allons donc commencer par l'opposition officielle, le NPD, avec M. Mathieu Ravignat.

Mathieu, vous avez cinq minutes.

**M. Mathieu Ravignat:** Je remercie les témoins d'être ici. C'est un plaisir de vous voir ici au comité.

Je crois qu'on peut dire sans risque de se tromper que les Canadiens s'inquiètent plus que jamais de la protection de leur vie privée, que d'une certaine façon, nous ne suivons pas la cadence de l'évolution de la technologie, et peut-être aussi que l'éducation du public ne la suit pas non plus. Je pense que dans une certaine mesure, les entreprises de télécommunications, en cette période de transition, doivent assumer leur responsabilité sociale et informer leur clientèle.

Je m'inquiète aussi des atteintes à la vie privée qui se produisent au gouvernement, et de la relation entre le gouvernement et les compagnies de télécommunications. Il semble que le gouvernement ait demandé accès à des quantités alarmantes de renseignements personnels. Je me demandais si vous pouviez nous expliquer pourquoi vous n'informez pas vos clients quand le gouvernement vous demande des renseignements sur eux.

● (1125)

**M. Kenneth Engelhart:** Je vous remercie de cette question.

Je pense que le rapport que nous avons fait circuler ce matin est la première étape pour permettre à nos clients, aux membres de votre comité, au gouvernement et aux intéressés de comprendre la mesure dans laquelle les organismes d'application de la loi demandent ces renseignements. Je pense qu'à mesure que les compagnies fourniront ces renseignements, on commencera à avoir un tableau de la situation, qui pourrait éclairer le débat.

Pour ce qui est des données précises...

**M. Mathieu Ravignat:** Excusez-moi, mais vous m'avez fait penser à quelque chose. En l'absence d'un mandat, vous n'êtes pas tenu de fournir ces renseignements aux organismes d'application de la loi, n'est-ce pas?

**M. Kenneth Engelhart:** C'est exact.

**M. Mathieu Ravignat:** Mais vous décidez néanmoins de le faire?

**M. Kenneth Engelhart:** Ce n'est que dans des situations très précises, et il ne s'agit en fait que de données comme le nom et l'adresse, ou dans les situations d'urgence.

En cas d'urgence, évidemment, on le fait parce que la vie de quelqu'un est en danger et que les policiers n'ont pas le temps d'obtenir un mandat. Pour ce qui est du nom et de l'adresse, par exemple, à savoir si Colin McKay est un client de Rogers, nous répondons par « oui » ou « non »; autrement, ils vont se munir d'un mandat. S'il se trouve que Colin McKay n'est pas notre client, ils vont s'adresser à Telus. S'il n'est pas son client, ils se tourneront vers Bell. Cela fait gagner du temps aux policiers. Nous ne pensons pas que ce soit une atteinte aux droits de nos clients, parce que c'est tout simplement un moyen de faire gagner du temps aux policiers, qui sauront pour quelle compagnie obtenir le mandat. C'est pourquoi nous le faisons.

**M. Mathieu Ravignat:** Mais ces renseignements sont accessibles ailleurs.

**M. Kenneth Engelhart:** Bien souvent, oui. Il y a moyen de faire une recherche inversée de certains de ces renseignements sur Internet. C'est une autre des raisons qui fait qu'on ne pense pas que c'est tellement important.

**M. Mathieu Ravignat:** Mon cynisme me porte à demander pourquoi, alors ils s'adressent à vous. Il ne paraît pas tellement logique qu'ils vous demandent des renseignements qu'ils pourraient obtenir ailleurs, ou qu'ils sont habitués d'obtenir ailleurs, à moins qu'ils obtiennent d'autres types de renseignements.

**M. Kenneth Engelhart:** Permettez-moi de vous donner un exemple pour l'expliquer.

Il existe, dans le système de télécommunications, quelque chose qui s'appelle la conservation de numéro. Disons que vous êtes un client de Rogers et que vous avez pris la terrible décision de devenir un client de Bell. Il vous serait possible de transférer votre numéro de Rogers à Bell. Il se pourrait bien que le numéro qu'on a trouvé sur Internet soit le vôtre, mais ce n'est plus le numéro d'un client de Rogers. C'est l'une des raisons qui pourrait les amener à s'adresser à nous.

Il peut aussi arriver que le numéro soit remis dans le bassin des numéros et ait été attribué à un autre client, alors que sur Internet, il apparaît encore au nom du premier client.

Voilà donc le genre de raisons qui les amènent à s'adresser à nous, pour gagner du temps.

Je peux vous assurer que nous préférerions simplement fournir un service téléphonique. S'il n'en tenait qu'à nous, nous préférerions ne pas avoir à répondre à cette demande de la police, pas du tout, mais nous avons une entreprise socialement responsable et nous essayons de trouver le juste équilibre entre faire tout en notre pouvoir pour...

**M. Mathieu Ravignat:** À l'interne, avez-vous des critères ou des normes, ou même un processus d'examen pour gérer ces demandes qui, parfois, vous fait dire, « Non, je regrette, mais je ne peux pas vous fournir ces renseignements »?

Aussi, est-ce que le gouvernement demande des renseignements que vous ne fournissez pas? Pouvez-vous confirmer qu'il vous a demandé des renseignements que vous refusez de fournir?

**M. Kenneth Engelhart:** Oh, bien sûr.

**Le président:** Votre réponse devra être très brève, monsieur Engelhart.

**M. Kenneth Engelhart:** Oui, c'est juste.

**M. Mathieu Ravignat:** Il vous a demandé plus de renseignements que ce que vous êtes prêt à fournir?

**M. Kenneth Engelhart:** Il demande ce qu'il a le droit de demander, mais lorsqu'il n'est pas autorisé à demander certains renseignements, souvent, nous refusons de les lui fournir.

**M. Mathieu Ravignat:** C'est inquiétant.

**Le président:** Je regrette, mais votre temps est écoulé, monsieur Ravignat.

Nous passons maintenant au Parti conservateur, pour cinq minutes. Monsieur Calandra, vous avez la parole.

● (1130)

**M. Paul Calandra:** Je vous remercie, monsieur le président.

Je remercie également les témoins.

Monsieur McKay, je dois vous dire que j'étais au comité plusieurs fois lorsqu'il a donné du fil à retordre à Google, mais je pense que je vais me concentrer aujourd'hui sur Rogers pour un moment.

Peut-être serez-vous étonné, mais je tiens à vous féliciter pour ce rapport, monsieur Englehart. Je ne sais pas si Bell ou Telus produisent des rapports comme celui-ci, mais il est très instructif. Je ne sais pas si on pourrait demander à Bell ou à Telus s'ils préparent ce genre de documents, mais je pense que ces rapports aident vraiment à comprendre ce qu'est l'accès.

M. Ravignat a parlé du gouvernement qui accède aux données ou qui communique avec vous. Je pense qu'il a donné l'impression que le Cabinet du premier ministre vous appelle pour vous demander des renseignements sur un abonné. Est-ce que c'est ce dont il est question ici? Quand on parle du gouvernement, vos statistiques semblent indiquer que c'est le ministère du Revenu ou un organisme d'application de la loi qui vous appelle. Est-ce que je me trompe, ou est-ce bien le genre de demandes que vous recevez?

**M. Kenneth Engelhart:** C'est tout à fait exact, monsieur. C'est soit un ministère qui a un pouvoir conféré par la loi de faire cette demande, soit un organisme d'application de la loi.

**M. Paul Calandra:** Dans le cas des organismes d'application de la loi, nous en avons beaucoup entendu parler, et j'ai moi-même fait des recherches inversées. Quand je suis revenu ici, en octobre, il y avait un petit problème avec le Sénat, et il y avait eu des échanges de courriels et d'appels téléphoniques qui étaient presque troublants, pour ainsi dire. Dans ce genre de cas, on peut faire une recherche inversée et on peut voir, mais la question de la conservation du numéro pose problème parce qu'il arrive que des gens passent de Rogers à Bell.

Quand la police communique avec vous, je me demande si vous avez des exemples de situations d'urgence. Avez-vous un exemple où la police a demandé à Rogers de l'aider, et pouvez-vous nous dire le type de renseignements que vous avez fournis ou la nature de la situation d'urgence?

**M. Kenneth Engelhart:** Oui, en fait, mon collègue, M. Storr, et moi-même avons pris l'avion ensemble aujourd'hui, et il m'a montré un courriel de remerciements qu'il a reçu ce matin. Un policier atteint du trouble de stress post-traumatique avait signifié sur un site Web son intention de se suicider. Le groupe de M. Storr a reçu une demande d'accès d'urgence pour connaître le nom de la personne associée à cette adresse IP. Il a fourni le nom et l'adresse et, ce matin, il a reçu une note de remerciements pour avoir contribué à sauver la vie de cet homme.

Ce genre de chose est très courant. On reçoit ces demandes tout le temps.

**M. Paul Calandra:** Cette question pourrait vous paraître injuste, alors je vais vous la poser à tous les deux. Quels sont ces investissements dont vous parlez? Je suppose que la protection de l'identité représente quelque chose d'énorme... Je ne veux pas dire que c'est un problème nouveau, mais la façon dont des gens s'en prennent à l'identité d'autres personnes est en train de changer, c'est évident. Quels genres de ressources... Je sais que vous avez dit avoir 250 ingénieurs, Colin, mais quel est cet investissement financier dont vous parlez, tous les deux, pour lutter contre le vol d'identité?

Colin, voulez-vous répondre en premier?

**M. Colin McKay:** Je pense que la réponse ne peut être que de nature anecdotique puisque, de toute évidence, nous sommes très bien placés pour faire d'importants investissements. La raison pour laquelle de nouvelles compagnies et de nouvelles initiatives de logiciels sont souvent victimes d'atteintes à la protection des données et d'activités criminelles à grande échelle, c'est le manque de ressources qu'elles consacrent à la sécurité. Leurs compétences et leurs investissements sont trop faibles.

Nous parlons d'investissements importants dans l'infrastructure technique. Aussi, on s'arrache les gens qui comprennent ce monde et qui comprennent les vulnérabilités les plus récentes et la façon de les résoudre. Aussi, il y a la question de la conformité et du régime juridique qu'il faut pour créer le genre de structure hiérarchique qu'a décrite Rogers aujourd'hui, afin de gérer les demandes des organismes d'application de la loi de façon juste, équitable et rapide. C'est un investissement de taille.

Nous sommes disposés à le faire parce que nous avons besoin de maintenir la confiance de nos utilisateurs et de leur rendre des comptes, mais très franchement, c'est un défi constant. Bien souvent, il faut partager des ressources entre compagnies également.

● (1135)

**Le président:** Merci, monsieur Calandra. Votre temps est écoulé.

Je suis désolé pour cette version écourtée de ce qui constituerait des renseignements intéressants et importants.

C'est maintenant au tour des libéraux. Nous entendrons M. Scott Andrews, qui dispose de cinq minutes.

**M. Scott Andrews (Avalon, Lib.):** Merci beaucoup, monsieur le président.

Monsieur Engelhart, les 87 000 demandes auxquelles vous répondez par oui ou par non prennent évidemment beaucoup de temps. Existe-t-il une entité centralisée au sein de votre entreprise pour le traitement de ces demandes? Si la demande exige davantage qu'une réponse par oui ou par non et qu'elle atteint un niveau plus élevé d'urgence, comment est-elle traitée à l'interne?

**M. Kenneth Engelhart:** M. Storr gère une équipe de professionnels en service 24 heures sur 24, 7 jours sur 7. Ce groupe traite ce type de demandes et les demandes provenant du 911.

**M. Scott Andrews:** Vous avez parlé des adresses IP qui ne sont pas données. Pourriez-vous nous donner un exemple où une adresse IP serait fournie? Dans quelles circonstances fournirait-on une adresse IP?

**M. Kenneth Engelhart:** On fournit l'adresse IP seulement en vertu d'un mandat, ou si vous avez remarqué les chiffres, vous voyez qu'il y a 711 cas relatifs à l'exploitation d'enfants. Dans ces cas précis, on fournit l'adresse IP. On la fournit aussi en cas d'urgence. Ce sont là les trois catégories.

**M. Scott Andrews:** Il y a 9 000 demandes urgentes. Croyez-vous que ce chiffre est élevé ou raisonnable? Si je fais le calcul rapide, cela signifie 25 par jour. S'agit-il d'un chiffre raisonnable?

**M. Kenneth Engelhart:** Oui, mais il faut garder à l'esprit que la plupart de ces demandes proviennent de la police. Un chiffre probablement cinq fois plus élevé de demandes provient des téléphonistes du 911, qui font parfois partie des corps policiers et parfois non. Donc le chiffre est encore plus élevé, mais puisqu'il s'agit de téléphonistes du 911, on ne considère pas ces demandes comme une demande provenant d'un organisme d'application de la loi. On considère qu'il s'agit d'une demande par téléphone. C'est pourquoi elles ne sont pas incluses dans les 9 000 demandes.

**M. Scott Andrews:** Lorsqu'on entend parler de vol d'identité, on entend dire que des fraudeurs fabriquent des identités. Souvent, ils obtiennent une adresse, un numéro de téléphone et ainsi de suite. Pouvez-vous nous éclairer au sujet des fraudeurs qui tentent d'usurper l'identité de quelqu'un, d'obtenir un numéro de téléphone et de fabriquer ce genre d'identité? Pourriez-vous ensuite faire un lien avec les téléphones jetables et les personnes qui revendent des téléphones? Dans quelle mesure est-ce important pour les voleurs d'identité?

**M. Kenneth Engelhart:** Oui, je suis entièrement d'accord avec Colin. Il existe des failles et des attaques au moyen de technologies de pointe, mais aussi des attaques au moyen de technologies plus conventionnelles. Nous avons un grand nombre d'ingénieurs et d'informaticiens à notre service qui protègent constamment notre réseau contre les attaques, mais il ne faut pas oublier les technologies plus conventionnelles. Prenez l'exemple de ce qui s'est passé avec Target aux États-Unis, où les renseignements personnels de 40 millions de clients ont été volés. Tout a commencé lors de l'embauche d'un responsable de l'entretien à un magasin Target qui a réussi à installer des appareils la nuit lorsque personne ne pouvait s'en apercevoir.

Il existe aussi un réel problème, lorsque le crime organisé infiltre des centres d'appels et des magasins pour tenter de voler des identités. Il faut être très vigilant, tant avec les technologies de pointe qu'avec les technologies plus conventionnelles. Il faut aussi se méfier des bons vieux escrocs, qui téléphonent aux centres d'appels et qui se font passer pour vous ou pour moi. Dans tous les cas, il faut être vigilant.

Nous luttons contre le vol d'identité à tous les jours et à tous ces niveaux.

**M. Scott Andrews:** Colin, à propos des comptes de courrier électronique fictifs et de ceux qui les créent pour fabriquer une identité, quelle est l'ampleur de ce problème? Êtes-vous souvent en communication avec les organismes d'application de la loi concernant des personnes qui établissent ce type de comptes pour fabriquer des identités?

**M. Colin McKay:** Je ne peux pas vous dire précisément si nous entretenons une relation avec les organismes d'application de la loi à cet égard, mais je peux vous dire que tout service de courrier électronique ouvert offre un certain niveau d'anonymat ou permet l'utilisation de pseudonymes, ce qui permet de créer un compte de courrier électronique en utilisant n'importe quel nom ou n'importe quelle identité. Notre entreprise érige certaines mesures de sécurité dans le cadre de sa relation avec les clients, parce qu'à partir du moment où vous commencez à fournir davantage de renseignements à votre sujet, ils sont de plus en plus difficiles à inventer. On a besoin de plus d'un élément de vérification, mais le processus demeure assez facile à mettre en place.

De l'autre côté, si les organismes d'application de la loi cherchent des renseignements à propos d'un compte, je dois répéter ce que Ken a dit à propos des processus suivis par Rogers. Nous ne fournissons pas de renseignements sans mandat, sans ordonnance de la cour, sauf si les circonstances l'exigent, dans les cas où il y a des risques de méfait ou des images d'enfants à caractère sexuel. Dans ces cas-là, nous déployons autant d'efforts que possible en collaboration avec nos partenaires de longue date afin de mettre fin à ces activités et de fournir les renseignements pour assurer un suivi.

● (1140)

**Le président:** Il vous reste 30 secondes.

**M. Scott Andrews:** Kenneth, à propos de l'aide fournie par Rogers aux victimes de vol d'identité, l'entreprise dispose-t-elle de mécanismes d'aide pour ces victimes?

**M. Kenneth Engelhart:** Si l'un de nos clients est victime d'une atteinte à la protection des données, nous l'avisons immédiatement. Ensuite, nous lui donnons un accès gratuit à la surveillance de la limite de crédit afin qu'il puisse surveiller son dossier de crédit et ainsi s'assurer que son identité n'a pas été usurpée.

**M. Scott Andrews:** Merci.

**Le président:** Juste à temps. Merci beaucoup, monsieur Andrews.

Nous disposons encore de quelques minutes. J'ai décidé que nous devrions poursuivre jusqu'à la toute dernière minute. C'est maintenant au tour des conservateurs. M. Calandra a de nouveau la parole.

**M. Paul Calandra:** Merci beaucoup.

Pouvons-nous demander aux représentants de Bell et de Telus, avant qu'ils viennent témoigner, s'ils ont un système semblable?

Je ne sais pas si vous pouvez nous renseigner à ce sujet.

**Le président:** On peut demander aux analystes de s'en enquérir.

**M. Kenneth Engelhart:** Nous sommes les premiers à le faire, alors ils y travaillent probablement en ce moment même.

**Des voix:** Oh, oh!

**M. Paul Calandra:** C'est une très bonne idée, et c'est une chose que nous prendrons sans doute en considération dans notre rapport. Merci.

Encore une fois, j'aimerais revenir sur...

Veuillez m'excuser. Je me sens coupable et peut-être que je devrais divulguer, monsieur le président, que j'ai déjà travaillé chez Rogers lorsque j'étais à l'école secondaire et à l'université. Je répondais aux demandes relatives à la câblodistribution par téléphone. Je dois admettre que même à l'époque — et voilà, je me sens coupable —, Rogers prenait vraiment les renseignements personnels au sérieux. Je pense qu'à l'époque, l'entreprise s'était dotée d'un des systèmes les plus avancés.

À mon arrivée au gouvernement provincial, j'ai amené des ministres du gouvernement pour une visite afin qu'ils constatent comment fonctionnent vos systèmes — cette visite remonte à 1995 ou 1996 — en ce qui concerne la protection des renseignements personnels et les façons dont il serait plus facile pour les clients d'obtenir de l'information. J'ai toujours pensé que vous étiez des chefs de file dans ce domaine.

J'aimerais revenir sur la vérification du nom et de l'adresse parce qu'il s'agit d'une question qui inquiète beaucoup les gens.

D'un côté, vous ne fournissez qu'une confirmation afin que la police puisse s'orienter. Il s'agit tout simplement d'un mécanisme pour économiser du temps, faisant en sorte que dans certains cas, la police évite le dédoublement extraordinaire de renseignements ou évite de consulter différentes sources et ainsi ils n'ont qu'à vous consulter pour s'assurer d'obtenir la bonne information afin d'obtenir leur mandat. Pour l'essentiel, vous protégez les droits garantis par la Charte, vous ne fournissez que des renseignements de base à la police.

**M. Kenneth Engelhart:** C'est exact, monsieur.

**M. Paul Calandra:** En plus, ce n'est pas n'importe qui au gouvernement qui s'immisce dans vos affaires et qui demande... Ce n'est pas Paul Calandra qui appelle Rogers et dit, « Voici les renseignements que je veux ». Il s'agit uniquement des services d'urgence et des institutions gouvernementales y étant autorisés par la loi.

**M. Kenneth Engelhart:** Oui, il s'agit essentiellement de la police.

**M. Paul Calandra:** Pourriez-vous m'expliquer un peu les métadonnées? L'un de vous peut-il expliquer le pouvoir... Là encore, au bout du compte, je suis un peu gêné, parce que je devrais... On me fournit différentes descriptions des effets néfastes que les métadonnées pourraient avoir.

Colin, ou tous les deux, pouvez-vous nous parler des métadonnées et des raisons pour lesquelles elles devraient nous traumatiser?

**M. Colin McKay:** Selon moi, dans le contexte de votre étude actuelle sur le vol d'identité, les métadonnées constituent un élément, mais un élément mineur de ce qui est utilisé pour créer une identité. Si quelqu'un essaie de commettre un vol d'identité, il doit connaître des renseignements bien précis sur un individu ou alors créer ces renseignements pour établir un cyberorganisme viable à moitié fonctionnel.

Les métadonnées en soi portent plutôt sur des transactions, sur vos intérêts et sur la transmission de données. Dans certains contextes, les métadonnées peuvent être extrêmement pertinentes, comme les adresses IP. Mais s'il s'agit de vos préférences en matière de recherche, de vos résultats de recherche ou même de l'historique de votre emplacement, c'est un peu moins vrai. La raison pour laquelle vous avez entendu toute une série de définitions est que, selon la personne à laquelle vous vous adressez et le contexte dans lequel les métadonnées sont appliquées, elles peuvent avoir toute une série d'applications très différentes et constructives.

● (1145)

**M. Kenneth Engelhart:** Pour le système téléphonique alors, les métadonnées ne sont pas les renseignements échangés au cours de l'appel; c'est qui on appelle, qui vous appelle, et le lien entre les deux. Ce peut même être l'endroit à partir duquel on appelle.

Les métadonnées sont un outil particulièrement utile pour l'application de la loi. Admettons que les autorités soupçonnent une personne et que cette personne connaît une autre personne que l'on sait, de source sûre, a été impliquée dans un crime. Si ces deux personnes s'appellent, c'est un outil important pour la police.

Je l'ai dit et je le répète: nous fournissons les métadonnées uniquement sur production d'un mandat de perquisition ou d'une ordonnance. Jamais nous ne le ferions autrement.

**M. Paul Calandra:** Entendu.

**Le président:** Nous allons devoir vous interrompre. Vos cinq minutes sont écoulées et, en plus, la sonnerie se fait entendre et les lumières clignotent. Nous n'avons pas le choix: quand la sonnerie retentit, nous devons filer en vitesse.

Nous tenons à remercier Rogers Communications et Google d'avoir pris le temps de nous aider aujourd'hui dans le cadre de l'importante étude que nous effectuons. Vos contributions ont été très instructives, comme d'habitude. Nous vous remercions, vous et vos organisations, de nous avoir aidés aujourd'hui.

Je vais lever la séance. Nous ne reprendrons pas après le vote, mesdames et messieurs. Je vous verrai donc mardi.

La séance est levée.