CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 165 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mercredi 29 mai 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le mercredi 29 mai 2019

● (1615)

[*Français*]

Le vice-président (M. Matthew Dubé (Beloeil—Chambly, NPD)): Bonjour à tous. Nous allons commencer la réunion, maintenant que nous avons enfin des représentants et du gouvernement et de l'opposition.

Avant de passer la parole à notre témoin, qui va se joindre à nous par vidéoconférence, je voulais prendre un moment pour discuter du déroulement de la séance.

Compte tenu du fait que nous avons perdu du temps ainsi que de l'incertitude relative à l'horaire de cet après-midi en raison, notamment, de la possibilité qu'il y ait d'autres votes suivant les tractations procédurales à la Chambre, j'aimerais faire une suggestion.

[*Traduction*]

Ce que je suggère, compte tenu du fait que nous avons encore du temps pour accommoder M. Amos au cours des séances restantes, et compte tenu de l'incertitude... Il est député et il se trouve souvent ici, alors il est plus facile de reporter son témoignage. Nous pourrions entendre le témoin, le questionner, puis, selon le temps qu'il nous reste, passer à autre chose et reporter le témoignage de M. Amos à un autre jour.

[*Français*]

J'aimerais avoir l'avis des membres du Comité.

Nous allons commencer par M. Graham.

M. David de Burgh Graham (Laurentides—Labelle, Lib.): M. Amos a l'intention de venir à la réunion de toute façon. Il s'est organisé pour se faire remplacer dans ses fonctions afin d'y être.

Je suggère que nous fassions tout le travail qu'il nous est possible de faire jusqu'à ce qu'il n'y ait plus de questions. S'il n'y a pas de vote à la Chambre, nous pourrions recevoir le représentant de PayPal pendant une période de 45 à 60 minutes, en fonction du nombre de questions, puis nous donnerions le temps à M. Amos de faire sa présentation à la fin.

Le vice-président (M. Matthew Dubé): C'est une possibilité, mais le problème — et c'est ce qui me préoccupe —, c'est que M. Amos est le parrain de la motion. Il est possible que nous n'ayons aucune occasion de l'interroger s'il est près de 17 h 30 ou si les cloches sonnent pour nous appeler à aller voter.

Le greffier m'informe que cela aurait peu de conséquences sur notre horaire au cours des prochaines semaines jusqu'à la fin de la session.

Très sincèrement, c'est mon opinion personnelle. Je remplace M. McKay, mais je ne veux pas imposer mon point de vue. N'empêche que nous risquons de ne pas pouvoir faire avancer de façon substantielle l'étude demandée dans la motion de M. Amos, en raison du nombre de jours qui nous restent.

Je suis tout de même ouvert à votre suggestion, monsieur Graham.

Monsieur Paul-Hus, qu'en pensez-vous?

M. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, PCC): Je suis d'accord avec vous, monsieur le président.

Écoutons la présentation de M. Johnson, de PayPal, qui attend depuis une heure. Donnons-nous du temps pour poser correctement nos questions et mettons fin ensuite à la séance.

Nous pourrons accueillir M. Amos une autre fois.

Le vice-président (M. Matthew Dubé): Avez-vous des objections importantes à ce que nous procédions de cette façon?

Je ne crois pas qu'il soit nécessaire de faire autrement.

M. David de Burgh Graham: Cela dépend du moment où nous serons en mesure d'y revenir.

Une motion a été adoptée à l'unanimité à la Chambre nous recommandant de faire cette étude. Je veux m'assurer que nous allons nous pencher là-dessus le plus vite possible. Il ne faudrait pas que cela traîne pendant un autre mois. Nous avons déjà a perdu la journée d'aujourd'hui.

C'est pourquoi je suggère que M. Amos fasse la présentation de sa motion. Comme cela, nous nous engagerions dans l'étude.

Le vice-président (M. Matthew Dubé): Encore une fois, le greffier m'a informé du fait qu'il n'y avait aucun problème en ce qui a trait à l'horaire. J'ai validé l'information. Cela peut suffire à vous rassurer, monsieur Graham, en ce qui concerne notre capacité d'accueillir M. Amos à un autre moment. Comme l'a dit M. Paul-Hus, nous avons déjà fait attendre le témoin.

Nous disposons d'une heure et quart, mais, même si le témoignage de ce témoin ne prend que 45 minutes et que M. Amos comparaît par la suite, il est possible que nous manquions de temps ou que nous soyons appelés à aller voter. Je préfère donc ne pas vivre avec cette incertitude, surtout considérant la facilité avec laquelle nous pouvons inviter un député à une autre séance. Cela est rarement possible dans le cas d'autres témoins.

Nous allons donc poursuivre la séance.

● (1620)

M. David de Burgh Graham: D'accord.

Commençons, ne perdons pas plus de temps.

[*Traduction*]

Le vice-président (M. Matthew Dubé): Merci, chers collègues.

Je cède maintenant la parole à notre témoin. Je tiens à remercier M. Johnson de sa patience. Les querelles de procédures qui ont lieu à la Chambre ont parfois cet effet. Nous accueillons par vidéoconférence M. Brian Johnson, directeur principal de la sécurité de l'information à PayPal.

Monsieur Johnson, vous avez 10 minutes pour votre déclaration liminaire. Nous passerons ensuite aux questions des députés. Nous vous remercions d'avoir pris le temps d'être avec nous cet après-midi.

M. Brian Johnson (directeur principal, Sécurité de l'information, PayPal, Inc.): Merci beaucoup. Bonjour, monsieur le président, et mesdames et messieurs les membres du Comité.

Encore une fois, je m'appelle Brian Johnson et je suis directeur principal de la sécurité de l'information à PayPal. Je vous suis reconnaissant de nous donner l'occasion de vous parler aujourd'hui et de prendre le temps malgré votre horaire chargé.

Je soupçonne que vous connaissez tous un peu PayPal en général, mais permettez-moi d'ajouter quelques détails.

Fondée en 1998, PayPal est une société de premier plan dans le domaine des plateformes technologiques qui facilitent les paiements numériques et mobiles pour le compte de plus de 277 millions de consommateurs et de commerçants dans plus de 200 marchés dans le monde. Nous offrons des services d'acquisition et de transfert d'argent en ligne et mobile pour les commerçants. PayPal est le portefeuille numérique le plus populaire au Canada.

Nous sommes basés à San Jose, en Californie, et notre siège social canadien est à Toronto, avec des bureaux à Vancouver. PayPal Canada a été incorporée en 2006. Nous comptons plus de 7,1 millions de clients, dont plus de 250 000 petites entreprises au Canada.

Animée par la conviction fondamentale que l'accès aux services financiers crée des possibilités, PayPal s'engage à démocratiser les services financiers et à donner aux personnes et aux entreprises les moyens de s'intégrer et de prospérer dans l'économie mondiale. Notre plateforme ouverte de paiements numériques donne aux 277 millions de titulaires de comptes actifs de PayPal la confiance nécessaire pour se connecter et effectuer des transactions d'une manière nouvelle et puissante, qu'ils soient en ligne ou sur un appareil mobile. Grâce à une combinaison d'innovations technologiques et de partenariats stratégiques, PayPal crée de meilleures façons de gérer et de transférer de l'argent et offre choix et flexibilité lors de l'envoi de paiements, de paiement ou d'encaissement.

Nous croyons que le moment est venu de réimaginer l'argent et de démocratiser les services financiers afin que la gestion et le transfert d'argent soient un droit pour tous les citoyens, pas seulement pour les riches. Nous croyons que chaque personne a le droit de participer pleinement à l'économie mondiale. Nous avons l'obligation de donner aux gens les moyens d'exercer ce droit et d'améliorer leur santé financière. En tant que pionnier de la technologie financière et chef de file établi, nous croyons en la fourniture de services financiers et de paiements numériques simples, abordables, sûrs et fiables qui permettent à des millions de personnes dans le monde de réaliser leurs espoirs, leurs rêves et leurs ambitions. Nous avons l'engagement fondamental de placer nos clients au centre de tout ce que nous faisons.

Sécuriser nos clients et leurs données sont au cœur de notre mission. Pour les sociétés financières, la sécurité des données est le pilier principal. Grâce à des partenariats solides, des investissements stratégiques et un engagement inlassable à protéger les consommateurs, PayPal s'est promis d'être un chef de file de l'industrie en matière de cybersécurité et de contribuer à rendre Internet plus sûr.

Nous avons en notre faveur plus de 20 ans d'expérience dans le traitement sécurisé des transactions électroniques. PayPal possède l'un des moteurs de prévention de la fraude les plus sophistiqués au monde, qui devient plus intelligent à chaque transaction qui passe par notre système. Grâce à notre technologie avancée de surveillance de la fraude, nous détectons et prévenons les attaques avant qu'elles ne se produisent.

La sécurité est dans notre ADN, et c'est l'épicentre de tout ce que nous faisons à PayPal. Nous sommes la première marque de confiance en matière de commerce électronique et de commerce mobile dans le monde. Les gens font confiance à PayPal parce qu'ils savent que nous ne communiquons pas les informations financières des clients aux commerçants, aux détaillants ou aux vendeurs en ligne. Nos normes de sécurité rigoureuses garantissent que chaque partie d'une transaction est sûre et sécurisée.

À PayPal, nous croyons que nous avons la responsabilité d'aider à protéger nos utilisateurs contre les méfaits. La protection de la vie privée a toujours été l'une de nos principales préoccupations. Nos clients nous confient leurs données. Nous prenons cette confiance très au sérieux. Nous ne recueillons que les données nécessaires à l'exécution des services demandés par un client, à l'amélioration de l'expérience des produits et à la diffusion de publicité PayPal pertinente et à la prévention de la fraude. Nous ne vendons ni ne louons jamais d'information sur nos clients.

Il est communément admis par les organismes mondiaux d'application de la loi que la cybercriminalité et les méthodes de fraude en ligne sont maintenant plus courantes que les crimes commis dans le monde physique et hors ligne. Comme le Comité le sait certainement, au cours des cinq dernières années, la GRC à elle seule a observé une augmentation de près de 50 % des signalements de cybercriminalité par les Canadiens. Je félicite le Comité d'avoir pris des mesures énergiques et d'avoir appuyé la stratégie de sécurité nationale du Canada, en prévoyant des fonds importants pour investir dans la cybersécurité dans le cadre de votre engagement à l'égard de la sûreté et la sécurité. La création d'un cyberécosystème novateur et adaptatif est une étape cruciale pour être en mesure d'évaluer et de combattre rapidement les nouvelles menaces qui pèsent sur les infrastructures essentielles, le gouvernement, les entreprises et l'information numérique des particuliers.

En conclusion, j'aimerais souligner l'engagement de PayPal à l'égard de la cybersécurité et notre volonté de collaborer avec le gouvernement et l'industrie canadienne.

Merci encore de m'avoir invité à discuter de ces sujets très pertinents et de présenter la position ferme de PayPal en faveur de la protection des données et de la vie privée des consommateurs.

● (1625)

Je serai heureux de répondre à vos questions.

Le vice-président (M. Matthew Dubé): Super. Merci beaucoup, monsieur Johnson.

Nous allons passer aux questions. Nous allons commencer par Mme Sahota. Vous avez sept minutes.

Mme Ruby Sahota (Brampton-Nord, Lib.): Merci, monsieur Johnson, d'être parmi nous aujourd'hui.

Y a-t-il des différences dans votre façon de fonctionner au Canada par rapport aux États-Unis, ou êtes-vous principalement basé aux États-Unis et c'est là que toute l'information se retrouve lorsque les Canadiens utilisent votre service?

M. Brian Johnson: [*Inaudible*] les clients de PayPal sont stockés dans des centres de données américains et dans des centres d'hébergement de données localisés, de sorte que les données des clients canadiens sont également localisées dans les installations hébergées aux États-Unis.

Mme Ruby Sahota: Pour plus de précision, il n'y a pas de différence dans la façon dont vous fonctionnez quand il s'agit de clients canadiens par rapport aux clients américains, n'est-ce pas?

M. Brian Johnson: Outre la localisation pour la devise ou d'autres préférences localisées, les données et les informations sont stockées de la même manière que celles des clients basés aux États-Unis.

Mme Ruby Sahota: Je suis très heureuse d'entendre cela, parce que je me disais qu'après deux décennies d'exploitation — plus longtemps que d'autres concurrents dans ce domaine — vous devez avoir beaucoup de données en mémoire. Il est bon d'entendre que vous ne vendez pas les données que vous avez reçues. Merci de nous avoir fourni cette information.

Toutefois, j'ai vu qu'il y a eu plusieurs articles sur PayPal au cours des derniers mois. L'un portait sur les pirates informatiques — je suppose qu'il s'agit de pirates éthiques — payés pour essayer de protéger la sécurité de votre système. Pourrais-je en savoir un peu plus à ce sujet, et comment cela fonctionne-t-il? Faites-vous cela depuis longtemps? Le paiement de pirates pour pirater votre système est-il une tendance récente? Quels avantages en tirez-vous?

M. Brian Johnson: C'est une excellente question, madame Sahota.

Notre programme s'appelle Bug Bounty, et c'est une méthode acceptée à l'échelle de l'industrie qui consiste à utiliser des contractuels, essentiellement des chapeaux blancs dans le cadre d'un programme géré. Les chapeaux blancs sont contrôlés pour éviter qu'ils agissent de façon indésirable ou qu'ils attaquent des systèmes sans que la demande n'ait été faite et sans que les responsables ne soient mis au courant. Ces personnes sont considérées comme des chercheurs professionnels en sécurité dans toute l'industrie, et bon nombre d'entre eux sont spécialisés dans d'autres domaines et utilisent leur temps libre pour travailler à la pige ou à des emplois secondaires pour fournir ce qu'on appelle le piratage éthique de la chasse aux bogues. Cela nous aide à exposer des problèmes ou des vulnérabilités dans les systèmes qui ne sont pas détectés par des outils internes mais qui sont recensés grâce aux programmes de chasse aux bogues, qui, encore une fois, sont couramment utilisés par de nombreuses entreprises pour que la communauté des chercheurs en sécurité puisse collaborer avec nous sur ces vulnérabilités.

Mme Ruby Sahota: Avez-vous des contrats avec ces pirates?

M. Brian Johnson: Nous établissons des contrats avec un groupe qui s'appelle Hackerone, lequel offre un service de filtrage et, grâce à la divulgation responsable, les vulnérabilités nous sont signalées afin que nous puissions y remédier avant qu'elles ne soient rendues publiques, ainsi nous réglons les vulnérabilités qu'ils nous présentent.

Mme Ruby Sahota: Advenant que quelqu'un viole le système ou la vie privée de quelqu'un, qui serait responsable? Est-ce que PayPal en assumerait la responsabilité?

M. Brian Johnson: S'il y avait une brèche dans le système, cela dénoterait une activité non autorisée et serait traitée comme un accès malveillant et illégitime comme pour tout autre cas de piratage mal intentionné. Nous ne demandons pas aux chapeaux blancs qui font la chasse aux bogues de mener des attaques ou des violations de système, et dans le cadre de notre politique, ils n'ont pas le droit d'accéder aux données des clients ni de faire des manipulations ou d'apporter des changements à l'information. Ces chercheurs peuvent divulguer les vulnérabilités qu'ils détectent dans le système et nous en faire rapport grâce au programme de divulgation responsable.

Mme Ruby Sahota: PayPal utilise également une application pour faciliter la tâche des clients, est-ce exact?

● (1630)

M. Brian Johnson: Une application pour des raisons de commodité? Nous avons en fait une application mobile.

Mme Ruby Sahota: Une application mobile, oui c'est exact.

M. Brian Johnson: Effectivement, nous offrons des applications mobiles.

Mme Ruby Sahota: J'ai également vu des articles tout récemment, ce mois-ci, à propos de gens dont les comptes en banque avaient fait l'objet de fraudes allant jusqu'à 9 000 $, et cela s'est produit parce que les applications peuvent être piratées. Par conséquent, la vulnérabilité de l'application permet aux pirates d'accéder directement aux comptes de banque des clients.

Des compagnies de cartes de crédit nous ont dit que cette information n'est jamais divulguée directement. Les renseignements bancaires ne sont jamais directement divulgués aux compagnies de cartes de crédit, mais il semblerait que, dans ce cas-ci, l'information bancaire est communiquée directement à PayPal, de sorte que s'il y a une vulnérabilité dans le système, les pirates peuvent accéder à toute l'information.

Que faites-vous pour vous protéger contre ces violations?

M. Brian Johnson: Les articles médiatiques ne sont pas toujours exacts. Pour être techniquement exact, l'accès à l'information des comptes PayPal ne peut se faire que par l'entremise d'un détenteur de compte autorisé ou lorsque les gens perdent leurs pièces d'identité ou leur appareil. Si un client perd ses pièces d'identité — disons qu'un maliciel se trouve sur leur ordinateur et que leurs identifiants de connexion sont volés ou perdus — l'accès à leur compte lors d'une tentative de piratage serait intercepté par notre plateforme antifraude ou notre système de détection des risques. Si une vulnérabilité quelconque ne permet pas de déceler la fraude, le seul accès dans le compte PayPal pourrait se faire par le solde PayPal, mais le pirate n'aurait pas directement accès à l'information bancaire du client. L'information bancaire est stockée dans nos systèmes et n'est pas rendue visible, même après avoir été entrée dans le système par le client.

Tout ce que le pirate pourrait faire, c'est d'essayer d'extraire des données en utilisant le système PayPal pour procéder à des transactions. Le pirate pourrait essayer de commettre des fraudes, mais il ne serait pas en mesure d'obtenir de l'information sur un compte de banque par l'entremise de cette plateforme.

Mme Ruby Sahota: C'est intéressant. L'article conseille aux gens de vérifier régulièrement leurs comptes bancaires et d'examiner les transactions PayPal pour déceler celles qui n'auraient pas été autorisées.

Lorsque cela se produit, vers qui peut se tourner le client? Doit-il demander d'être remboursé auprès de sa banque? Ou bien est-il remboursé par PayPal?

M. Brian Johnson: Nous offrons de la protection aux acheteurs de sorte que s'il y a des transactions malveillantes ou non voulues à partir du compte d'un consommateur, nous offrons une protection à l'acheteur en matière de responsabilité pour les transactions frauduleuses de manière à protéger le consommateur.

J'aimerais toutefois rappeler qu'un accès malveillant à un compte PayPal est tout à fait différent d'un accès malveillant dans un autre compte. Si une fraude en ligne a lieu, nous assumons la responsabilité pour l'acheteur, pour le consommateur, dans ce cas. La protection que nous offrons au vendeur comprend d'autres types de couvertures pour les marchands qui vendent en passant par nous. Le fait d'avoir accès au compte PayPal ne signifie pas que le pirate aura nécessairement accès directement au compte de banque. Les pirates n'ont pas accès aux identifiants ni à l'information du compte bancaire, ils ont uniquement accès aux liens que nous fournissons pour le compte de banque à titre d'instrument de financement pour le compte PayPal.

Mme Ruby Sahota: Très bien.

Je me suis servie de PayPal il y a de nombreuses années, mais j'ai arrêté de m'en servir après un moment, car je recevais continuellement des courriels frauduleux m'avisant de certaines transactions qui auraient été faites. J'ai une dernière observation; ces courriels peuvent prêter à confusion pour l'utilisateur. C'est pour cette raison que j'ai cessé d'utiliser le service, parce que je trouvais que je recevais trop de courriels frauduleux soi-disant en provenance de PayPayl.

Le vice-président (M. Matthew Dubé): Malheureusement, nous allons devoir nous arrêter là.

[*Français*]

Nous cédons la parole à M. Paul-Hus pour sept minutes.

M. Pierre Paul-Hus: Merci, monsieur le président.

Voici ma première question.

Monsieur Johnson, vous avez mentionné que PayPal était une organisation qui existait depuis 1998. Vous êtes donc présents depuis les débuts d'Internet.

On sait que les problèmes de cybersécurité sont venus avec l'évolution d'Internet. L'entreprise PayPal est-elle en mesure de suivre cette évolution et de s'ajuster afin de contrer les menaces?

[*Traduction*]

M. Brian Johnson: Un grand nombre de nos employés qui s'occupent de la sécurité de l'information sont membres d'alliances sectorielles qui travaillent sur le renforcement de la sécurité Internet. Nous procédons à de nombreux investissements et nous en sommes à l'étape de la recherche et du développement. Le hameçonnage et l'anti-hameçonnage sont d'autres domaines de travail également, comme l'a dit Mme Sahota. Certains de nos plus importants investissements se font dans le domaine de la sécurité des courriels, la sécurité d'Internet et la sécurité des fureteurs.

● (1635)

[*Français*]

M. Pierre Paul-Hus: Vous avez également mentionné que les gens faisaient confiance à PayPal.

Quels moyens prenez-vous pour faire en sorte que les gens qui font affaire avec PayPal lui fassent pleinement confiance?

[*Traduction*]

M. Brian Johnson: Comme je l'ai dit, nos programmes de protection du consommateur incluent une protection contre toute fraude impliquant un compte client. Nous investissons aussi énormément dans des initiatives de cybersécurité et nos plateformes antifraude et de détection des risques. Nous avons des indicateurs de premier plan dans l'industrie qui montrent que notre taux de fraude est très faible, c'est-à-dire que nous offrons une bonne protection et évitons un grand nombre de fraudes, et notre indice de protection des marchands et des consommateurs utilisant notre plateforme est très élevé, ce dont nous sommes très fiers.

[*Français*]

M. Pierre Paul-Hus: Excellent.

Parmi les témoins que nous avons rencontrés lors de notre étude, il y a eu les représentants de différentes banques, dont la Banque Toronto-Dominion. L'un de ses représentants nous a dit que la banque subissait des cyberattaques provenant de différents pays.

Êtes-vous en mesure de nommer les pays qui attaquent le système de PayPal?

[*Traduction*]

M. Brian Johnson: Je ne suis pas en mesure de divulguer d'information sur les pays étrangers — vous avez parlé de nations-États —, mais les attaques par des particuliers en ligne contre des sites Web sont très fréquentes. Ces fraudeurs ne sont pas concentrés dans une région géographique particulière. Bien entendu, une forte proportion des cyberattaques sont difficiles à attribuer à un pays en particulier, puisque l'origine de ces cyberattaques est difficile à retracer. En effet, un grand nombre de pays participant à l'infrastructure permettent qu'elle soit piratée. Par exemple, le pirate peut se trouver dans un pays, mais utiliser les services Internet d'un autre pays pour mener son attaque. Les criminels exploitent une économie à multiples niveaux, et diverses parties y sont impliquées dans diverses régions.

[*Français*]

M. Pierre Paul-Hus: Je comprends la nuance entre le pays d'origine d'un individu et le pays à partir duquel provient une attaque, mais ma question visait plus l'État que l'individu. Est-ce que PayPal subit des attaques provenant d'États?

[*Traduction*]

M. Brian Johnson: Pas particulièrement. Nous ne connaissons pas de concentration de pays qui nous attaquent comme entreprise uniquement.

[*Français*]

M. Pierre Paul-Hus: D'accord, c'est parfait.

Votre entreprise se trouve aux États-Unis et elle fait affaire dans plusieurs pays qui ont chacun une réglementation différente. Puisque nous étudions la perspective canadienne, est-ce que la réglementation ou les lois canadiennes ont une incidence sur les activités de PayPal? Est-ce que nos lois sont trop ou pas assez restrictives en matière de protection de la vie privée, par exemple?

[*Traduction*]

M. Brian Johnson: C'est une excellente question. Les effets sur la protection des données et la protection des renseignements personnels de ce que le Canada propose et qu'il a défini comme cadre constituent un excellent soutien pour l'industrie et les entreprises du monde entier.

Pour répondre à la première partie de votre question au sujet de nos activités à l'échelle mondiale, nous avons du personnel dans bon nombre de régions qui ont resserré la réglementation. Nous sommes présents dans de nombreux pays, y compris en Europe, où nous avons du personnel de soutien pour le Règlement général sur la protection des données, et dans la région de Singapour, où nous avons du personnel de soutien pour nos activités dans la région Asie-Pacifique. Nous disposons de personnel et d'un soutien local pour chacune de ces régions, ainsi que dans d'autres régions du monde pour ce qui concerne la réglementation locale. Nous avons une main-d'œuvre mondiale, nous avons des effectifs partout dans le monde qui encouragent la participation avec les législateurs et les organismes de réglementation locaux. Nous travaillons en étroite collaboration avec les examinateurs et les organismes de réglementation lorsqu'il existe des lois sur la protection des données et la protection des renseignements personnels, afin de nous assurer non seulement de les appliquer et de nous y adapter, mais aussi de bien nous conformer aux règlements qui évoluent et de guider leurs applications pratiques dans un contexte qui convient à une économie mondiale.

[*Français*]

M. Pierre Paul-Hus: Selon vous, est-ce qu'il y a des éléments que le Canada devrait améliorer? Vous avez dit que notre pays avait des lois fortes, mais avez-vous quand même des recommandations à nous faire sur le plan législatif?

● (1640)

[*Traduction*]

M. Brian Johnson: Soit dit en passant, à propos de l'annonce de la nouvelle charte numérique, PayPal tient à féliciter le ministre Bains et le gouvernement du Canada d'avoir pris les devants dans ce dossier important qu'est la protection des données. Nous croyons que cette responsabilité nous aide à protéger les utilisateurs contre les menaces ou préjudices et à soutenir les lois sur la protection de la vie privée. C'est un bon premier pas. Cela repose sur certains principes. Je crois que le 10e principe, ou tout du moins le dernier, était celui de la reddition de comptes et de l'application de la loi. Il serait utile d'avoir plus de détails à ce sujet.

Le Canada a bénéficié du fait de ne pas avoir été le premier pays à adopter une loi sur la protection des renseignements personnels et il a pu ainsi apprendre des autres régions et organismes de réglementation et voir qu'il existe un juste équilibre en matière de protection des renseignements personnels. Mais en ce qui concerne précisément la protection des renseignements numériques et les règlements que vous encouragez les entreprises à adopter, il faudra établir un équilibre délicat entre le cadre que vous avez élaboré et les principes directeurs qui aideront à orienter la bonne conduite et un bon régime de reddition de comptes. De plus, il faut travailler avec l'industrie et des partenaires privés pour pouvoir élaborer des lois solides que vous pourrez appuyer dans les années à venir.

[*Français*]

Le vice-président (M. Matthew Dubé): Merci beaucoup.

Nous passons maintenant la parole à M. Picard pour sept minutes.

M. Michel Picard (Montarville, Lib.): Monsieur le président, normalement, vous auriez vous aussi droit à un temps de parole de sept minutes.

Dans les circonstances, je propose d'allouer sept minutes au président pour qu'il puisse poser ses questions au nom de son parti.

Le vice-président (M. Matthew Dubé): Vous êtes très généreux, merci.

[*Traduction*]

M. Michel Picard: Je ne le ferai plus.

Monsieur, j'aimerais examiner vos activités du point de vue du blanchiment d'argent. Lorsque j'achète des crédits ou que je mets de l'argent dans mon compte, ma première question naïve est: où va mon argent?

M. Brian Johnson: Où va votre argent dans le système de soldes PayPal?

M. Michel Picard: Oui.

M. Brian Johnson: Les soldes PayPal sont garantis par un certain nombre de banques américaines, de sorte que nous permettons le dépôt et le placement en toute sécurité, ainsi que le dépôt de l'argent dans le compte. Le premier élément concernait l'utilisation des crédits. Est-ce que c'était un commentaire d'appui, ou quelle était votre idée avant que je vous réponde?

M. Michel Picard: Lorsque j'achète un certain nombre de crédits... et que je mets de l'argent dans mon compte pour d'autres achats, mon argent se retrouve dans une banque qui garantit votre transaction. Admettons que j'ai 100 $ dans n'importe quelle devise, ou cela pourrait être simplement des dollars, et que je veuille acheter quelque chose. Retracez-vous l'origine de la transaction pour voir d'où elle vient, s'il s'agit d'une carte de crédit, d'un compte bancaire ou d'une autre chose de ce genre?

M. Brian Johnson: Oui, je suis désolé. Je comprends maintenant votre question, monsieur Picard.

Oui. L'origine de l'argent... Du point de vue de la lutte contre le blanchiment d'argent, nous avons un service de lutte contre le blanchiment d'argent et nous avons beaucoup investi dans la détection de ce genre d'activité. Nous prenons cela très au sérieux et retraçons tout le circuit que suit l'argent, depuis son origine, sa source de financement ainsi que la méthode de dépôt originale, et nous appuyons les efforts des forces de l'ordre dans la lutte contre toute opération de blanchiment d'argent ou de fraude qui serait détectée ou déclarée sur la plateforme.

M. Michel Picard: Vous appuyez les efforts déployés pendant l'enquête, mais lorsque vous obtenez l'argent de quelque carte de crédit que ce soit, à votre niveau, je suppose que vous acceptez la transaction tant qu'il y a suffisamment d'argent à la source. Cela signifie que si j'ai, par exemple, une carte de crédit prépayée, et que je veux mettre de l'argent dans mon solde, j'utilise ma carte de crédit, vous vérifiez le solde, l'argent est là, vous le prenez, et il n'y a plus d'enquête, peu importe son origine. Que cette origine soit criminelle ou non, vous ne pouvez pas le vérifier.

M. Brian Johnson: Nous validons effectivement la source de données ou la source de l'argent à son origine, et dans certaines circonstances, les cartes prépayées ont des limites quant au montant d'argent que nous autorisons à déposer, au montant d'argent qui peut être retiré dans une période de temps donné ou encore au montant qui peut être dépensé sur certains sites Web. Les plateformes antifraude et de détection des risques sont assorties de règles très granulaires qui détectent certains instruments financiers utilisés en fonction du niveau de risque. S'il existe une méthode de lutte contre le blanchiment d'argent ou une méthode de blanchiment d'argent que nous avons inscrite dans nos modèles de fraude pour ce cas d'utilisation, comme le prépayé, par exemple, nous imposons des limites et certains critères pour limiter les pertes et minimiser les risques dans ce cas-là.

● (1645)

M. Michel Picard: Avez-vous une analyse de modèles pour les types de transactions?

M. Brian Johnson: Oui. Nous effectuons des analyses comportementales et nous disposons de certaines méthodes d'intelligence artificielle qui sont intégrées à nos plateformes de détection des risques. Il s'agit d'un modèle d'apprentissage et de comparaison de comportement et des habitudes de paiement à l'échelle de la plateforme.

M. Michel Picard: Habituellement, lorsque j'ai de l'argent dans mon compte, je ne peux pas retirer de l'argent tel quel. Je dois acheter quelque chose. Est-ce le cas, ou y a-t-il des exceptions qui me permettent de retirer de l'argent de mon solde?

M. Brian Johnson: Nous offrons des méthodes de retrait d'argent dans certaines régions du monde, selon l'endroit d'où vient l'argent, bien entendu. Il peut être retiré de différentes façons. Nous avons un partenariat, par exemple, avec Walmart qui permet le retrait d'argent comptant. Avec Walgreens et les détaillants locaux, nous avons établi des partenariats qui permettent le dépôt et le retrait d'espèces en monnaie locale. Grâce à notre intégration à la plateforme Zoom, nous permettons également le transfert international de fonds ou le transfert transfrontalier de différentes transactions et le retrait d'argent chez les détaillants, et ce, de différentes façons. L'argent peut également être déposé ou retiré en espèces au moyen de certaines méthodes.

M. Michel Picard: Quel est le montant maximal d'argent qui peut être déposé dans mon solde en une seule transaction?

M. Brian Johnson: Je crois que cela dépend des règles de risque. Ce n'est pas mon domaine d'expertise, donc je ne connais pas tous les détails, mais il y a des limites selon l'ancienneté du compte, et d'autres limites, à savoir si votre compte a été vérifié avec identification et si nous avons vérifié l'historique du titulaire du compte. Il existe d'autres méthodes qui nous permettent d'augmenter cette limite. Nous nous fondons sur les indicateurs de savoir et de connaissance du client qui nous permettent d'établir un lien de confiance avec le titulaire de compte.

M. Michel Picard: Avez-vous l'obligation de déclarer au CANAFE au Canada s'il y a des transactions ou des dépôts de plus de 10 000 $?

M. Brian Johnson: Je n'en suis pas certain. Je ne travaille pas dans le domaine de la fraude ou de la lutte contre le blanchiment d'argent, mais je sais que nous faisons rapport concernant certains critères par l'intermédiaire du FinCEN et d'autres réseaux aux États-Unis, des réseaux que je connais. Toutefois, je ne connais pas notre façon de signaler les fraudes au Canada. Je peux certainement me renseigner à ce sujet.

M. Michel Picard: Si je mets de l'argent dans mon propre compte pour que je puisse moi-même retirer mon argent, vous ne pouvez pas savoir si je suis la même personne qui effectue les deux transactions... Si, par exemple, je prends une carte prépayée, ou que mon argent est dans un compte de banque, toujours à la même banque, et que cette banque est soupçonnée, puisque c'est le cas pour certaines banques.

M. Brian Johnson: D'accord.

M. Michel Picard: Je mets de l'argent sur mon compte PayPal. Deux ou trois jours plus tard, je retire mon argent. La seule chose que vous devez savoir pour effectuer cette transaction est si le compte a été ouvert avec le bon nom d'utilisateur et le bon mot de passe, idem pour le retrait d'argent. Il n'y a donc rien qui vous permette de vérifier si c'est la même personne qui effectue les deux transactions. Mon collègue et moi pourrions utiliser le même compte.

M. Brian Johnson: Nous vérifions la télémétrie de l'appareil. Nous recueillons des renseignements sur l'appareil, l'ordinateur que vous utilisez. Nous appuyons sur la géolocalisation et sur d'autres modèles de détection des fraudes pour tenter de vérifier l'authenticité de l'utilisation du compte. Le titulaire du compte, bien sûr, doit avoir le justificatif d'identité nécessaire pour effectuer ce paiement ou cette transaction.

M. Michel Picard: Il ne me reste pas beaucoup de temps de parole. J'ai une question portant sur la nature des attaques que vous ciblez.

Quel progrès avez-vous remarqué au fil du temps quant à la complexité de ces attaques? Pouvez-vous nous en parler?

M. Brian Johnson: De manière générale, l'empreinte des cyberattaques est devenue beaucoup plus complexe et à la fine pointe de la technologie. Les cybercriminels représentent une économie à part entière et ont superposé leurs outils, leurs données et leurs méthodes d'attaque de façon très sophistiquée, et dans bien des cas, très coordonnée.

Les criminels créent des outils, puis ils les utilisent ou en louent l'accès. Les attaques par déni de services distribués, ou attaques DDOS, sont devenues plus importantes et avancées au fil du temps. Le paysage cybernétique des menaces et les tendances émergentes dans ce domaine sont certainement devenus plus complexes et se sont considérablement élargis au cours des dernières années.

M. Michel Picard: Merci.

Le vice-président (M. Matthew Dubé): Chers collègues, comme vous pouvez le constater, les cloches sonnent. Nous avons besoin du consentement unanime du Comité pour poursuivre la séance. Le cas échéant, nous devons également nous entendre sur la durée du reste de la séance. Nous pourrons prendre cette décision à la lumière du nombre de questions qu'il vous reste à poser à notre témoin.

Monsieur Graham.

M. David de Burgh Graham: Je propose de rester jusqu'à ce que les cloches sonnent trois fois d'affilée. On aurait alors cinq minutes pour monter à l'étage.

Le vice-président (M. Matthew Dubé): Vous proposez donc de prolonger la séance encore 20 minutes?

M. David de Burgh Graham: Oui, encore 22 minutes.

Un député: Cela nous donnera suffisamment de temps?

M. David de Burgh Graham: Cela nous donnera cinq minutes pour monter deux étages dans le même édifice.

Le vice-président (M. Matthew Dubé): Tout le monde est d'accord pour deux tours de questions de cinq minutes pour chacun des partis présents? Cela vous convient?

Des députés: Oui.

Un député: Voulez-vous [*Inaudible*], monsieur le président?

Le président: Cela me convient, merci de votre générosité.

Monsieur Eglinski, vous disposez de cinq minutes.

● (1650)

M. Jim Eglinski (Yellowhead, PCC): J'aimerais d'abord remercier le témoin de sa présence.

Monsieur Johnson, j'aimerais poursuivre dans la même veine d'idée que M. Picard.

Vous nous disiez plus tôt dans votre témoignage que l'argent déposé dans le compte PayPal va aux États-Unis. Est-ce vrai pour tous les pays où vous effectuez des transactions?

M. Brian Johnson: Je n'en suis pas certain, monsieur Eglinski.

Je vais devoir vérifier auprès de notre équipe de production où l'argent est déposé dans des sources finales selon l'endroit.

M. Jim Eglinski: Concentrons-nous sur les clients canadiens.

Est-ce que tous les fonds à partir desquels nous faisons des transactions avec vous vont aux États-Unis, ou est-ce qu'une partie de ces fonds se trouve ici, au Canada?

M. Brian Johnson: Désolé. Je ne suis pas certain des produits qui permettent de stocker des données et renferment des soldes de comptes, ce qui m'empêche de répondre clairement à cette question.

M. Jim Eglinski: D'accord.

Existe-t-il un organisme de réglementation aux États-Unis qui exige que vous signaliez les intrusions dans votre programme? Comme vous l'avez indiqué tout à l'heure à M. Picard, vous avez un programme qui se déclenchera si une transaction est effectuée et qu'une deuxième transaction donne lieu à un retrait d'un emplacement différent.

S'agit-il d'une exigence pour vous? Signalez-vous ces situations à certaines agences de sécurité aux États-Unis ou au Canada?

M. Brian Johnson: Nous avons un certain nombre d'obligations de notification imposées par des organismes de réglementation dans le monde. Encore une fois, ils sont gérés à l'échelon régional au niveau des États, aux États-Unis, et au niveau régional par chacun des organismes de réglementation.

Nous sommes régis par la Commission de surveillance du secteur financier en Europe, qui administre notre permis bancaire européen, et la MAS, ou administration monétaire de Singapour. Nous sommes aussi régis dans un certain nombre d'autres pays où nous exploitons des permis pour des services de remise de fonds et de paiements que nous effectuons aux États-Unis et au Canada.

Les obligations de notification varient selon les situations, mais nous informons les organismes de réglementation des cas d'atteinte à la protection des données pour lesquels le seuil de notification a été franchi, ou de toute opération de blanchiment d'argent ou de fraude que nous pouvons détecter sur la plateforme. Ces cas sont signalés par l'entremise des organismes de réglementation comme on l'exige.

M. Jim Eglinski: Êtes-vous membre de l'Échange canadien de menaces cybernétiques?

M. Brian Johnson: Non, monsieur, ce n'est pas le cas. Nous avons discuté avec ce groupe et notre équipe du renseignement sur les menaces l'a déjà rencontré, mais nous n'en sommes pas membres pour le moment.

M. Jim Eglinski: Y a-t-il une raison à cela?

M. Brian Johnson: Je crois qu'il y avait d'autres canaux qui remplaçaient cela — des plateformes d'échanges de menaces qui ne sont pas expressément régionales. L'Échange canadien de menaces cybernétiques suit en fait certaines des sources d'information sur les menaces dont nous sommes déjà membres. Je crois qu'ils échangent déjà des données sur les menaces par l'entremise d'un certain nombre de plateformes. Nous ne nous y opposons pas, mais, comme nous en avons discuté avec eux, il n'était tout simplement pas nécessaire d'avoir une seule et unique plateforme d'échange de données.

M. Jim Eglinski: D'accord, merci.

Je suis membre de PayPal depuis environ 2000, je crois, et je l'ai utilisé assez souvent au cours des dernières années.

M. Brian Johnson: Merci de faire affaire avec nous.

M. Jim Eglinski: Quelle quantité de mes renseignements personnels ou de ceux d'autres utilisateurs transite par votre service? Où ces renseignements sont-ils stockés? Sont-ils tous stockés aux États-Unis ou dans d'autres pays?

M. Brian Johnson: Tout est stocké aux États-Unis. Les renseignements personnels sont tous chiffrés. Nous disposons de technologies de chiffrement de très haut niveau à tous les échelons de notre infrastructure technologique. Nous ne communiquons aucun renseignement personnel permettant d'identifier une personne. Encore une fois, nous ne vendons ni ne louons ces données à qui que ce soit à des fins de marketing ou à toute autre fin. Ils sont stockés et demeurent dans les systèmes de PayPal aux États-Unis, dans nos centres d'information.

M. Jim Eglinski: Avez-vous été piratés?

M. Brian Johnson: Avons-nous été piratés? Pour répondre directement, nous n'avons pas fait l'objet d'intrusion. Si vous faites référence à une intrusion relative à une situation de PayPal devant être signalée à un client, non. Comme vous le savez peut-être, d'autres sociétés que nous avons acquises au fil des ans ont signalé des incidents cybernétiques. Nous avons mis à jour certaines vulnérabilités, qui pourraient être considérées comme « piratage » dans certains produits servant d'interface, mais rien n'a entraîné d'atteinte massive ou de perte de données suffisamment grave pour qu'elle justifie d'être signalée.

M. Jim Eglinski: Vous avez indiqué que toutes les données sont stockées aux États-Unis. Sont-elles stockées dans un seul centre ou avez-vous quelque chose comme un système de sauvegarde?

● (1655)

M. Brian Johnson: Nous effectuons plusieurs sauvegardes, en effet. Nous sommes géographiquement répartis sur des zones de centres de données à haute disponibilité, afin de maintenir notre résilience et nos capacités de reprise après sinistre sur l'ensemble de la plateforme.

M. Jim Eglinski: D'accord. Merci.

[*Français*]

Le vice-président (M. Matthew Dubé): Merci, monsieur Eglinski.

Nous passons maintenant la parole à M. Graham pour les cinq dernières minutes.

[*Traduction*]

M. David de Burgh Graham: J'ai une question à vous poser sur une note un peu plus légère.

Savez-vous qu'au bas de l'écran, on peut lire l'inscription: « SCF Superman »?

M. Brian Johnson: Oui, en effet. C'est le nom de ma salle de conférence.

Des voix: Oh, oh!

M. David de Burgh Graham: D'accord. Je me posais la question parce qu'il s'agit d'une séance télévisée et que tout le monde peut le voir.

M. Brian Johnson: Oui. C'est une blague, donc pas de problème.

M. David de Burgh Graham: Vous avez indiqué que vous ne faisiez pas le commerce de données. N'y a-t-il donc aucune interaction de quelques données que ce soit, à part les données relatives aux transactions, entre PayPal et d'autres sociétés, pour quelques motifs que ce soit? Cela est-il correct?

M. Brian Johnson: Nous ne vendons ni ne louons de données. Nous employons certaines méthodes de détection de la fraude et autres. Il y a certainement des intégrations avec les commerçants quand nous avons besoin de certains types de données. Nous ne vendons ni ne louons les données de nos clients. L'empreinte des données-clients n'est pas transmise à des tiers à des fins de marketing, sauf si nos clients l'ont acceptée sur la plateforme PayPal.

M. David de Burgh Graham: Outre les données de l'historique de transactions, quelles données PayPal collecte-t-elle auprès de ses propres clients à des fins de marketing?

M. Brian Johnson: Désolé, monsieur Graham, je ne suis pas dans le service marketing et ne suis donc pas certain des éléments de données qu'utilise ce service. Une fois encore, nous ne louons ni ne vendons ces données à l'extérieur de la plateforme. Je ne suis pas certain de ce que nous utilisons à l'intérieur de la plateforme d'un point de vue marketing. Voulez-vous savoir s'ils obtiennent d'autres données, en d'autres termes, ou si d'autres données sont collectées auprès des clients de PayPal?

M. David de Burgh Graham: J'essaie juste d'aller au fond des choses. M. Picard et moi venons tout juste de terminer trois jours de travaux du grand comité sur la protection de la vie privée, et nous avons discuté des avatars créés par les entreprises et de ce genre de choses, alors c'est évidemment frais en mémoire et j'essaie de comprendre le niveau d'information que PayPal a sur ses utilisateurs. Est-ce exact de dire: cette personne a envoyé un certain montant d'argent, et c'est tout ce que nous savons à son sujet, ou y a-t-il beaucoup plus d'information conservée par PayPal sur ses utilisateurs?

M. Brian Johnson: Certes, d'un point de vue financier, et en ce qui concerne certaines des questions précédentes relatives à la détection du blanchiment d'argent et à la prévention de la fraude, nous devons recueillir davantage de données sur les détails des transactions, l'utilisation de la plateforme et les informations relatives aux dispositifs électroniques, afin de nous conformer aux exigences des forces de l'ordre et des régulateurs locaux qui nous obligent à colliger certains renseignements au sujet des clients.

Du point de vue de la connaissance du client, l'historique des transactions et l'utilisation de certains ordinateurs et appareils des clients sont des éléments d'information que nous utilisons pour détecter la fraude. Encore une fois, ils ne sont pas utilisés à des fins de marketing. Nous ne vous commercialiserions pas parce que vous vous êtes connecté avec un certain type d'appareil, si, par exemple, nous utilisons ces renseignements pour prévenir la fraude. Encore une fois, à ma connaissance, l'équipe de marketing n'aurait pas accès à ce genre de renseignement, elle ne pourrait s'en servir en dehors de cette fonction.

M. David de Burgh Graham: Il y a quelques années, beaucoup d'encre a coulé au sujet d'un recours collectif contre PayPal pour avoir accepté des dons à des organismes de bienfaisance qui n'étaient pas membres de PayPal, qui a finalement été soumis à un arbitrage exécutoire. Par hasard, connaissez-vous l'état d'avancement de cette poursuite?

M. Brian Johnson: Non. Je me souviens d'avoir lu à ce sujet, mais je ne me souviens pas de l'état d'avancement de cette poursuite.

M. David de Burgh Graham: Vous ne pouvez donc pas nous dire pourquoi PayPal accepte des dons de clients qui ne sont pas les siens.

M. Brian Johnson: En effet, moi, mon domaine, c'est la cybersécurité.

Si j'ai bien compris, cependant, il s'agissait d'une situation comme celle d'un organisme de charité dont la légitimité est remise en question. Je ne me souviens pas si c'était bien là la question, parce que cela ne relève pas de moi.

M. David de Burgh Graham: Dans le temps qu'il me reste, pouvez-vous nous donner un aperçu de l'évolution de la cybersécurité à PayPal?

Vous y êtes depuis 1998, et la situation a énormément changé depuis. Y a-t-il eu des moments clés que vous pouvez nous décrire?

M. Brian Johnson: Certainement.

PayPal faisait partie d'eBay jusqu'à il y a cinq ans. Pendant cette période, il y avait eu des cyberincidents à eBay. Dans le cadre de notre programme, nous avons tiré des enseignements de ces expériences. Nous sommes devenus un chef de file mondial des plateformes de paiements numériques.

Nous avons beaucoup investi pour bien connaître nos partenaires du secteur, et pour collaborer avec les gouvernements, le public et les organismes d'application de la loi pour bien comprendre l'environnement de chacune des régions où nous sommes présents. Nous avons aussi investi dans nos plateformes antifraude pour mieux comprendre les criminels qui tentent de frauder nos clients. Et, bien sûr, nous continuons de protéger les données des consommateurs avec nos pratiques exemplaires et notre programme de protection des acheteurs qui protège les consommateurs dans toutes les situations.

M. David de Burgh Graham: Merci beaucoup d'avoir témoigné. Bien d'autres entreprises de votre secteur ont refusé de le faire. Je vous sais gré d'avoir pris le temps de venir discuter de ces questions avec nous.

● (1700)

M. Brian Johnson: Merci de nous avoir invités.

Le vice-président (M. Matthew Dubé): Merci, et je fais écho à cette observation.

Monsieur Johnson, merci beaucoup, non seulement de nous avoir accordé votre temps, mais d'avoir été patient puisque nous avons commencé en retard.

[*Français*]

Chers collègues, merci beaucoup.

Étant donné l'heure et le fait que nous devons aller voter, il ne sert à rien de revenir plus tard. Je vais donc vous remercier de votre indulgence à mon égard pendant le remplacement temporaire de M. McKay et j'ajoute que notre réunion est ajournée.

La séance est levée.