CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de l'industrie, des sciences et de la technologie

INDU • NUMÉRO 082 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 7 novembre 2017

Président

M. Dan Ruimy

Comité permanent de l'industrie, des sciences et de la technologie

Le mardi 7 novembre 2017

● (1105)

[*Traduction*]

Le président (M. Dan Ruimy (Pitt Meadows—Maple Ridge, Lib.)): Je déclare la séance ouverte.

Bonjour à tous et bienvenue à Ottawa en cette magnifique et froide journée ensoleillée pour assister à la 82e séance du Comité permanent de l'industrie, des sciences et de la technologie, qui poursuit son étude de la Loi canadienne anti-pourriel.

Avant de commencer, je voudrais faire une brève salutation. Je sais que certains d'entre nous participent à la journée d'accompagnement des Grands Frères et Grandes Soeurs sur la Colline. Pouvons-nous demander aux membres des Clubs des garçons et filles de se lever?

Regardez toutes ces personnes qui viennent pour la première fois sur la Colline pour observer leurs députés. Bienvenue à la séance du Comité. Nous espérons que nous vous divertirons avec nos envolées théâtrales.

Aujourd'hui, nous recevons Kim Arsenault, qui est directrice principale aux Services à la clientèle chez Inbox Marketer.

Fait très intriguant, nous entendrons également Louis Lau, agent de la cybercriminalité de la Direction de la cybercriminalité d'Interpol, qui témoigne depuis Singapour. Je vous lève mon chapeau, car il est minuit là-bas. Vous êtes donc dans une position plus difficile que la nôtre.

Nous accueillons enfin Chris Lewis, expert scientifique en chef chez Spamhaus Technology.

Nous entendrons d'abord Louis Lau, d'Interpol.

Vous disposez de huit minutes pour faire un exposé. La parole est à vous.

M. Louis Lau (agent de la cybercriminalité, Direction de la cybercriminalité, INTERPOL): Merci, monsieur le président et distingués membres du Comité. Je vous remercie de m'avoir invité à participer à votre examen législatif de la Loi canadienne anti-pourriel.

Je m'appelle Louis Lau, agent de police de Hong Kong en affectation à Interpol, où j'ai été invité à occuper les fonctions d'agent de la cybercriminalité au sein de la Direction de la cybercriminalité. Mon poste de travail se trouve au...

Le président: Pardonnez-moi, monsieur Lau. Je vous demanderais d'attendre un instant. Nous commençons à éprouver des problèmes de volume ici.

Faites un essai.

M. Louis Lau: Essayons de nouveau.

Le président: Merci. C'est excellent.

M. Louis Lau: Mon poste de travail se trouve au centre mondial d'innovation d'Interpol à Singapour. En fait, je me trouve à Singapour en ce moment même.

La Direction de la cybercriminalité a pour rôle de fournir du soutien opérationnel aux pays membres dans le cadre d'enquêtes sur la cybercriminalité. Ses tâches principales consistent à aider ces derniers à coordonner et la faciliter les enquêtes relatives aux crimes transnationaux en mettant l'accent sur la cybercriminalité pure, laquelle prend la forme de réseaux de zombies, de maliciels et de facilitateurs de haute technologie, comme les services d'hébergement impénétrables, les services de transfert professionnels ou les attaques par saturation.

Je crois comprendre que nous sommes ici pour traiter de la Loi anti-pourriel. Sachez que la Direction de la cybercriminalité d'Interpol ne porte pas beaucoup attention aux activités de lutte contre les pourriels, s'intéressant davantage aux enquêtes criminelles. Je peux toutefois vous fournir des détails sur le contexte de la cybercriminalité, puisque cette dernière repose beaucoup sur les pourriels.

Parmi les pratiques utilisant les pourriels, la fraude par compromission de courriels d'affaires constitue un des exemples les plus typiques. L'envoi de pourriels frauduleux est une forme de diffusion de pourriels commerciaux normaux. Nous ne parlons pas ici de pourriels commerciaux normaux, lesquels ne contiennent que des messages commerciaux, sans pièce jointe ou maliciel. La plupart des fraudes par compromission de courriels d'affaires, parfois appelée « fraude du président-directeur général », commencent par des pourriels.

Avant d'étudier la question plus en profondeur, il faut comprendre la manière dont ces crimes sont perpétrés. La plupart du temps, le PDG ou un autre haut dirigeant reçoit des pourriels contenant des pièces jointes malveillantes. S'ils ouvrent ces pièces jointes, cela compromet leur ordinateur. Le coupable, après avoir accédé au compte de courrier électronique du PDG, lit les courriels et peut ainsi étudier les activités de l'entreprise, la manière dont elle dépense et même le style de rédaction du PDG. Il choisira ensuite le moment le plus opportun, pendant les vacances du PDG, par exemple, pour envoyer des courriels frauduleux en son nom afin de demander des versements dans des comptes bancaires précis.

Cette façon de procéder a été confirmée grâce aux affaires de fraude par compromission de courriels d'affaires mises au jour par des pays membres qui ont demandé l'aide d'Interpol. Elle a également été confirmée lors d'une enquête proactive à laquelle Interpol a pris part. En 2016, avec l'aide d'experts d'entreprises externes, nous nous sommes adonnés à un exercice de rétroingénierie sur des échantillons de maliciels envoyés avec des pourriels courants. Nous avons constaté que la pièce jointe, une fois ouverte, installait une fonction permettant de connaître les justificatifs d'ouverture de session des victimes. Une analyse détaillée du comportement du maliciel nous a permis de déceler des indices qui ont révélé l'identité du suspect qui contrôlait ces maliciels. Nous avons fini par être capables d'identifier complètement ce suspect grâce à une enquête exploitant des sources ouvertes. Ces renseignements ont été communiqués à l'organisme d'exécution de la loi du pays où se trouvait le suspect, et en juin 2016, ce dernier a enfin été arrêté.

Après son arrestation, notre équipe a été invitée à participer à l'examen de l'ordinateur portatif qui avait été saisi chez le suspect. Nous avons ainsi confirmé une fois de plus que l'envoi de pourriels servait à hameçonner des victimes afin de compromettre leurs comptes de courrier électronique. Les preuves montraient que le suspect téléchargeait des millions d'adresses de courrier électronique et utilisait un logiciel précis pour envoyer de grandes quantités de pourriels de manière automatisée. Le contenu du courriel était très simple:

> Bonjour,
>
> Vous trouverez la copie finale de la facture en pièce jointe.
>
> Bien à vous.
>
> xxx

Un fichier nommé « facture » se trouvait en pièce jointe. Nous avons effectué une analyse poussée de ce fichier et constaté qu'il s'agissait bel et bien d'un maliciel capable de voler les justificatifs d'ouverture de session des victimes.

● (1110)

Après avoir volé ces informations, le suspect accédait aux ordinateurs des victimes et à leurs comptes de courrier électronique pour consulter leurs courriels. Les preuves donnent à penser qu'il s'est connecté plus de 200 fois à certains comptes en l'espace de quelques mois, compromettant ainsi des centaines de courriels.

Les preuves semblent également indiquer que le suspect modifiait des factures qu'il avait fort probablement obtenues dans des comptes compromis. Sur son ordinateur, il modifiait les informations relatives au compte de banque du document original afin de tromper les agents financiers pour qu'ils déposent de l'agent dans des comptes frauduleux.

Interpol n'a pas recueilli de chiffres sur la criminalité auprès des pays membres, et je crains de ne pouvoir vous fournir de statistiques quantitatives. Cependant, des pays membres ont fait savoir à Interpol que le problème de compromission de comptes d'affaires constituait le genre de crime qui suscitait le plus de préoccupations dernièrement.

Interpol a récemment organisé deux conférences internationales, une en Espagne en juin et une en France en octobre, lesquelles portaient sur la compromission de comptes d'affaires. Y ont participé 60 participants issus de 30 pays qui ont exprimé des inquiétudes à propos de ce problème.

C'est tout.

Le président: Merci beaucoup.

Nous allons maintenant entendre Mme Arsenault.

Vous disposez de huit minutes.

Mme Kim Arsenault (directrice principale, Services à la clientèle, Inbox Marketer): Merci, monsieur le président et distingués membres du Comité, de me donner l'occasion de témoigner aujourd'hui. Je m'appelle Kim Arsenault et je suis directrice principale des services à la clientèle chez Inbox Marketer.

Cette dernière est une entreprise axée sur les données offrant des services de marketing par courrier électronique et des solutions technologiques. Elle est d'ailleurs un chef de file du domaine du marketing par courrier électronique depuis 15 ans, servant des clients en Amérique du Nord et en Europe. Depuis huit ans, nous nous intéressons de près à la Loi canadienne anti-pourriel, collaborant étroitement avec l'Association canadienne du marketing au sein du groupe de travail fédéral mis sur pied en 2005, ainsi qu'avec Industrie Canada pour informer les entreprises quant à la conformité à la Loi canadienne anti-pourriel.

La bonne nouvelle, c'est que depuis l'adoption de cette loi, il y a trois ans, les données sur le parcours de navigation examinées au sein d'un éventail de clients montrent que comparativement aux données recueillies un an avant cette adoption, les données sur les courriels se sont, de façon générale, améliorées au chapitre des taux de participation, de retour et de désinscription, et de la livraison dans la boîte de réception. Cette amélioration est en grande partie attribuable au fait que les expéditeurs ont adopté de meilleures pratiques de gestion de liste qui leur ont permis de tenir des listes d'envoi de meilleure qualité et d'envoyer moins de courriels non sollicités ou expédiés à des adresses électroniques invalides.

À notre avis, depuis la mise en oeuvre de la Loi canadienne anti-pourriel en 2014, les professionnels canadiens du marketing par courrier électronique se sont disciplinés et ceux qui s'adonnent à ces activités de façon légitime au pays prennent la Loi avec le plus grand sérieux. Les entreprises de marketing responsables se sont adaptées en devenant plus diligentes. Elles ont constitué des groupes de travail et nommé des personnes pour s'occuper activement de la conformité à la Loi en effectuant des vérifications ponctuelles régulières, des intégrations de la technologie et de la formation professionnelle.

Cela étant dit, nous avons certaines préoccupations dont nous voudrions vous faire part aujourd'hui.

La première est le fardeau économique qu'impose la Loi sur bien des entreprises canadiennes sur le plan de la conformité. Il leur en coûte entre quelques dizaines de milliers de dollars et des millions de dollars, selon leur taille, pour pouvoir mettre à jour leurs processus et leurs technologies afin qu'ils soient conformes à la Loi. Et ce ne sont là que les frais relatifs aux processus et à la technologie. À cela s'ajoute le coût des ressources nécessaires pour former et éduquer continuellement le personnel au sujet de la conformité d'entreprise.

À ce chapitre, nous nous préoccupons également du fait que même quand les entreprises ont instauré des programmes de conformité et adapté leurs processus et leurs technologies, elles ne savent toujours pas très bien ce qui est exigé d'elles sur le plan de la tenue de dossiers, ce qui peut être très problématique pour des organisations qui tentent de se conformer à la Loi. Le CRTC a publié des lignes directrices à portée générale au sujet de la conformité, mais a également indiqué à plusieurs reprises que les entreprises sont libres d'interpréter comment elles doivent appliquer la tenue de dossiers efficace dans leur situation.

Le fait est que les entreprises doivent investir des sommes et des ressources considérables pour adapter leurs systèmes et leurs processus, en se fondant sur leur interprétation et leurs suppositions éclairées, tout cela pour risquer de découvrir qu'ils ne sont pas acceptables advenant une contestation en vertu de la Loi. Cela les aiderait beaucoup si le gouvernement pouvait fournir une orientation claire et des exemples précis des pratiques de tenue de dossiers qui seraient acceptables afin de permettre aux organisations d'être certaines que le temps et les ressources qu'elles affectent à cet égard leur permettent de se conformer pleinement à la Loi.

De plus, nous constatons encore que bien des organisations ne considèrent pas la Loi canadienne anti-pourriel comme une mesure législative simple et intuitive. Cette loi sème la confusion chez un grand nombre d'entreprises et, pour celles qui ne la connaissent pas en détail, il peut s'avérer difficile de non seulement tenter de la comprendre, mais aussi de constamment informer leurs employés de ce qui constitue, selon elles, la procédure correcte.

Trois ans après l'adoption de la Loi, nous conseillons encore des entreprises qui cherchent à comprendre la distinction entre le consentement exprès et le consentement tacite. En raison de l'ambiguïté et du manque de clarté et d'orientation de la part du gouvernement, certaines organisations ne se servent plus du courrier électronique pour communiquer avec leurs clients actuels et potentiels. Par exemple, des établissements financiers et des compagnies d'assurances nous ont indiqué qu'avant l'arrivée de la Loi anti-pourriel, elles avaient des équipes de vendeurs et de conseillers qui utilisaient le courrier électronique pour communiquer des offres et du contenu intéressant à leurs clients existants. Maintenant que la Loi est entièrement en vigueur, la crainte et l'anxiété qu'éprouvent certaines organisations en raison du manque de clarté et des inexactitudes qui circulent les ont inévitablement poussées à abandonner la communication par courrier électronique.

Or, ce mode de communication a, pendant des années, offert un rendement de l'investissement de 40:1. De nombreuses études continuent de montrer que les consommateurs préfèrent que les marques utilisent la voie électronique pour communiquer avec eux. Ainsi, quand de grandes entreprises délaissent le courrier électronique par crainte de ne pas être conformes, cela peut avoir des conséquences substantielles sur ces dernières.

Nous nous préoccupons également du fait que les autorités de réglementation ont mis des années à rédiger la Loi anti-pourriel. La rédaction de la loi a commencé en 2004, et la Loi est entrée en vigueur en 2014, comme nous le savons tous. Or, la technologie évolue à un rythme très différent. Le marketing, par exemple, a plus évolué au cours des cinq dernières années qu'au cours des 50 dernières années, et nul ne peut prédire à quelle vitesse la technologie et les médias numériques évolueront au cours des cinq prochaines années. Nous ne pouvons pas laisser les entreprises canadiennes d'aujourd'hui utiliser davantage des moyens de communication comme le téléphone, lesquels sont plus chers et moins efficaces que les courriels et les médias sociaux, parce qu'elles ont trop peur de ce qu'il se passera si elles utilisent le courrier électronique. Or, c'est exactement ce que certaines d'entre elles font aujourd'hui.

● (1115)

La Loi canadienne anti-pourriel a pour objectif de favoriser l'efficacité et l'adaptabilité de l'économie canadienne. Le fait que des organisations délaissent le courrier électronique ou décident de ne pas faire de marketing au Canada est contraire à cet objectif.

Nombreux sont ceux qui se demandent ce que font les autorités de réglementation pour suivre le rythme de la technologie et des médias sociaux. Les lignes directrices relatives à l'application de la Loi anti-pourriel dans les médias sociaux sont extrêmement vagues, alors que les médias sociaux évoluent à vitesse grand V. Par exemple, plus de la moitié de la population mondiale est maintenant en ligne et 2,7 milliards de personnes utilisent activement les médias sociaux. Le fait est que le marketing numérique et social constitue aujourd'hui un élément essentiel de la boîte à outils des marques.

Je vous présenterais aussi quelques recommandations. Les autorités de réglementation doivent accorder du temps et des ressources afin de tenir leur site Web à jour et de fournir plus d'éclaircissements sur les points suivants.

Tout d'abord, qu'est-ce qui constitue un message électronique commercial, ou MEC? Ce n'est pas clair pour bien des entreprises. Cela pourrait être un bulletin, par exemple, dont le contenu porte sur la crédibilité et les connaissances de l'organisation. Si le logo situé dans le coin supérieur gauche contient un lien vers le site Web de l'entreprise qui fait la promotion des activités commerciales de cette dernière, cela confère-t-il un caractère commercial au bulletin? Ce n'est pas clair. Qui plus est, le fait que les courriels purement transactionnels soient considérés comme des MEC en vertu du paragraphe 6(6) est extrêmement mêlant, très difficile à mettre en application et superflu. Nous recommandons donc d'éliminer complètement cette disposition de la Loi.

En outre, les autorités de réglementation devraient indiquer plus clairement ce qui peut et ne peut pas être fait sur les médias sociaux pour que les entreprises puissent tirer adéquatement parti de ces moyens de communication.

Les autorités de réglementation devraient de plus expliquer complètement ce qu'il faut faire pour tenir adéquatement les dossiers. Les organisations devraient savoir que leur solution de 4 millions de dollars sera acceptée par le CRTC.

Enfin, les autorités de réglementation devraient éliminer la confusion et l'exigence relatives aux périodes de six mois ou de deux ans au chapitre du consentement tacite. Elles devraient définir clairement ce que sont le consentement exprès et le consentement tacite, et éliminer les périodes de six mois et de deux ans. Il est très difficile pour bien des entreprises, peu importe leur taille, de maintenir ce degré de détail qui peut constamment changer et évoluer. Ce ne sont pas toutes les solutions technologiques qui peuvent consigner adéquatement des renseignements à ce sujet.

Les grandes entreprises comptant plusieurs secteurs d'activités, et donc plusieurs systèmes de gestion des relations avec la clientèle, ont toutes besoin de communiquer avec leurs clients, dont un grand nombre sont présents dans plus d'un secteur. Dans un grand nombre d'entreprises d'aujourd'hui, il n'est pas réaliste de s'attendre à ce que tous les messages soient gérés et contrôlés à partir d'un point central.

Pour de nombreuses entreprises, il est très difficile de savoir dans quelles situations appliquer les périodes de six mois et de deux ans; certaines d'entre elles n'autorisent donc la communication que si le client a donné son consentement exprès. Elles perdent ainsi des occasions de croissance, car elles ne comprennent pas parfaitement comment elles peuvent utiliser le consentement tacite. La crainte, le risque et l'incertitude sont bien trop importants à leur goût.

Monsieur le président, distingués membres du Comité, je vous remercie de nouveau de m'avoir donné l'occasion de vous parler aujourd'hui de certaines des conséquences de la Loi canadienne anti-pourriel sur les citoyens et les entreprises du Canada.

● (1120)

Le président: Merci beaucoup.

Nous allons maintenant entendre notre dernier témoin.

Monsieur Lewis, de Spamhaus Technology, vous avez la parole pour huit minutes.

M. Chris Lewis (expert scientifique en chef, Spamhaus Technology Ltd.): Merci et bonjour, monsieur le président.

Je m'appelle Chris Lewis et je suis expert scientifique en chef chez Spamhaus Technology, laquelle fait partie de Spamhaus, une des sources les plus importantes et les plus respectées de renseignements sur les menaces sur Internet dans le monde. Même si la plupart d'entre vous n'ont pas entendu parler de nous, plus de la moitié d'Internet utilise nos données d'une manière ou d'une autre, qu'elles portent la marque de Spamhaus ou non.

Contrairement à la plupart des témoins qui traitent des pourriels au Canada, je travaille profondément dans les entrailles de la technologie elle-même. Pour moi, la lutte aux pourriels est un effort de tous les instants, et avec la technologie que nous employons, je vois de 750 millions à un milliard de pourriels par jour dans les systèmes que je gère afin d'analyser la situation et de trouver une solution pour mettre fin à ce problème.

De 1991 à 2012, d'abord, j'ai travaillé à Ottawa à titre d'architecte principal en matière de sécurité pour Bell Northern Research, qui est, bien sûr, ensuite devenue Nortel. Je m'occupe des pourriels d'une manière ou d'une autre depuis environ 1993. À compter de 1997-1998, il est devenu évident que le courrier électronique constituait le champ de bataille qu'il fallait sauver pour qu'Internet prospère et que le courrier électronique continue.

Depuis lors, j'ai principalement concentré mon attention sur les pourriels, les maliciels et les réseaux de zombies au lieu de m'occuper de l'envoi délibéré de courriels sans permission, m'intéressant particulièrement à l'aspect technique de la question. En 2003, j'ai mis au point une nouvelle technologie qui a considérablement amélioré l'efficacité des filtres de Nortel, laquelle avait besoin de grandes quantités de données des quatre coins d'Internet. J'analysais les données venant de partenaires et de fournisseurs, puis je les publiais gratuitement sur Internet. C'est ainsi que les choses se sont passées pendant des années. Puis, à la fin de 2012, Nortel a réduit son effectif au point où elle n'avait plus besoin de moi pour gérer un serveur pour 50 personnes. J'ai donc déménagé mes pénates chez Spamhaus le lendemain.

Je suis un des membres fondateurs de la Coalition contre le courrier commercial électronique non sollicité. J'ai été invité à m'adresser au groupe de travail sur les pourriels de la Federal Trade Commission; prodiguer des conseils quant à la CAN-SPAM Act des États-Unis; suis un membre fondateur du projet SLAM-SPAM de l'Alliance nationale d'intervention judiciaire et de formation contre la cybercriminalité et du FBI; ai reçu un prix du FBI pour les efforts que j'ai déployés pour sécuriser les réseaux du gouvernement américain; ai été invité à agir à titre de conseiller technique principal auprès du Messaging, Malware and Mobile Anti-Abuse Working Group, ou M3AAWG; ai fait partie de nombreux groupes de travail techniques s'attaquant aux pourriels et aux maliciels; ai formé et aidé un grand nombre de groupes de réglementation et d'application de la loi du monde, y compris le CRTC et des organisations des Pays-Bas, de l'Australie, des États-Unis et de nombreux autres pays; et suis membre du Plan d'action de Londres, aussi appelé UCENet. Ne me demandez pas ce que cela signifie, car je l'ai oublié.

À l'heure actuelle, Spamhaus fournit gratuitement au Centre canadien de réponse aux incidents cybernétique de la Sécurité publique un très important jeu de données de pourriels ciblant des adresses de courrier électronique de citoyens canadiens, que le Centre utilise à certaines fins, notamment pour entamer des poursuites en collaboration avec la GRC et le CRTC. Le Centre s'en sert également pour avertir la population canadienne au sujet des infections de ses systèmes et produit périodiquement des rapports avisant des fournisseurs, et parfois des particuliers, que leurs systèmes ont été infectés et leur indiquant comment régler le problème.

Je traite principalement des pourriels, même s'il existe d'autres formes de problèmes aussi, voire plus importantes et posant davantage de risque. La fraude par maliciel et hameçonnage, à laquelle on a déjà fait allusion, constitue un problème de taille, et tous ces problèmes empirent.

Ce qui est particulièrement intéressant ici, c'est que lorsque j'étais conseiller auprès du M3AAWG, j'ai passé une bonne partie de mon temps avec des expéditeurs de courriels, comme Inbox Marketing et d'autres entreprises, pour les aider à adopter des pratiques exemplaires afin de gérer leurs listes d'abonnés, de déterminer quand ils sont autorisés à envoyer des courriels et de comprendre d'autres questions. J'ai grandement contribué à l'élaboration d'une partie des pratiques exemplaires communes des expéditeurs du M3AAWG, lesquelles sont encore mises à jour et publiées. Ces pratiques sont considérées comme une des lignes directrices les plus importantes de l'industrie, et la plupart des grands expéditeurs de courriels s'y conforment déjà. En fait, une organisation d'envoi de courriels ne peut faire partie du M3AAWG à moins qu'elle ne s'y conforme.

● (1125)

On peut donc se demander pourquoi on se préoccupe tant de la conformité si la plus grande partie de l'industrie se conforme aux pratiques exemplaires communes du M3AAWG, dont une bonne partie s'inspire directement de la Loi canadienne anti-pourriel, contenant les mêmes principes et les mêmes éléments.

Je vais donc vous faire part de faits et de détails précis recueillis ces dernières années.

Nous utilisons des capteurs qui surveillent, dans un sens ou dans un autre, des milliards de courriels par jour aux termes d'ententes avec les fournisseurs. Nous gérons aussi notre propre infrastructure pour recevoir des courriels envoyés à des adresses qui n'existent plus sur Internet, comme certaines adresses de courrier électronique qui étaient utilisées chez Nortel il y bien des années. Le Centre canadien de réponse aux incidents cybernétique de la Sécurité publique est maintenant propriétaire de ces domaines et nous a demandé de nous en servir comme si les utilisateurs existaient toujours. Nous pouvons voir quels pourriels nous recevons, déterminer d'où ils viennent, établir des corrélations et communiquer l'information à nos clients, bien souvent gratuitement, afin que les fournisseurs et d'autres entreprises puissent protéger leurs utilisateurs des pourriels.

Au cours des sept dernières années, le nombre de pourriels a atteint un sommet en 2011 avec 10 milliards de pourriels par mois; nos propres serveurs ont enregistré des sommets de 750 millions de pourriels par jour. Ce n'était pas dans la masse de données fournies, mais dans les courriels que nous gérons nous-mêmes. Ces pourriels venaient souvent du réseau de zombies Rustock, tristement célèbre pour son volume élevé de pourriels proposant des pilules bidon et des montres contrefaites. Ces dernières constituent de simples fraudes, mais les faux médicaments sont dangereux; en effet, un grand nombre d'entre eux ont été analysés par des gens que nous connaissons dans l'industrie, lesquels ont découvert que ces pilules contiennent littéralement des balayures et d'autres matières. Les malfaiteurs compressaient tout ce qui leur tombait sous la main, teignaient le résultat en bleu et vendaient le produit.

Quelques années plus tard, le volume était en moyenne de trois milliards de pourriels par mois, puisque le réseau Rustock avait été démantelé grâce aux efforts d'un certain nombre d'organisations sur Internet et du FBI. Ces dernières années, le volume est presque revenu à 10 milliards de pourriels par mois. Au lieu de médicaments et de montres contrefaits, ce sont le réseau de zombies Necurs et les pourriels de services de rencontre russes qui posent problème. Fait encore plus troublant, le réseau de zombies Necurs envoie aussi le rançongiciel dont il est question dans les nouvelles et qui crypte tous les jeux de données des hôpitaux, qui ne peuvent plus les utiliser à moins de verser des montants substantiels.

Pourtant, parmi ces énormes quantités de messages dangereux se trouve un volume très élevé de pourriels vantant les mérites de compagnies ou de produits légitimes, douteux et carrément frauduleux offerts par des gens faisant totalement fi du concept de protection des renseignements personnels et embauchant des pirates pour voler des adresses de courrier électronique, faire de l'hameçonnage et commettre d'autres délits.

Des chefs de file de l'industrie comme SenderBase Talos, une filiale de Cisco, qui sont depuis longtemps des sources fiables de statistiques réelles et « branchées », tendent de façon générale à convenir que nos chiffres sont exacts. Nous ne nous attendons pas à ce que tous les chiffres concordent, car les échantillons de pourriels peuvent être étonnamment différents, mais nos tendances, nos sommets et tous les autres renseignements coïncident exactement.

J'ai eu l'occasion de surveiller le volume de courriels et de pourriels reçus par certains des anciens domaines de Nortel qui datent de presque 20 ans. J'ai conçu et géré les serveurs de courrier électronique quand ils étaient en service et au cours de leurs 18 années d'inutilisation. Comme je l'ai souligné plus tôt, ces domaines appartiennent maintenant au Centre canadien de réponse aux incidents cybernétiques à titre de ressource nationale sur le plan des menaces, et le Centre nous a demandé de les gérer en son nom.

En 1997, Nortel a déclassé ces domaines et a transféré tous les utilisateurs vers le domaine de courrier électronique principal qu'elle utilisait à l'époque. Cette année-là, les domaines ont reçu trois millions de courriels, dont 40 % étaient des pourriels. En 2001, ce nombre était de quatre millions de courriels, qui étaient tous des pourriels. En 2003, ce sont sept millions de pourriels qui ont été reçus, un chiffre qui a atteint 150 millions de messages en avril 2016. Aujourd'hui, ce sont 350 millions de pourriels qui sont reçus chaque mois, soit 350 fois plus qu'il y a 20 ans.

Vous vous demandez « Est-ce que mon volume de pourriels a tant augmenté? » Non, il n'a pas tant augmenté, mais ce n'est que grâce aux efforts de votre fournisseur de service Internet et d'organisations comme la nôtre que ce nombre a décru.

● (1130)

Les volumes continuent de croître. Les polluposteurs mettent nos systèmes au défi, et il est très difficile de poursuivre la lutte.

On me fait signe; je vais donc abréger mon propos.

Un des points qui nous intéressent dans la Loi anti-pourriel est le droit privé d'action. Nous voulons pouvoir intervenir quand des personnes reçoivent des volumes très élevés de pourriels. Un de mes associés avait un domaine de courrier électronique avec sa conjointe; or, un jour, il s'est mis à recevoir un million de pourriels par jour. Nous ignorons pourquoi. J'ai quelques doutes à cet égard, mais nous ne disposons d'aucun renseignement solide expliquant pourquoi cela s'est produit. Le volume était si élevé qu'il ne pouvait même plus utiliser son propre serveur en raison du coût. Le droit privé à l'action lui donne l'occasion de réagir en pareille situation.

Je dirai enfin que le pollupostage est un problème humain et non technique, et qu'il faut s'y attaquer sous les deux angles.

Le président: Merci beaucoup.

Je n'ai qu'une version anglaise de votre document. Nous le ferons traduire et veillerons à ce que chaque membre en obtienne une copie, car il contient un peu plus d'information. Nous nous assurons qu'il soit distribué une fois qu'il aura été traduit.

Cela étant dit, je vous remercie tous les trois de vos exposés.

Nous passerons immédiatement aux questions, en commençant par M. Longfield.

Vous disposez de sept minutes.

M. Lloyd Longfield (Guelph, Lib.): Merci, monsieur le président.

Je vous remercie tous d'être venus de loin. C'est formidable qu'une entreprise de Guelph comme Inbox Marketer soit ici.

Je veux traiter de ce que certains témoins nous ont dit à propos de la distinction entre les activités techniques, frauduleuses et normales.

Madame Arsenault, je sais que vous êtes cofondatrice d'Inbox et que vous avez assisté à l'essor du marketing par courrier électronique ces dernières années. Au cours de votre exposé, vous avez déjà indiqué que la Loi anti-pourriel avait favorisé l'efficacité de cette forme de marketing.

Selon ce que j'entends, vous considérez que cette loi est nécessaire, tout en considérant qu'il existe une certaine confusion quant à son interprétation. Pourriez-vous nous en dire plus sur l'amélioration l'efficacité et nous expliquer comment la Loi anti-pourriel a contribué à cette amélioration?

Mme Kim Arsenault: Je pense qu'à ce chapitre, la Loi a permis aux entreprises de marketing d'examiner leurs listes d'envoi et d'en retirer les adresses inconnues. Comme nous avons fourni des services de conseil à un grand nombre d'entreprises, nous avons dû vérifier leurs bases de données et leur demander où elles avaient obtenu l'autorisation pour tous les dossiers. Pour chaque dossier pour lequel elles n'avaient pas d'autorisation ou ignoraient la source de l'adhésion, nous leur recommandions d'adopter une approche prudente et de l'éliminer.

Nous avons constaté que lorsque la Loi anti-pourriel est entrée en vigueur, les entreprises de marketing et les marques ont été obligées d'éliminer les adresses qui n'étaient peut-être pas de bonne qualité. Dans le domaine du marketing par courrier électronique, certaines marques préfèrent la quantité à la qualité, et la Loi les a obligées à réduire la taille de leurs listes. Certaines listes sont ainsi passées de 1 million à 200 000 dossiers, mais ces 200 000 adresses sont celles de personnes intéressées et pertinentes qui veulent faire partie de la base de données. Les programmes de marketing par courrier électronique sont donc bien plus efficients, ce qui améliorer l'efficacité, puisque toutes les pratiques offrent désormais un meilleur rendement de l'investissement.

C'est ainsi que la Loi a favorisé l'efficacité. Nous convenons que des règlements doivent régir la manière dont nous utilisons le courrier électronique; il faut imposer des restrictions à cet égard. Cependant, la Loi anti-pourriel impose des frais bien trop élevés aux entreprises et est trop complexe. Une telle loi ne devrait pas être aussi complexe, et trois ans après son entrée en vigueur, des entreprises ne devraient pas nous demander quelle est la différence entre le consentement tacite et le consentement exprès.

● (1135)

M. Lloyd Longfield: Je vous poserai une question, à vous et à M. Lewis, à propos de la consultation qui a précédé l'élaboration de la Loi anti-pourriel et vous demanderai si cette consultation s'est poursuivie à mesure que la technologie a évolué.

Est-ce que le groupe qui s'était formé avant l'élaboration de la Loi se réunit encore à l'occasion?

M. Chris Lewis: Des discussions informelles ont eu lieu. Évidemment, étant donné que je m'entretiens directement avec le CRTC, je peux vous dire que les consultations évoluent. Les situations avec lesquelles on doit composer évoluent. On apprend énormément. En fait, la courbe d'apprentissage est très abrupte, mais on fait des progrès.

L'une des choses qui m'a frappé, lorsque j'ai vu pour la première fois l'ébauche de la LCAP en 2012, c'était à quel point elle ratissait large. Elle a été rédigée de façon à pouvoir s'appliquer à la technologie, au besoin.

Je ne crois pas que la Loi proprement dite soit trop étroite ou contraignante. C'est davantage une question d'éducation. Il s'agit ici de déterminer quand cela devient un problème et comment on doit répartir les ressources.

M. Lloyd Longfield: Merci.

Avez-vous quelque chose à ajouter?

Mme Kim Arsenault: Non. Depuis que la LCAP est entrée en vigueur, le groupe de travail n'a pas été très actif. Nous avons laissé la Loi faire son travail puis nous attendons cet examen triennal.

M. Lloyd Longfield: D'accord. Très bien.

Nous nous penchons sur les détails du droit privé d'action. Monsieur Lewis, vous avez parlé des citoyens. Nous avons de la difficulté à les amener à témoigner sur la façon dont le droit privé d'action pourrait s'appliquer. Pouvez-vous faire la distinction entre les entreprises légitimes et semi-légitimes et les entreprises frauduleuses, et comment vous y prenez-vous?

M. Chris Lewis: Je crois que des mesures de protection sont intégrées à la Loi lorsqu'il s'agit du droit privé d'action. Par exemple, il y a le CRTC, le commissaire à la protection de la vie privée et la Direction générale de la concurrence qui ont la capacité prioritaire d'intervenir. À cet égard, les lois canadiennes sont très différentes des lois américaines. Certains des abus que nous avons vus aux États-Unis — et effectivement, il y a eu des abus — ne seraient possiblement pas un problème ici. On donne aux gens la possibilité de régler des dossiers dont le CRTC, le commissaire à la protection de la vie privée et la Direction générale de la concurrence ne pourraient pas s'occuper, compte tenu des exigences prévues par la Loi concernant le nombre de plaintes ou de personnes ayant été la cible d'attaques, et ainsi de suite. Grosso modo, dans le cas dont je parlais plus tôt, il pourrait faire quelque chose en fonction de la Loi, mais cela lui coûterait 10 000 $ pour avoir un avocat.

M. Lloyd Longfield: D'accord.

Du point de vue d'Interpol, lorsqu'il est question du droit privé d'action, nous nous comparons aux États-Unis, étant donné notre proximité, mais sur Internet, l'adhésion importe peu. Y a-t-il une pratique exemplaire ailleurs dans le monde dont on pourrait s'inspirer? Savez-vous si le droit privé d'action est appliqué de façon générale par certains de vos pays membres?

M. Louis Lau: Nous n'avons pas réalisé beaucoup d'études là-dessus. Je ne suis pas sûr si je peux vous parler de mes expériences, mais comme je l'ai mentionné, nous nous concentrons surtout sur les enquêtes criminelles. Comme je l'ai dit, les pourriels sont à l'origine d'un grand nombre de cybercrimes, particulièrement la compromission de courriels d'affaires ou les rançongiciels dont j'ai parlé plus tôt.

M. Lloyd Longfield: Étant donné qu'il me reste seulement 20 secondes, je vais tout de suite remercier nos témoins d'avoir été des nôtres. J'ai encore beaucoup d'autres questions, mais je suis certain que mes collègues s'exprimeront dans le même sens que moi.

Le président: Excellent. Merci.

Je cède maintenant la parole à M. Eglinski.

Vous avez sept minutes.

M. Jim Eglinski (Yellowhead, PCC): Merci.

Monsieur Lau, avez-vous examiné la réglementation anti-pourriel au Canada? Le cas échéant, lorsqu'on parle de contrôle réglementaire, où est-ce qu'on se situe par rapport aux autres pays avec lesquels vous traitez à l'échelle internationale? Notre situation est-elle meilleure ou pire? Devons-nous améliorer des choses?

● (1140)

M. Louis Lau: La loi anti-pourriel n'est pas appliquée dans tous les pays, surtout les pays en développement. Je ne serais pas en mesure de me prononcer sur la Loi canadienne de manière professionnelle. J'ai réalisé beaucoup d'évaluations dans différents pays — par exemple, dans les pays en développement — et sachez que la loi anti-pourriel n'est pas très courante dans ces pays. J'estime que c'est une bonne chose de mettre en oeuvre une loi anti-pourriel, tout comme d'avoir un processus de consultation comme celui que nous avons en ce moment.

M. Jim Eglinski: D'accord. Merci.

Est-ce que vous et Interpol avez travaillé sur des cas au Canada ou avec l'un ou l'autre de nos organismes, disons le CRTC?

M. Louis Lau: Notre plus grande préoccupation demeure les cybercrimes, commis à partir de l'envoi de pourriels, et nous avons organisé plusieurs conférences internationales afin d'aborder cet enjeu.

Dans le cadre d'une conférence que nous avons tenue à Madrid, en juin dernier, le Canada était l'un des pays à avoir exprimé des inquiétudes au sujet de la compromission des courriels d'affaires. Nous avons discuté ensemble des façons de remédier à ce problème. Il s'agit de notre seule collaboration avec le Canada.

Nous savons que le Canada aimerait collaborer davantage avec Interpol et d'autres pays pour s'attaquer au problème de la compromission des courriels d'affaires. Nous travaillons en ce moment sur plusieurs opérations de suivi.

M. Jim Eglinski: Monsieur Lewis, vous nous avez parlé de votre parcours, qui est très impressionnant. Vous travaillez dans le secteur depuis longtemps.

Selon vous, depuis son entrée en vigueur en 2012, la Loi a-t-elle nui à l'industrie et aux entreprises, ou les a-t-elle plutôt aidées? Trouvez-vous qu'elle est compliquée? Certains témoins nous ont dit qu'elle était compliquée et entraînait des coûts importants. J'aimerais connaître votre avis là-dessus.

M. Chris Lewis: J'ai participé aux délibérations du Groupe de travail canadien sur le pourriel en 2005-2006. On m'a consulté au moment d'adopter cette loi, et j'ai observé ce qui s'est fait dans le secteur par la suite. Ce qui m'a surpris, c'est que certaines entreprises semblent en faire trop sur le plan de la conformité.

La raison pour laquelle certaines personnes en font plus qu'elles ne le devraient, selon moi, c'est parce qu'il s'agit d'une loi plutôt que de pratiques exemplaires. Je pense que les pratiques ressemblent à ce qui se fait déjà dans le secteur. L'Union européenne a une réglementation presque aussi ferme que la nôtre, tout comme l'Australie, et la réglementation en Europe est sur le point d'être beaucoup plus stricte. Il est important de tenir compte de ce qui se fait ailleurs. J'ai été étonné de voir à quel point des gens dépassaient les exigences.

Aujourd'hui, lorsque je donne mon adresse de courriel à une entité canadienne, je sais qu'elle ne sera pas vendue. La situation a changé. Il n'y avait pas de contrôle par le passé, alors les choses sont beaucoup mieux qu'avant.

M. Jim Eglinski: Madame Arsenault, il y a quelque temps, un témoin nous a donné une ventilation des coûts. Vous nous avez également parlé des coûts, de façon plutôt vague — entre quelques dizaines de milliers de dollars et des millions de dollars. Ce n'est pas ce que nous avons entendu auparavant. J'aimerais savoir ce qui soutient ces chiffres, parce qu'on nous a dit que certaines petites entreprises devaient payer 600 $ pour obtenir des conseils et des renseignements, puis entre 200 et 300 $ par année pour poursuivre les vérifications. Pourriez-vous nous donner quelques précisions là-dessus?

● (1145)

Mme Kim Arsenault: Absolument. Nous travaillons avec de nombreuses sociétés financières et d'assurances et certaines grandes marques mondiales. Une grande institution financière pourrait avoir plus de 40 bases de données différentes de gestion des relations avec la clientèle, et la Loi stipule qu'il faut relier chaque personne à chaque communication et faire un suivi de tout ce à quoi elle s'inscrit et se désinscrit. Si on a 40 bases de données au sein d'une entreprise mondiale, l'intégration ne coûtera pas 1 000 $.

Les entreprises que nous avons consultées nous ont dit qu'elles ont dû investir plus de 5 millions de dollars dans la technologie pour mettre à jour leurs systèmes afin de pouvoir suivre le niveau de permission exigé par la LCAP — consentement tacite par rapport à exprès, période de six mois par rapport à deux ans. Ensuite, bien sûr, les petites organisations ont des bases de données plus petites. Elles n'ont pas autant de bases de données de gestion des relations avec la clientèle, ce qui leur coûte beaucoup moins cher.

Il faut également tenir compte du coût pour former les employés et du temps qu'on doit y consacrer. De nombreuses entreprises ont dû demander des avis juridiques, car elles craignaient de mal interpréter la Loi, et cela coûte cher d'obtenir de tels conseils.

M. Jim Eglinski: Au fur et à mesure que l'entreprise croît, les coûts augmentent.

Je crois que je n'ai presque plus de temps.

Le président: En fait, vous avez dépassé le temps qui vous était alloué et vous êtes au banc des punitions.

Des voix: Ah, ah!

Le président: Je vais maintenant céder la parole à M. Masse qui, si je ne me trompe pas, va présenter un avis de motion.

Allez-y, je vous prie.

M. Brian Masse (Windsor-Ouest, NPD): Merci, monsieur le président.

Il s'agit d'un avis de motion très simple pour permettre au Comité de participer à un processus. Je vais vous lire ma motion, et je crois comprendre qu'elle fera partie de nos travaux futurs.

À la lumière des révélations récentes dans les médias sur l'évasion fiscale massive au Canada, et puisqu'un projet de loi du gouvernement actuellement au Sénat offre la possibilité de mettre en place immédiatement des mesures précises qui renforceraient la capacité du Canada à lutter contre l'évasion fiscale et le blanchiment d'argent, la motion au comité de l'industrie est la suivante:

> Que le Comité permanent de l'industrie, des sciences et de la technologie de la Chambre des communes élabore des modifications à renvoyer dans la correspondance au comité sénatorial qui sera chargé d'examiner le projet de loi C-25, Loi modifiant la Loi canadienne sur les sociétés par actions, la Loi canadienne sur les coopératives, la Loi canadienne sur les organisations à but non lucratif et la Loi sur la concurrence, dans le but de régler les problèmes de transparence fiscale au Canada, incluant la politique fiscale, la propriété effective, et la réglementation bancaire.

On en parlera plus tard. Le Comité pourrait envoyer une lettre au Sénat, par exemple.

Merci, monsieur le président. Je vais enchaîner tout de suite avec mes questions.

Le président: Allez-y.

M. Brian Masse: Merci, monsieur le président.

Monsieur Lau, l'un des aspects qui nous intéressent avec la LCAP — et j'aimerais aborder la question des appareils personnels, qu'il s'agisse des téléphones mobiles ou des ordinateurs. On paie pour le service et l'appareil en question, et on consacre son propre temps à sa gestion — envoyer des courriels et des renseignements non sollicités à quelqu'un est un privilège. Ce n'est pas un droit que quelqu'un devrait avoir, étant donné que cela implique des coûts pour quelqu'un d'autre.

Je m'inquiète du coût additionnel des pourriels lorsqu'il s'agit de la vie privée et de la sécurité des gens.

Au sein de votre entreprise, la menace est-elle plus grande? Est-ce que les pourriels risquent de porter davantage atteinte à la vie privée des gens ou à leurs dossiers financiers, entre autres? Je m'inquiète du risque accru auquel s'exposent les consommateurs, les Canadiens et d'autres gens ailleurs dans le monde lorsque les pourriels mènent à des activités illégales.

M. Louis Lau: J'aimerais faire une mise au point. Êtes-vous préoccupé par l'incidence ou la capacité des pourriels d'entraîner des coûts pour les gens?

M. Brian Masse: La menace est-elle plus difficile à gérer, étant donné tous les pourriels qui pourraient compromettre la vie privée et les renseignements personnels?

● (1150)

M. Louis Lau: Tout d'abord, je pense que nous devons faire la distinction entre deux types de pourriels. Il y a les pourriels qui se concentrent uniquement sur les renseignements des entreprises, puis les pourriels qui ont des pièces jointes. Nous nous intéressons surtout à ces derniers pourriels. Il y a toutes sortes de pièces jointes qui peuvent être envoyées dans un courriel.

Comme nous l'avons dit précédemment, certains courriels contiennent des logiciels malveillants, et dans mon cas, comme je l'ai dit tout à l'heure, nous avons la preuve que le suspect a commis une fraude par compromission de courriels d'affaires. Le maliciel qu'il a envoyé lui a permis d'obtenir les justificatifs de connexion des comptes de courrier électronique. Par exemple, si vous cliquiez sur ce courriel, qui avait une pièce jointe, vos justificatifs d'ouverture de session étaient envoyés au suspect. Ensuite, le suspect a pu consulter vos courriels, et ce, sans que vous ne le sachiez. Il a pu avoir accès à vos courriels pendant une longue période et a pu trouver le bon moment pour se faire passer pour vous et envoyer des courriels au département des finances, par exemple, afin d'obtenir de l'argent. Ce n'est qu'un exemple parmi d'autres.

Il y a également des attaques par rançongiciel. Les rançongiciels sont également envoyés dans des pourriels. Si vous les exécutez, certains fichiers de votre ordinateur seront chiffrés et, pour y accéder de nouveau, vous devrez soit payer pour obtenir des outils de déchiffrement, soit utiliser vos propres moyens pour les déchiffrer. Autrement, les fichiers seront chiffrés de façon permanente. Interpol essaie justement de fournir des outils de chiffrement aux victimes.

Ce sont les deux activités que l'on observe couramment.

M. Brian Masse: Nous avons un choix à faire. Nous étudions la Loi. Nous pouvons la renforcer, ne rien changer du tout ou l'assouplir, ce qui, selon moi, ouvrirait la porte à davantage de pourriels. J'essaie simplement de réduire la situation à sa plus simple expression.

À l'heure actuelle, si on assouplit la Loi... Depuis quelques années, croyez-vous que les gens et les consommateurs sont davantage menacés par les atteintes à la vie privée, avec l'arrivée des rançongiciels et ainsi de suite? Ce projet de loi a été adopté il y a trois ans, mais à partir du moment où on l'a publié dans la *Gazette*... cette Loi est appliquée depuis deux ou trois ans. Est-ce que la menace à la vie privée des Canadiens a diminué ces dernières années? Si nous décidons d'assouplir les règles, la menace ne risque-t-elle pas d'augmenter dans les années à venir?

Je sais qu'on ne peut pas prédire l'avenir, mais d'après vous, qu'est-ce qui va arriver?

M. Louis Lau: Je dirais qu'on peut aborder la question à deux différents niveaux. Tout d'abord, il y a des messages qui sont envoyés par des gens dans le secteur des affaires. Ces personnes n'ont pas d'intention malveillante lorsqu'elles envoient ces courriels. C'est peut-être dans un but commercial, mais quoi qu'il en soit, on abuse du système. C'est la première chose.

Ce dont il est question ici, ce sont les personnes qui ont évidemment de mauvaises intentions lorsqu'elles envoient ces courriels; il faut cibler ces personnes. Même avec la loi la plus exhaustive, ces personnes continueront d'envoyer des pourriels. La façon la plus efficace d'y remédier, ce serait au niveau des infrastructures. On peut miser sur les FSI ou les infrastructures pour bloquer ce type de pourriels. C'est la façon la plus efficace d'y parvenir.

Lorsqu'on essaie de comprendre la situation, il faut savoir que ces pourriels viennent de différentes sources. Ce sont deux types de pourriels totalement différents.

M. Brian Masse: Merci beaucoup.

Le président: Merci.

Je vais maintenant céder la parole à M. Baylis. Vous disposez de sept minutes.

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

J'aimerais examiner davantage la question des courriels malveillants avec vous, messieurs Lau et Lewis.

La LCAP visait principalement à lutter contre ces courriels malveillants. Monsieur Lau, en ce qui concerne vos échanges avec le Canada, la LCAP était censée faciliter l'échange international de données. Avez-vous remédié à ce problème ou comblé ce besoin? Pourriez-vous nous parler de vos communications avec le Canada?

● (1155)

M. Louis Lau: Comme je l'ai dit, le Canada participe à des conférences internationales concernant la compromission de courriels d'affaires. Il est disposé à collaborer avec Interpol et d'autres pays pour s'attaquer à ces enjeux. Je dois dire qu'à l'heure actuelle, nous n'avons pas de système établi pour communiquer des renseignements sur les cas avec le Canada ou d'autres pays qui ont les mêmes inquiétudes, mais...

M. Frank Baylis: Si vous n'avez pas ces systèmes, est-ce parce que vous ne pouvez pas recevoir ces renseignements ou parce que le Canada ne vous les communique pas? Est-ce parce qu'Interpol n'est pas encore prête à recevoir ces données?

M. Louis Lau: Oui et non. Nous n'avons pas les systèmes pour le faire. De plus, il nous faut envisager comment nous utiliserons les données qui nous sont communiquées, même si, un jour, disons, nous aurons les systèmes pour les analyser.

Je comprends que la situation est un peu différente de celle des pays européens. Europol possède les systèmes. Les pays de l'Union européenne aussi et les analystes de données. La situation d'Europol est plutôt différente de celle d'Interpol.

M. Frank Baylis: Merci.

Monsieur Lewis, des témoins nous ont encore dit, notamment, au sujet des courriels malicieux qu'il fallait imposer à leurs expéditeurs des sanctions plus rigoureuses que s'ils avaient commis une erreur accidentelle, par exemple, l'envoi, par Rogers, de 100 000 courriels, sans tentative d'hameçonnage ou d'installation de logiciel espion. Ils préconisent cette distinction. Qu'en pensez-vous?

M. Chris Lewis: La loi prévoit déjà beaucoup de ces situations. Il suffit à l'auteur du courriel de nous écrire une lettre avec promesse de ne pas recommencer. C'est déjà dans la loi.

À mon avis, on peut éviter de lourdes sanctions ou même toute sanction si on peut établir le caractère légitime de ses activités et prouver la simple erreur. Le régime est assez modéré. Par exemple, des dispositions autorisent le CRTC et ainsi de suite à intenter un procès au lieu du particulier exerçant son droit privé d'action.

La loi est assez bien faite. Elle est raisonnable. Elle n'impose pas automatiquement une amende pour tel type d'action. Elle n'est pas faite ainsi. À partir d'un contexte de...

M. Frank Baylis: Très bien. Changement de sujet: constatez-vous, d'après votre expérience de l'examen des vieux courriels de Nortel et tout le reste, une réduction du pollupostage en provenance du Canada? Le constatez-vous, si vous voyez ce que je veux dire?

M. Chris Lewis: Oui. Je m'intéresse particulièrement aux réseaux d'ordinateurs zombis, mais je vois bien ce qui se passe ailleurs. Il y a beaucoup moins de ce que vous appelleriez des courriels de masse envoyés par erreur. Nous voyons le côté criminel. Il y a plus de gris. Le noir prédomine. Nous sommes toujours à la poursuite des dirigeants de réseaux d'ordinateurs zombis ayant un affilié canadien, et tout ça. Nous en voyons beaucoup. Pour toutes sortes de choses, nous pouvons remonter à des Canadiens, à des hébergeurs canadiens. Ils forment un maillon contre lequel le CRTC a été vraiment efficace en pouvant s'adresser à un hébergeur...

M. Frank Baylis: Vous constatez l'existence de logiciels malveillants, qui ne proviennent pas nécessairement du Canada, mais d'une entreprise ayant des affiliés au Canada. C'est bien ce que vous dites?

● (1200)

M. Chris Lewis: Un exemple est la publicité de fausses pilules, envoyée par des groupes nombreux dont les courriels comportent un hyperlien vers le site où se vendent ces pilules illégales. À l'activation de ce lien, qui amène le client sur le site, l'affilié est automatiquement crédité d'un cent. Ça se passe comme ça.

L'autre forme, dont j'ai parlé, est l'hébergement...

M. Frank Baylis: Et cet affilié est un Canadien.

M. Chris Lewis: C'était un Canadien.

M. Frank Baylis: À votre connaissance, est-ce que le CRTC réprime ces activités dont vous êtes le témoin?

M. Chris Lewis: Oui. J'ignore si son intervention a toujours abouti, mais il enquête.

L'autre mode d'intervention, moins judiciaire, consiste à s'attaquer aux Canadiens qui, sur le Web, fournissent des services d'hébergement aux participants d'une infrastructure de pollupostage criminel, c'est-à-dire du site Web de vente de pilules ou d'un point de commande et de contrôle de réseaux malveillants d'ordinateurs zombis...

M. Frank Baylis: Le libellé de la Loi canadienne anti-pourriel lui accorde-t-il des pouvoirs suffisants contre ce genre d'activité malveillante? Faut-il renforcer la loi ou la modifier...

M. Chris Lewis: Elle est tout à fait satisfaisante. Le CRTC a besoin de plus de temps et d'expérience dans ses rapports avec ces gens.

M. Frank Baylis: Est-ce que vous dites que la loi est satisfaisante, mais que le CRTC pourrait faire plus pour s'attaquer à eux?

M. Chris Lewis: Oui. C'est une question d'expérience, de temps et d'assiduité à la tâche. M. Lau ne voit pas l'interaction du CRTC avec les organisations, la police et les organismes de réglementation internationaux. Moi je la vois.

M. Frank Baylis: Vous voyez qu'il...

M. Chris Lewis: Oui. Il s'en passe beaucoup plus que ce que nous avions l'habitude de voir.

Le président: Merci beaucoup. Nous passons à un autre intervenant.

[*Français*]

Monsieur Bernier, vous disposez de cinq minutes.

L'hon. Maxime Bernier (Beauce, PCC): Je vous remercie, monsieur le président.

[*Traduction*]

Ma première question est destinée à Mme Arsenault.

[*Français*]

Bonjour, madame Arsenault.

[*Traduction*]

Les coûts, tout est question de coûts. Vous avez expliqué, en réponse à mes collègues, ce qu'ils sont pour la grande entreprise. Mais que pourrait faire une PME qui ambitionne de faire du bon marketing pour se conformer à la loi? Avez-vous des PME parmi vos clients? Savez-vous ce qu'elles font pour respecter la loi?

Mme Kim Arsenault: Oui. Nous discutons beaucoup des risques que les organisations sont disposées à courir. Une grande institution financière très connue y sera très peu disposée, tandis qu'un petit joueur pourrait volontiers en courir de plus grands. Ses politiques et ses procédures sont donc susceptibles de ne pas être aussi rigides que celles de la grande institution. Beaucoup de ses semblables adoptent les pratiques exemplaires typiques de leur secteur. Même s'ils risquent de ne pas pouvoir se conformer rigoureusement à la lettre de la loi, ils se sentent suffisamment à l'aise de suivre les pratiques exemplaires légitimes de l'industrie en matière de courriels, c'est-à-dire en envoyer aux personnes qui leur ont manifesté le désir d'en recevoir, leur faire parvenir des messages pertinents et supprimer les noms des personnes qui veulent se désinscrire. Il leur est ensuite un peu plus facile de profiter de l'initiative de marketing par courriel. Pour eux, les coûts ne seront pas aussi élevés.

Encore une fois, la grande marque doit posséder la technologie qui permet, si on le lui demande, de prouver exactement quelle version du courriel elle a envoyée.

Permettez-moi un exemple. Certaines grandes entreprises veulent envoyer un million de versions différentes d'un courriel. Ça fait longtemps qu'elles n'emploient plus la méthode de l'envoi du même courriel à tous ses clients potentiels inscrits. Elles cherchent une configuration de leur système pour prouver, quand on le leur demandera, que, à telle date, elles ont envoyé telle version précise de tel courriel à tel client. C'est une tâche difficile. Les petites organisations ne sont pas parvenues à ce degré de complexité.

L'hon. Maxime Bernier: Vous demandez plus de clarté dans les lignes directrices du CRTC et du gouvernement.

Mme Kim Arsenault: Absolument.

L'hon. Maxime Bernier: Très bien.

Monsieur Lewis, vous offrez vos services aux grandes organisations étatiques, mais, d'après ce que j'ai compris, le public ne peut pas se procurer votre logiciel. Pourriez-vous expliquer comment ferait une petite entreprise pour être aussi sécurisée qu'une organisation étatique? Comment pourra-t-elle accéder au genre de technologie que vous offrez à l'État?

● (1205)

M. Chris Lewis: Spamhaus offre gratuitement ses données sur les menaces aux particuliers et aux petites entreprises. Il l'a toujours fait. Nous sommes tous convaincus de bien agir. Mais nous supposons que nous permettons à la grande organisation d'économiser des millions de dollars et de rendre ses clients heureux. Nous avons des frais de gestion, nous achetons du matériel. Elle doit payer. Mais, pour les petits joueurs, c'est gratuit.

Toutes les équipes nationales d'intervention contre les incidents obtiennent nos données gratuitement, ce qui les aide à sécuriser leur pays. Le Centre canadien de réponse aux incidents cybernétiques aussi. Le CRTC en obtient certaines gratuitement. Nous le faisons souvent. Peu de compagnies font comme nous.

Les petites entreprises qui essaient de se protéger peuvent se servir de nos données, de la façon que nous proposons. Elles peuvent s'adresser à d'autres organisations possédant des données semblables ou disposant de logiciels. Nous avons tendance à ne pas exiger l'achat d'un logiciel par l'utilisateur. Il achète l'information et emploie le logiciel qu'il possède déjà, mais on peut bien mieux se protéger par d'autres solutions.

L'hon. Maxime Bernier: Croyez-vous que beaucoup d'entreprises privées peuvent offrir ces services aux PME?

M. Chris Lewis: Oui. En fait, en réponse à la question sur les méthodes de marketing des petites organisations et sur leur souci de s'en charger elles-mêmes, elle a parlé de l'existence d'un marché florissant d'entreprises spécialisées dans la conduite de campagnes de publicité et de marketing pour les petites entreprises. Certains de leurs services sont gratuits ou presque. Les petits joueurs peuvent utiliser leur matériel, leurs logiciels et leurs produits et, moyennant très peu d'argent. ils peuvent être assez sûrs de respecter absolument la Loi canadienne anti-pourriel.

L'hon. Maxime Bernier: Merci.

Le président: Merci.

Monsieur Jowhari, vous disposez de cinq minutes.

M. Majid Jowhari (Richmond Hill, Lib.): Merci, monsieur le président. Je partage mon temps avec M. Lametti.

Je remercie tous les témoins.

Monsieur Lewis, je vous questionnerai surtout sur le droit privé d'action.

Des témoins nous ont conseillé de focaliser davantage ce droit et d'adapter la punition à la nature du crime. J'ai cru comprendre, d'après vos observations, que d'autres éléments en place pouvaient nous épargner la peine de le focaliser davantage, notamment la disposition relative à l'erreur commise de bonne foi et la disposition accordant le droit prioritaire d'intervenir.

Vous avez précisément parlé de la capacité prioritaire d'intervention de l'ARC. Vous avez aussi souligné la différence entre les lois canadiennes et américaines. Pouvez-vous en dire plus sur la capacité prioritaire d'intervention de l'ARC et sur son efficacité ainsi que sur les différences qui existent entre les lois?

M. Chris Lewis: Avez-vous dit l'ARC?

M. Majid Jowhari: Désolé. Je voulais dire le CRTC. Mon erreur.

M. Chris Lewis: Très bien.

Je pense que si on invoque un droit privé d'action contre la société X et que le CRTC ou le commissaire à la protection de la vie privée ou la Direction générale de la concurrence décide de prendre l'affaire en main, le droit privé d'action doit céder la place.

C'est ainsi que je comprends le mécanisme de la loi en la matière. Le CRTC peut avoir préséance sur un droit privé d'action.

M. Majid Jowhari: Comment peut-on le déterminer?

M. Chris Lewis: Eh bien, par exemple, si le CRTC s'apercevait que je poursuis quelqu'un pour avoir commis telle action, il pourrait dire que ça fait partie d'un problème plus vaste, invoquer ce genre d'argument, puis mettre sur pied une enquête. Il suspend ensuite le droit privé d'action

M. Majid Jowhari: D'accord.

Qu'en est-il alors de la différence entre les lois canadiennes et américaines?

M. Chris Lewis: À mon avis, elle réside surtout dans le fait que, au Canada, contrairement aux États-Unis, celui qui perd paie. Ça signifie qu'on peut, grâce à une avalanche de faux procès, encaisser énormément d'argent, des procès qui feront souvent reculer les adversaires.

Je crois que c'est arrivé dans le Nevada. Un cabinet d'avocats a obtenu des détenus d'une prison l'abandon, à son profit, de tous leurs droits privés d'action contre les courriels indésirables. Grâce à tous les courriels reçus, il a encaissé beaucoup d'argent en intentant des poursuites contre les expéditeurs. À mon avis, ça ne peut pas se produire ici.

● (1210)

M. Majid Jowhari: D'accord.

Je cède la place à M. Lametti.

M. David Lametti (LaSalle—Émard—Verdun, Lib.): C'est sur un sujet semblable, le droit privé d'action.

Limiteriez-vous cette possibilité aux torts réellement subis ou conserveriez-vous les dommages-intérêts prévus par la loi?

M. Chris Lewis: Je maintiendrais les dommages-intérêts prévus dans la loi, parce que certaines preuves sont extrêmement difficile à faire. Voici comment ça devrait se passer en réalité: « j'ai reçu ce courriel après avoir demandé qu'on cesse d'en envoyer ». Ça devrait suffire, tant que le tribunal, si l'affaire concerne un cas particulier, est d'avis que c'est plausible.

Il faut rester assez général, parce qu'il ne faudrait pas seulement viser les courriels indésirables, ce que vise partiellement la Loi canadienne anti-pourriel. La loi vise aussi les attaques informatiques par saturation. Si on se limite au courriel indésirable, on laisse à son voisin la décision de faire sauter son ordinateur. Il peut le faire maintenant, et les voies judiciaires se révéleraient très difficiles.

Le droit privé d'action permet de réagir, parce qu'on vous a fait parvenir un message non sollicité. C'est visé par la loi.

Voilà pourquoi j'ai parlé, dans mon exposé, de ma satisfaction devant le fait que cette loi avait été rédigée pour prévoir à peu près tout ce à quoi nous pouvions songer. Jusqu'ici, elle le permettrait encore, très concrètement, après 12 ou 13 ans. Ce n'est pas mal.

Je n'en modifierais pas grand-chose. Je m'assurerais de conserver les mêmes limites, peut-être, sur les abus, mais je pense que la portée générale est à peu près correcte.

M. David Lametti: D'accord.

De même, par rapport au droit privé d'action, quel est votre avis sur les possibilités d'action collective?

M. Chris Lewis: Ça me rend effectivement nerveux.

Dans le cas du droit privé d'action, il ne me déplairait pas qu'il ait un plus... Vous savez, dans trois ans, ce droit sera autorisé. J'aime cette façon de parfois procéder par gradation: « Comment ça va jusqu'ici? » — « Bien. Encore un tour de vis. Si ça ne marche pas, on peut revenir en arrière ». Comme la loi prévoit un examen obligatoire de ses dispositions, c'est une possibilité.

Je ne voudrais pas vraiment des actions collectives dans le droit privé d'action maintenant. Allons-y avec les actions des particuliers.

Le président: Merci beaucoup.

Revenons à M. Bernier.

[*Français*]

Vous disposez encore de cinq minutes.

[*Traduction*]

L'hon. Maxime Bernier: Merci beaucoup.

Monsieur Lau, merci beaucoup d'être avec nous grâce à la technologie.

Petite question sur les rapports du Canada avec d'autres pays pour collaborer avec vous et votre organisation.

Croyez-vous que nous ayons besoin d'un nouveau traité international? Est-ce que le traité actuel pour la communication de renseignements et la collaboration suffit ou faut-il relever nos rapports avec d'autres pays au niveau de nos rapports avec Interpol?

M. Louis Lau: Je dirais que, dans la plupart des cas, la situation actuelle est satisfaisante. Nous avons établi des systèmes pour la communication de renseignements et la connexion de différentes forces policières à la plateforme d'Interpol. Je dirais que c'est suffisant pour des objectifs généraux.

Pour les renseignements sur le publipostage excessif, en particulier, je proposerais plus de communications entre le Canada et d'autres pays, et je m'en réjouirais, mais, pour les enquêtes criminelles ou la communication de renseignements sur une affaire, je dirais que le système actuellement fourni par Interpol est suffisant.

● (1215)

L'hon. Maxime Bernier: Merci.

Je partage mon temps avec Jim.

Le président: Vous disposez de trois minutes et demie.

M. Jim Eglinski: Je vais poser une question à Mme Arsenault et à M. Lewis.

Supposons qu'aujourd'hui, c'est votre grande journée et que vous savez ce que la Loi canadienne antipourriel comporte. Dites une chose que vous changeriez aujourd'hui si vous en aviez la chance. Vous pouvez tous les deux répondre.

Mme Kim Arsenault: Abolir les périodes de six mois et de deux ans.

M. Jim Eglinski: Pouvez-vous nous en expliquer la raison?

Mme Kim Arsenault: C'est inutilement complexe pour bien des organisations. Les consommateurs ne comprennent pas nécessairement la relation fondée sur le consentement « tacite », et il est difficile pour les organisations de gérer cela. Ce qui définit la période de six mois par rapport à la période de deux ans n'est pas clair pour bien des sociétés. À cause de cela, certaines organisations ne se fient pas du tout au consentement tacite, et cela leur fait perdre des occasions. Je pense qu'il serait plus simple d'abolir les périodes de six mois et de deux ans.

M. Jim Eglinski: Monsieur Lewis, aimeriez-vous dire quelque chose?

M. Chris Lewis: J'ai dit avoir été impressionné par la Loi quand elle a été proposée initialement, et je le demeure. Je réglerais quelques petits aspects opérationnels: les ressources, la stabilité et de meilleures interactions. J'aimerais que le DPA, ou droit privé d'action, soit en place. Il faut probablement clarifier les choses, mais je pense que la Loi est vraiment bonne dans son état actuel.

M. Jim Eglinski: Vous en êtes satisfait, alors que Mme Arsenault voudrait y voir un changement.

Combien de temps me reste-t-il? Pas beaucoup?

Le président: Il vous reste une minute et demie.

M. Jim Eglinski: Madame Arsenault, vous traitez avec des clients. Croyez-vous que la LCAP est assez claire, ou plutôt qu'il faut y apporter des changements à certains égards pour rendre...

Mme Kim Arsenault: Je ne crois pas qu'elle est assez claire. Nous sommes une agence et nous conseillons beaucoup nos clients afin qu'ils soient en mesure de faire le nécessaire pour se conformer à la LCAP. Cependant, de nombreuses organisations avec lesquelles nous ne travaillons pas s'adressent à nous et nous demandent conseil. C'est bien trop complexe. Il y a beaucoup d'ambiguïté. Il y a des choses contradictoires, dans la Loi.

Je pense que le gouvernement peut faire beaucoup mieux et clarifier la Loi pour qu'elle n'en laisse pas tant à l'interprétation. Je pense que ce qui est difficile pour les organisations, c'est qu'il leur incombe de l'interpréter. Il faut supprimer les zones grises.

M. Jim Eglinski: Je crois qu'il me reste quelques secondes pour entendre M. Lewis.

Le président: Vous avez 30 secondes.

M. Jim Eglinski: Croyez-vous que certaines sociétés rendent les choses exagérément complexes, comme vous le dites, en particulier les grandes sociétés? On dirait que cela devient plus complexe quand les services juridiques des grandes sociétés s'en mêlent.

M. Chris Lewis: Mon travail est très étroitement lié au droit depuis très longtemps, et ce qui me frappe, c'est qu'il est plus simple qu'il n'y paraît de se conformer. La Loi ne comporte que quatre articles exécutoires en tout, et tout le reste n'est que de l'infrastructure.

Oui, il faut y apporter des éclaircissements, mais je pense que bien des gens compliquent les choses beaucoup plus qu'il le faut. Dans certains cas, je pense qu'ils le font pour élargir leurs occasions d'affaires.

Le président: Merci.

C'est maintenant au tour de M. Sheehan.

Vous avez cinq minutes.

M. Terry Sheehan (Sault Ste. Marie, Lib.): Merci beaucoup à tous nos présentateurs.

Ma première question s'adresse à Kim.

Dans votre déclaration, vous avez mentionné que la LCAP s'applique aux médias sociaux, comme Facebook, entre autres. Nous avons entendu toute sorte de choses dans les divers témoignages, et il y a certainement de la confusion: oui, elle s'applique; non, elle ne s'applique pas. Puis le Bureau de la concurrence nous a affirmé que, oui, la Loi s'applique à ces formes de messages électroniques.

Pouvez-vous nous décrire ce qui différencie d'après vous les messages dans les médias sociaux des messages par courriel, selon la LCAP? Nous avons consacré beaucoup de temps au courriel, mais quel est l'effet exact sur la LCAP, concernant les médias sociaux?

Mme Kim Arsenault: Ce qu'on nous demande très souvent, c'est: « Avons-nous le droit d'utiliser des médias sociaux comme LinkedIn pour communiquer dans l'environnement interentreprises? » Il y a beaucoup d'incertitude à savoir si les gens peuvent utiliser LinkedIn. L'adresse de courriel est très évidente. Est-ce que cela me donne un consentement implicite pour une période de six mois? Est-ce que cela relève de l'exemption relative aux communications interentreprises?

Il y a beaucoup d'inconnu concernant l'utilisation de LinkedIn. Certaines organisations, plutôt que de communiquer ainsi, vont simplement prendre le téléphone et utiliser des façons traditionnelles de faire de la prospection et de conclure des ventes. Ce n'est pas efficace, de nos jours. Nous avons besoin de plus de clarté sur les façons dont les entreprises — surtout dans les communications interentreprises — peuvent miser sur les médias sociaux comme LinkedIn pour communiquer convenablement par courriel. Il y a beaucoup trop d'inconnus sur les façons d'utiliser ces outils.

● (1220)

M. Terry Sheehan: Chris, avez-vous quelque chose à dire à propos des médias sociaux?

M. Chris Lewis: L'une des différences fondamentales entre les médias sociaux et le courriel, c'est que pour les médias sociaux, c'est un facteur d'attirance qui joue — vous devez en fait aller chercher le consentement pour faire quelque chose avec cela — alors que le courriel s'appuie sur la poussée. Je vous envoie un courriel, alors que pour les médias sociaux, je suis allé quelque part pour voir quelque chose.

Là où cela s'embrouille parfois, avec des choses comme LinkedIn, c'est que vous êtes allé sur la plateforme pour maintenir votre relation professionnelle avec quelqu'un d'autre, puis quelqu'un se met à vous envoyer des publicités. On dirait que c'est surtout une forme de poussée, alors qu'en général, les petites entreprises ont leurs pages Facebook, leurs amis, leurs collègues, et ils écrivent des commentaires sur la nourriture et ce genre de choses. C'est dans une grande mesure un facteur d'attirance. On ne m'impose rien de force. On ne me demande pas d'envoyer de l'argent que je n'aurais pas normalement dépensé pour cela. C'est purement volontaire. J'ai choisi de participer en me servant de mes yeux. Je suis allé à la recherche de cela, alors qu'envoyer une publicité sans rapport à un compte LinkedIn est une chose complètement différente. En fait, pour l'exemple de LinkedIn en particulier, les seules choses qui sont vraiment pertinentes, ce sont les offres d'emplois.

M. Terry Sheehan: Merci.

Kim, nous avons souvent entendu des témoignages voulant que les entreprises trouvent cela ambigu à cause du manque d'information ou de communication. Des gens du CRTC sont venus ici et nous ont dit que beaucoup de questions se trouvent sur le Web, mais c'est très passif. Il faut que vous alliez voir. De nombreuses entreprises décident de ne pas se lancer en marketing électronique ou retiennent les services d'avocats qui leur disent: « Ne prenez même pas ce risque. »

Votre travail est essentiellement d'éduquer les gens et de les aider quand le gouvernement n'est peut-être pas là pour le faire. Quel conseil donneriez-vous au gouvernement pour qu'il éduque mieux le public?

Mme Kim Arsenault: Je ne crois pas que le site Web du gouvernement est mis à jour activement aussi souvent qu'il le pourrait de manière à fournir de l'information facilement accessible. On pourrait y trouver plus de webinaires. J'ai participé à plusieurs webinaires, et il arrive qu'on ne réponde pas directement aux questions, ce qui fait que même les réponses aux questions sont ambiguës. Concernant ce que M. Lewis a dit, le gouvernement a besoin d'un peu plus de temps et d'expérience pour comprendre entièrement les médias numériques et l'incidence de la LCAP sur le droit.

Les réponses du gouvernement sont souvent: « Interprétez la Loi et servez-vous de votre jugement. » C'est très difficile pour les sociétés qui ne veulent pas courir de gros risques. Cela leur fait craindre de subir de graves conséquences si leur interprétation n'est pas la bonne.

Encore une fois, il faut supprimer les zones grises et fournir des exemples plus précis afin qu'il n'y ait pas matière à interprétation. Il faut plus de webinaires et de documents, et les organisations doivent être consultées. De nombreuses organisations craignent de s'adresser au CRTC et de se retrouver ainsi par inadvertance avec un problème. De nombreuses entreprises veulent passer inaperçues. Cela aiderait les organisations si le CRTC semblait plus ouvert à la conversation.

Le président: Merci.

M. Terry Sheehan: C'était d'excellentes observations.

Le président: Monsieur Masse, vous avez deux minutes.

M. Brian Masse: Merci.

Les répercussions dont partie des choses auxquelles nous faisons toujours face. Si je reçois une annonce par courrier, je dois en payer le recyclage par l'intermédiaire de ma municipalité, et je dois payer de mon temps. Si je vois une publicité à la télé, ma télé ne se trouve pas infectée par un virus. C'est mon temps et mon espace. Je peux changer de poste, ou éteindre la télé.

Prenons l'exemple d'une publicité légitime que je reçois de PlayStation et à laquelle j'ai consenti. Le problème, c'est l'atteinte à ma vie privée qui se produit après, ce qui a été le cas.

Quelles sont les vraies répercussions alors, concernant l'engagement que nous avons pour la protection de la vie privée et l'utilisation? Il y a deux choses. Que trouvez-vous juste que les consommateurs tirent de cela, en particulier concernant les messages électroniques non sollicités et leur coût? Que trouvez-vous juste?

Les dispositifs de communication n'ont pas vraiment été conçus pour permettre que le consommateur soit inondé de publicités. On les utilise actuellement pour les urgences et pour beaucoup d'autres choses, en plus des communications. Quand mon téléphone est atteint d'un virus à cause d'un courriel non sollicité, ce n'est pas qu'un inconvénient; c'est un vrai problème parce qu'il ne peut fonctionner. Que trouvez-vous juste pour le consommateur, dans cette relation? J'aimerais vos observations à ce sujet.

● (1225)

Mme Kim Arsenault: En effet, il faut que les consommateurs soient protégés contre ce genre d'activité malveillante. Ce que nous constatons, c'est que les mesures législatives ont des effets sur les spécialistes du cybermarketing légitimes qui essaient de faire de l'excellent travail et d'envoyer aux consommateurs canadiens des offres pertinentes et du contenu pertinent, et qui, dans l'environnement interentreprises, s'efforcent d'être des leaders d'opinion et de produire de l'excellent contenu. Les spécialistes légitimes du marketing veulent protéger leurs consommateurs tout en étant motivants et pertinents.

M. Brian Masse: Vous dites qu'ils sont « légitimes ». Très bien. Mais qu'est-ce qui leur donne vraiment le droit pour commencer de faire obstruction à la vie privée, d'en causer la destruction ou de l'enfreindre?

Je comprends ce que vous dites — que le CRTC doit communiquer plus activement et tout cela —, mais il me semble que nous regardons les choses à l'envers, dans une certaine mesure. Le coût n'est pas assumé par ceux qui envoient les messages, mais bien par les gens qui les reçoivent. Si je suis engagé dans une relation selon laquelle j'ai convenu de recevoir vos courriels, ou selon laquelle je n'ai pas convenu de cela, et que vos messages finissent par me coûter du temps, de l'argent et autre, que trouvez-vous juste pour moi, à titre de consommateur, pour que je puisse me sortir de cela?

Mme Kim Arsenault: C'est une excellente question...

M. Brian Masse: C'est à ceux qui font le marketing qu'il incombe de payer pour cette restitution.

Mme Kim Arsenault: Tout à fait. Je ne pense pas que PlayStation s'attendait à se faire pirater. Je crois qu'elle essayait de protéger les données sur ses consommateurs aussi bien qu'elle le pouvait. La réalité, c'est que le monde numérique évolue plus vite que ce que bien des gens prévoyaient et qu'il y a de l'activité malveillante. M. Lewis serait sans doute mieux placé que moi pour vous parler de cela.

Le président: Je suis désolé, mais je vais devoir vous interrompre. Je vous ai laissé aller un peu trop longtemps. Vous aurez une autre période de sept minutes, cependant.

M. Brian Masse: D'accord. Merci, monsieur le président.

Le président: Nous avons terminé notre premier tour, et nous avons du temps pour quelques autres questions. Nous allons revenir à Mme Ng pour sept minutes. Ensuite, ce sera M. Masse, puis M. Baylis.

Allez-y, madame Ng.

Mme Mary Ng (Markham—Thornhill, Lib.): Bonjour. Merci à tous les témoins de leur présence. Je n'ai que quelques questions de clarification.

Madame Arsenault, vous avez dit de la LCAP qu'elle peut offrir un cadre qui permet de meilleures données et de meilleurs courriels et, par conséquent, de meilleures affaires pour les spécialistes en marketing. Vous avez ensuite suggéré des moyens de simplifier la loi actuelle en utilisant la définition d'un MEC, ou message électronique commercial, ou en faisant disparaître la période de six mois ou de deux ans.

La question ne s'adresse pas à vous, en fait, mais à M. Lewis, mais je lui donne le contexte.

Mme Arsenault a laissé entendre qu'elle et ses clients veulent s'engager dans de bonnes pratiques. Ils veulent permettre aux petites, moyennes et grandes entreprises de faire du bon marketing et de faire des affaires dans l'univers numérique actuel.

Trouvez-vous que les simplifications qu'elle suggère sont les bons ajustements à apporter à la LCAP pour la rendre plus efficace pour le milieu des affaires tout en garantissant que les protections voulues sont là et sont maintenues?

M. Chris Lewis: Je ne sais pas de quelles périodes elle parlait. Est-ce quelque chose qui est lié à...

Mme Kim Arsenault: C'est la demande présentée au cours des six mois par rapport aux deux années de relations d'affaires en cours. Si une personne présente une demande au moyen d'un formulaire, vous avez six mois de consentement implicite, alors que si vous avez des relations d'affaires en cours et téléchargez...

● (1230)

M. Chris Lewis: D'accord.

Mme Mary Ng: Nous avons entendu ces deux suggestions. Elles nous ont été faites par d'autres témoins. J'aimerais connaître votre perspective, à savoir si c'est sensé.

M. Chris Lewis: Du moment que c'est l'utilisateur qui a lancé les choses, plutôt que l'autre côté, une période raisonnable de six mois à un an... Je ne trouve pas que vous devriez rendre cela plus compliqué en ayant quelque chose de différent pour des circonstances différentes.

Mme Mary Ng: Ce que nous avons entendu, c'est que la capacité des entreprises de suivre le moment où le consentement a été donné, expressément ou implicitement, et l'exigence selon laquelle les entreprises doivent continuer de faire cela au fil du temps...

M. Chris Lewis: Cela m'a toujours frappé comme étant un peu étrange. Je suis un client de longue date de ma banque, et une fois de temps en temps, je reçois un message me demandant si j'accepte de continuer de recevoir ceci. Ce que je dis, c'est: « Je traite avec vous au moins une douzaine de fois par année, ce qui fait que c'est un peu stupide. » Une période de six mois ou d'un an pour une transaction commerciale ou une demande, c'est le genre de choses... Ils devraient avoir la permission indéfiniment. Il n'est pas nécessaire de renouveler cela.

Mme Mary Ng: Vous dites que c'est une modification acceptable de la LCAP, et que cela aiderait...

M. Chris Lewis: Oui. En fait, je suis sûr que si on présentait au CRTC quelque chose qui serait axé uniquement sur cela, ils diraient: « C'est du cas par cas, et vous êtes une personne raisonnable. Vous avez fait preuve de diligence raisonnable et vous avez accompli un travail raisonnable, alors où est le problème? »

Mme Mary Ng: C'est bon. Merci.

D'un côté, madame Arsenault, vous avez dit que le CRTC doit donner des directives plus claires aux entreprises. Monsieur Lewis, vous avez dit que le CRTC doit travailler à s'améliorer dans son rôle relatif à la LCAP.

Qu'est-ce qui doit se produire? Autrement dit, devons-nous dire au CRTC que d'après de nombreux témoignages reçus, il y a un manque de clarté et les entreprises auraient besoin de meilleures directives et de plus de clarté sur le plan de l'interprétation, que ce soit sous la forme de webinaires ou de simples communications — qu'il ne s'agit que d'une question de clarté et que la LCAP comme telle est bien —, ou devons-nous faire quelque chose?

M. Chris Lewis: Je crois qu'un des aspects du problème que nous voyons aujourd'hui, c'est que quand vous parlez à une personne au CRTC, si ce n'est pas un avocat et qu'elle ne parle pas au nom du CRTC, elle ne va pas juger spécialement une pratique par rapport à une autre.

Je me demande s'il serait mieux que le CRTC essaie de plutôt dire: « Voici ce que nous essayons d'accomplir. Si vous faites preuve de diligence raisonnable et que vous suivez les principes de base en fonction de ce que nous essayons de faire, vous n'aurez pas de problème. »

Mme Mary Ng: Est-ce que cela serait utile? C'est ce que beaucoup de témoins nous ont mentionné, et je comprends ce que vous dites, monsieur Lewis, à propos de l'importance de ce qu'on peut entendre. J'essaie de comprendre ce qu'il en est afin de voir si nous pouvons trouver un bon équilibre pour, d'une part, protéger les consommateurs et, d'autre part, faciliter les activités des entreprises, tout en comprenant que les pourriels constituent la première étape d'une activité très malveillante et frauduleuse à laquelle nous devons prêter une grande attention.

M. Chris Lewis: Il faut s'assurer que les principes de base sont compris. On peut ensuite indiquer en quoi ils sont raisonnables. La loi cherche toujours à établir des limites concrètes, mais devant les tribunaux, les humains s'appuient sur des principes de base et sur ce qui est raisonnable, c'est-à-dire sur ce qu'une personne raisonnable ferait, sur des critères de diligence raisonnable et ainsi de suite. La sensibilisation des gens à la façon dont il faut comprendre et gérer cela dans un domaine où on n'a jamais vu quoi que ce soit de semblable peut s'avérer un processus de longue haleine.

Mme Mary Ng: Nous avons entendu parler d'une façon pragmatique de procéder, peut-être de la part du CRTC, pour faire en sorte d'avoir des renseignements pragmatiques qui prennent en considération le fonctionnement des entreprises et qui présentent une application, une interprétation, une communication et une compréhension pratiques afin que les exploitants de PME possèdent les outils et l'interprétation nécessaires sans devoir embaucher une équipe juridique pour essayer de comprendre l'objectif de cette mesure législative.

● (1235)

Mme Kim Arsenault: Je suis d'accord.

M. Chris Lewis: Une documentation d'interprétation pourrait également être utile.

Mme Mary Ng: Bien.

Mme Kim Arsenault: Donnez-nous des exemples. La tenue des dossiers nécessite beaucoup d'efforts. Montrez-nous exactement quel est le niveau de documentation nécessaire pour donner suite à une demande.

Mme Mary Ng: Bien sûr.

Me reste-t-il du temps?

Le président: C'est tout ce que vous aviez.

Mme Mary Ng: Merci.

Le président: Nous allons passer à M. Masse, pour sept minutes.

M. Brian Masse: Merci, monsieur le président.

Monsieur Lau, que peut faire le Canada pour être davantage en mesure de lutter contre une partie des polluposteurs internationaux et du contenu que nous recevons dans notre pays? Avant d'avoir la Loi canadienne anti-pourriel, le Canada était considéré comme un des paradis des pourriels. À vrai dire, notre pays comptait parmi les territoires d'origine d'une grande partie de ce qui se faisait à l'échelle internationale. Y a-t-il une chose que nous pouvons mieux faire ou qui peut fonctionner dans un contexte plus rigoureux?

L'une des frustrations dont on nous fait part, c'est que cela tire souvent son origine de sources internationales, que les mesures que nous prenons ici n'y changent absolument rien et que nous ferions donc aussi bien d'alléger les restrictions au pays, car cela vient du Nigéria ou d'ailleurs. Je ne partage pas cet avis, car je ne crois pas que c'est une solution au bout du compte, mais que pouvons-nous faire, que ce soit en tirant parti de la mise en commun de nos expériences, d'organisations, de ressources ou d'autres choses? Avez-vous des propositions?

Une fois de plus, je vois la question un peu différemment, dans le sens où l'envoi de messages électroniques dans de la documentation, surtout lorsqu'il s'agit de messages non sollicités, est un privilège, et quelqu'un ne devrait pas avoir le droit de le faire, car on possède et contrôle l'appareil, et on s'en sert également pour apporter une contribution financière. Avez-vous des propositions qui s'appliquent à notre pays?

M. Louis Lau: Je peux peut-être en formuler d'un point de vue pratique. Vous m'avez probablement entendu dire qu'Interpol travaille avec un des pays d'Afrique de l'Ouest. Nous avons pu analyser l'ordinateur d'un suspect et nous avons constaté qu'il utilisait sur Internet des programmes automatisés pour envoyer des pourriels. Imaginez la saisie de fausses données personnelles dans ce genre de programmes et l'envoi automatique de courriels à des milliers de destinataires.

On pourrait s'attendre à ce que ces programmes soient exécutés à l'aide d'un serveur situé dans un des pays visés, n'est-ce pas? S'il est exécuté au Canada, par exemple, de quelle façon les autorités ou les organismes d'application de la loi peuvent-elles s'y attaquer? De plus, si ce genre de serveur ou de service n'est pas exécuté au Canada, mais qu'il est contrôlé par des Canadiens, existe-t-il des dispositions qui permettent aux autorités canadiennes de travailler avec d'autres pays ou d'autres organismes d'application de la loi pour lutter contre les services du genre? À mon avis, il s'agit là des faits.

M. Brian Masse: C'est intéressant, car nous n'avons pas trop pensé à cela. Je veux bien comprendre. Un programme, une technologie ou un service pourrait être mis au point au Canada et ensuite exporté pour pouvoir envoyer au pays des pourriels et d'autres messages non sollicités.

M. Louis Lau: Il y a différents points de vue. Cela peut soit être mis au point au Canada et exploité ensuite dans d'autre pays, soit être mis au point et exploité au Canada. Je crois que nous devons en tenir compte au moment d'envisager une loi. Cela porte davantage sur l'aspect criminel, et c'est très malveillant.

M. Brian Masse: C'est le point central, mais cela devient malheureusement un moyen.

Monsieur Lewis, je suis désolé. Je n'avais pas l'intention de vous ignorer aujourd'hui...

Des voix: Oh, oh!

M. Brian Masse: ... mais les deux témoins précédents font de très bonnes observations.

Que peut-on accomplir au moyen de la LCAP? Un point a été soulevé, et j'ai fait une blague en disant que nous avions besoin d'un manuel *La LCAP pour les nuls*. J'ai une certaine empathie. Le manuel ou le règlement devrait être très clair pour que les gens puissent comprendre. C'est un aspect de la question. Je crois toutefois qu'il incombe aux entreprises de comprendre la loi. Cela dit, cela semble un peu difficile, ou certaines décisions semblent un peu floues. Est-ce que cela peut se régler tout seul, avec le temps, ou y a-t-il des choses que nous pouvons améliorer tout de suite pour que les dispositions soient beaucoup plus claires?

● (1240)

M. Chris Lewis: Je ne suis pas certain. Il y a beaucoup d'acteurs. Ils sont tous à un stade différent de compréhension. Certaines personnes en feront plus que ce qui est nécessaire, pour différentes raisons. Les principes de base, les points importants, doivent être clairs. Les entrepreneurs doivent ensuite avoir pour objectif de suivre ces principes de base, et être au fait de certains aspects auxquels ils doivent penser. Il faut leur indiquer clairement qu'ils sont en assez bonne posture tant qu'ils font un travail raisonnable.

Pour les grandes entreprises, c'est le prix à payer pour faire des affaires. Elles doivent consacrer plus d'efforts pour se conformer, tandis que pour les petites entreprises qui envoient quelques centaines ou quelques milliers de messages par mois, cela demande moins d'efforts, comme il se doit, mais il y a un prix à payer pour faire des affaires, car, après tout, l'envoi d'un million de courriels coûte beaucoup moins cher que l'envoi de mille messages postaux.

M. Brian Masse: C'est exactement cela. C'est le problème. C'est très abordable pour les entreprises qui veulent procéder ainsi.

Ce qui m'a un peu troublé dans certains des témoignages que nous avons déjà entendus, c'est le cas de comptoirs de limonade, de cousins qui ne pouvaient pas communiquer, de choses du genre. Nous essayons de comprendre comment faire face à un problème grave dans le contexte législatif, de comprendre ce qui doit changer, car la modification de la loi pourrait créer encore plus de problèmes.

M. Chris Lewis: Tout à fait.

M. Brian Masse: Je pense que c'est un des aspects dont on a trop parlé.

M. Chris Lewis: En effet. Les dossiers qui se sont retrouvés devant le CRTC n'ont pas été problématiques du tout à cet égard. Le CRTC n'a poursuivi aucun comptoir de limonade. Il est toujours question de grandes organisations qui ont commis des erreurs ou délibérément fait des choses qu'elles n'auraient vraiment pas dû faire.

Les peines semblent avoir été adéquates pour ce qui est des sociétés. J'ai apporté un des jugements réussis du CRTC. J'ai mentionné que ce sont des gens importants. Ils ne sont pas mal intentionnés, mais il convient de les rendre un peu plus prudents à cet égard. On a mentionné que l'objectif était de les contrarier un peu, pour qu'ils renoncent à recourir au même moyen. Les exploitants de comptoir de limonade ne se verront pas infliger de lourdes peines.

Le président: Merci beaucoup.

Nous allons revenir à M. Baylis pour le dernier tour.

M. Frank Baylis: Monsieur le président, je vais partager mon temps de parole avec M. Longfield et M. Sheehan.

Le président: Bien.

M. Frank Baylis: Monsieur Lewis, il y a une petite contradiction dans votre témoignage. D'une part, vous dites qu'il n'est pas difficile de comprendre la LCAP et que les gens exagèrent un peu, qu'ils ne devraient pas dépenser des millions, des dizaines de milliers ou des centaines de milliers de dollars, comme l'a dit Mme Arsenault, et d'autre part, vous faites volte-face en disant que vous aimeriez également que le droit d'action préalable permette de faire pendre une épée de Damoclès au-dessus de la tête d'une entreprise.

Une entreprise pourrait faire face à des peines de 10 millions de dollars et ensuite à un droit d'action préalable; elle devra dépenser beaucoup d'argent. De toute évidence, si quelqu'un me propose une solution à 695 $ et que j'ai une grande société comme Rogers ou Bell, je ne vais pas mettre cette solution en oeuvre. Il est illogique qu'une chose aussi simple me protège contre les sanctions possibles; les poursuites peuvent facilement coûter des millions de dollars. Comment pouvez-vous concilier ces deux positions?

M. Chris Lewis: Il faut en partie voir ce qui s'est produit au fil des ans ainsi que l'incapacité des gens à gérer des problèmes qui leur sont propres, et comprendre dans quelle mesure les courriels favorisent la commercialisation à grande échelle. Il faut freiner les mesures excessives que nous voyons parfois.

Comme quelqu'un l'a fait remarquer, si toutes les petites entreprises au Canada comprenaient qu'elles n'avaient qu'un seul passe-droit par année, vous auriez constamment un quart de millions de courriels dans votre boîte de réception.

● (1245)

M. Frank Baylis: De nombreux représentants d'entreprises appelés à témoigner nous ont dit que c'est difficile à comprendre. Madame Arsenault, vous venez tout juste de dire que vous vous creusiez encore la tête après avoir parlé aux gens du CRTC.

La question s'adresse à vous deux. Je vais d'abord vous entendre, Madame, pour ensuite passer à vous, monsieur Lewis. Vous avez parlé de la définition de message électronique et de choses du genre. Pouvons-nous vraiment simplifier la loi de sorte que je la comprenne facilement, comme M. Masse l'a dit? Un manuel intitulé *La LCAP pour les nuls* serait bon pour moi. Je sais qu'il me regardait quand il en a parlé...

M. Brian Masse: Pourquoi pas *La LCAP pour les génies*?

M. Frank Baylis: En quoi ce manuel serait-il utile, madame Arsenault?

Mme Kim Arsenault: J'ai souris quand vous avez dit cela. Un manuel intitulé *La LCAP pour les nuls* est une excellente idée selon moi.

Je ne travaille pas au contentieux, mais je pense que les lois devraient toujours être assez faciles à comprendre pour que nous puissions nous y conformer. La législation sur la conduite en état d'ébriété est on ne peut plus claire. Dans le cas de la LCAP, une trop grande partie de la loi laisse place à l'interprétation. Je pense donc que le CRTC, avec lequel j'ai travaillé, doit lui-même mieux la comprendre, et ensuite...

M. Frank Baylis: Vous dites qu'il est difficile pour les gens du CRTC de la comprendre parce qu'elle laisse trop place à l'interprétation, et vous aimeriez qu'une grande partie des dispositions soient resserrées davantage.

Monsieur Lewis, serait-il logique selon vous de préciser davantage une grande partie des définitions, comme la définition de MÉC?

M. Chris Lewis: Ce qui me préoccupe surtout, c'est que des définitions plus précises contraignent les PME à faire plus de travail que ce qui est nécessaire. Vous rendriez ces définitions plus appropriées pour les grandes organisations pour ensuite essayer de les appliquer aux petites ou aux très petites entreprises, comme une entreprise unipersonnelle. J'hésite donc un peu à dire aux entreprises ce qu'elles doivent consigner pour chaque courriel. Cette mesure serait excessive pour 99 % des organisations.

M. Frank Baylis: Qu'en est-il des messages électroniques? Vous venez tout juste de donner l'exemple d'un bulletin d'information avec un logo. Lorsqu'on clique sur le logo, on se retrouve ailleurs. Le bulletin n'est pas un message commercial, mais l'hyperlien du logo en est un. Ne pourrions-nous pas mettre de l'ordre dans ce genre de choses?

M. Chris Lewis: Nous avons vu des choses présentées comme étant non commerciales qui finissent par être hautement commerciales, car c'est ce que les organisations tenteront de faire pour s'adresser aux gens.

Une partie du problème attribuable à cette technologie est que les choses sont si compliquées qu'on laisse intentionnellement la loi vague dans certains domaines. À défaut de quoi, on ne tiendrait pas compte de ce qui doit être pris en considération.

M. Frank Baylis: Bien. Merci.

Je vais céder la parole à M. Longfield.

M. Lloyd Longfield: Merci, monsieur Baylis.

J'aimerais approfondir davantage ces questions, mais je veux profiter de la présence de M. Lau qui comparaît par téléphone à partir de Singapour. Merci de rester réveillé aussi tard pour parler avec des Canadiens qui se creusent la tête à propos de cette mesure législative.

Dans son témoignage, un des représentants du gouvernement du Canada a dit que 50 % des courriels envoyés à l'échelle mondiale sont des pourriels, du moins cette année. Interpol fait-il un suivi des courriels transmis à l'échelle mondiale? Savez-vous où les poursuites ont lieu et quels pays sont les principales sources de pourriels? Gardez-vous des dossiers sur ce genre de choses?

M. Louis Lau: Interpol n'a pas d'unités spéciales pour faire ce genre de choses, mais je peux vous donner un exemple de la façon dont des pourriels ont contribué au cybercrime. Plus tôt cette année, nous avons mené une opération dans la région de l'ANASE et nous avons pu trouver environ 8 000 serveurs malveillants avec l'aide d'entreprises privées.

Juste pour vous donner une idée, parmi ces 8 000 serveurs, plus de 7 000 envoyaient des pourriels, tandis que les mille autres serveurs étaient utilisés pour demander des rançons, commettre des fraudes bancaires et ainsi de suite. Dans le domaine du cybercrime, il est très commun que des criminels se servent d'ordinateurs et de serveurs compromis pour envoyer des pourriels.

● (1250)

M. Lloyd Longfield: Merci.

Je crois que je commence à me faire une idée, d'après les témoignages que nous avons entendus. Nous avons une loi, mais il nous faut également des solutions techniques. Nous avons besoin des deux. Nous devons savoir ce que nous essayons de piéger, comment le piéger et comment trouver des solutions techniques pour contrer ces nombreux serveurs qui tentent d'attaquer notre marché.

M. Louis Lau: Je suis tout à fait d'accord.

En fait, la méthodologie et les techniques employées pour utiliser ces 7 000 serveurs dans le but d'envoyer des pourriels étaient très compliquées. Ils fonctionnent automatiquement, et je conviens donc comme vous que nous avons besoin d'un certain soutien technique.

M. Lloyd Longfield: Merci beaucoup.

Je vais céder mon temps à M. Sheehan.

Le président: Vous avez environ une minute.

M. Terry Sheehan: Merci.

Je vais me contenter de poursuivre auprès de Louis.

Les États-Unis, la Nouvelle-Zélande, l'Australie, l'Union européenne et le Royaume-Uni ont tous une loi anti-pourriel. Pouvez-vous nous dire quel pays selon vous à la loi la plus efficace? Il s'agit peut-être d'un pays que je n'ai pas nommé.

M. Louis Lau: Je suis désolé, mais je ne suis pas vraiment en mesure de me prononcer professionnellement, car je n'ai pas consacré beaucoup de temps à l'étude des lois d'autres pays. Si c'est vraiment nécessaire, nous pouvons vous revenir là-dessus plus tard.

M. Terry Sheehan: Nous vous en serions reconnaissants.

M. Louis Lau: Nous avons un certain nombre d'études.

M. Terry Sheehan: Bien.

Merci beaucoup.

Le président: Sur ce, monsieur Lau, nous allons vous laisser dormir, à moins que vous ne vous apprêtiez à patrouiller dans les rues de Singapour.

Je remercie tous les témoins de leur présence. Il y a manifestement beaucoup de matière à réflexion. Je crois que nous avons une tâche à accomplir. Merci beaucoup d'avoir témoigné.

Je vais juste rappeler aux membres du Comité que nous allons entendre les représentants du CRTC pendant la première heure de la séance de jeudi. Nous discuterons ensuite de la propriété intellectuelle au cours de la deuxième heure. Je crois que vous avez tous reçu une copie de l'ébauche n^{o} 3. Vous pouvez vous attendre à recevoir les recommandations traduites révisées aujourd'hui ou demain. Espérons que nous pourrons alors régler la question tout de suite. Ce serait formidable.

Nous pouvons partir quelques minutes plus tôt.

Bonne journée.

La séance est levée.