Ce qu'une adresse IP peut révéler à votre sujet

Rapport préparé par la Direction de l'analyse des technologies du Commissariat à la protection de la vie privée du Canada

2013 Mai

Table des matières

Introduction – Objet et motif de l'analyse

Au cours de la dernière décennie, le gouvernement du Canada a déposé différentes versions d'un projet de loi sur l'accès dit « légal ».

La plus récente énumérait six renseignements précis sur les abonnés qui pourraient être communiqués aux organismes responsables de l'application de la loi et de la sécurité nationale sans l'obtention préalable d'une autorisation judiciaire, soit :

- le nom;
- l'adresse;
- le numéro de téléphone;
- l'adresse de courriel;
- l'adresse de protocole Internet (IP);
- l'identifiant du fournisseur de services locaux.

(Une courte description de certains de ces renseignements [adresse IP, adresse de courriel et identifiant du fournisseur de services locaux] figure à l'Annexe A.)

« … les résultats permettent de conclure que, contrairement aux simples données contenues dans un annuaire téléphonique, les renseignements examinés peuvent servir à dresser un profil très détaillé d'une personne, de même que révéler ses activités, ses goûts, ses penchants et son style de vie ».

Les auteurs des versions précédentes du projet de loi considéraient que ces renseignements sur les abonnés étaient de nature similaire à ceux contenus dans un annuaire téléphonique[1]. Le présent document expose les résultats d'une analyse technique réalisée par le Commissariat à la protection de la vie privée du Canada (le Commissariat) afin d'examiner les conséquences sur la vie privée que peuvent avoir les renseignements sur les abonnés ne figurant pas dans un annuaire téléphonique, soit l'adresse de courriel, le numéro de téléphone cellulaire et l'adresse IP.

Les travaux de recherche liés à cette analyse ont pris fin le 19 décembre 2012 et ont été menés conformément au mandat du Commissariat qui consiste à appuyer et à effectuer des recherches sur des enjeux liés à la protection de la vie privée et à en faire connaître les conclusions, ainsi qu'à sensibiliser la population à ces enjeux en préparant et en publiant les résultats des recherches à l'intention du grand public, des institutions fédérales et des organisations du secteur privé.

Ils ont en outre été réalisés afin de permettre au personnel du Commissariat d'aborder en pleine connaissance de cause les enjeux soulevés par les propositions législatives antérieures et de formuler des conseils à l'intention du Parlement. Ils ne visent pas à formuler des commentaires sur les pratiques et procédures actuelles et futures en matière d'application de la loi ou à remettre celles-ci en question, mais simplement à brosser un portrait hypothétique de la situation.

En règle générale, les résultats permettent de conclure que, contrairement aux simples données contenues dans un annuaire téléphonique, les renseignements examinés peuvent servir à dresser un profil très détaillé d'une personne, de même que révéler ses activités, ses goûts, ses penchants et son style de vie.

Mention

Il ne s'agit pas de la première analyse du genre. Les travaux du Commissariat, qui ont débuté alors que la dernière mouture du projet de loi fédéral C-30 sur l'accès légitime figurait toujours à l'ordre du jour des travaux du Parlement, ont été précédés d'une analyse similaire réalisée par Christopher Parsons, candidat au doctorat en science politique à l'Université de Victoria.

L'analyse de M. Parsons, qui portait sur une version précédente de la législation sur l'accès légitime, a été publiée sur son blogue, *Technology, Thoughts and Trinkets,* sous le titre *The Anatomy of Lawful Access Phone Records*, le 21 novembre 2011[2]. Elle portait sur les renseignements sur les individus qu'il était possible d'obtenir au moyen du numéro d'identification internationale d'abonné mobile et du numéro d'identification internationale d'équipement mobile.

Même s'il a été proposé, dans les projets de lois précédents, que ces éléments de données soient divulgués aux autorités sans l'obtention préalable d'une autorisation judiciaire, ils ne figuraient pas parmi les éléments de données inclus dans la définition des renseignements de base sur l'abonné qui apparaît dans le projet de loi C-30.

Méthodologie – Procédures d'analyse

Aux fins de la recherche, le Commissariat a mené de simples tests afin de déterminer le type de renseignements pouvant être obtenus à partir d'une adresse IP (ou encore à partir d'une adresse de courriel ou d'un numéro de téléphone) :

1. Nous avons tout d'abord utilisé l'adresse IP du serveur mandataire Web du Commissariat ainsi que l'adresse IP d'un contributeur actif de Wikipedia.

2. Nous avons ensuite cherché le propriétaire de l'adresse IP, ainsi que toute personne ou organisation enregistrée à cette adresse, à l'aide d'outils comme WHOIS (un service en ligne qui permet notamment d'interroger des bases de données stockant de l'information sur les utilisateurs enregistrés ou les titulaires de noms de domaine ou de blocs d'adresses IP).

3. Nous avons effectué des recherches au moyen de l'adresse IP pour déterminer l'emplacement géographique du propriétaire de l'adresse IP et localiser le réseau utilisé.

4. Nous avons utilisé l'adresse IP comme terme de recherche dans différents moteurs de recherche (p. ex. Google ou Bing) et examiné les pages Web affichées dans la liste des résultats afin de trouver des exemples d'activités sur le Web (p. ex. entrées dans les journaux du serveur Web, participation à des forums en ligne).

En combinant les résultats obtenus à ces différentes étapes, il a été possible d'établir le profil détaillé des personnes ou des groupes associés à une adresse IP. Des exemples sont fournis dans les pages qui suivent.

Une fois que l'adresse IP, l'adresse de courriel ou le numéro de téléphone ont été obtenus auprès du fournisseur de service ou de l'abonné, aucun équipement ou logiciel spécial n'est nécessaire pour mener de tels tests. Une gamme de services sont offerts sur le Web pour obtenir des renseignements au sujet

d'adresses IP, d'adresses de courriel ou de numéros de téléphone. Il existe aussi des services permettant de trouver des renseignements liés à ces données, y compris le nom du propriétaire et son emplacement géographique. Enfin, certains services, comme Google et Bing, peuvent se révéler très puissants lorsque des données de ce type sont saisies comme termes de recherche.

Que peuvent révéler les renseignements de base sur l'abonné?

Les exemples qui suivent illustrent le type de renseignements supplémentaires qui peuvent être découverts à partir de certains renseignements de base sur l'abonné.

Comme le montrent les exemples, ces données permettent parfois de déterminer l'emplacement géographique réel (en plus de l'adresse municipale), des bribes de l'activité en ligne et possiblement le style de vie des abonnés.

1. Numéro de téléphone et adresse de courriel

Un numéro de téléphone (fixe ou mobile) peut être utilisé pour obtenir divers renseignements au sujet d'une personne, comme :

- les noms et adresses associés à ce numéro (à l'aide d'outils de recherche inversée, comme www.411.com);
- toute activité publique sur Internet ou document accessible au public où figure ce numéro de téléphone, y compris des billets de blogues, des messages affichés sur des forums de discussion, des dossiers financiers ou médicaux[3], etc. (à partir d'une recherche dans des sources ouvertes);
- tout domaine Internet associé à ce numéro de téléphone (en fouillant les dossiers d'enregistrement des domaines);

Tout comme le numéro de téléphone, l'adresse de courriel peut servir à obtenir des renseignements au sujet d'une personne, y compris :

- son nom réel (s'il figure dans l'adresse de courriel ou est associé à celle-ci d'une autre manière);
- son inscription à des services à partir de cette adresse de courriel (pour certains services [p. ex. LinkedIn], l'adresse de courriel sert de nom d'utilisateur);
- tout domaine enregistré à l'aide de cette adresse de courriel;
- des activités et documents sur Internet, y compris des courriels, qui contiennent l'adresse et ont été répertoriés par les moteurs de recherche;
- une liste d'amis sur les réseaux sociaux;
- les noms d'anciens employeurs (p. ex. si l'adresse figure dans un curriculum vitae affiché en ligne).

Les constatations du Commissariat…

NOTE : Les résultats des tests effectués au cours de l'analyse étaient très révélateurs et auraient pu permettre d'identifier des personnes. Afin de protéger la vie privée et de réduire les risques d'identification (correcte ou incorrecte) des personnes, les résultats présentés dans les exemples qui suivent ont été généralisés afin d'éliminer le plus de renseignements possible permettant de reconnaître celles-ci (p. ex. adresses IP, noms des sites Web, sujets des recherches, adresses URL, etc.).

À titre d'exemple, le numéro de téléphone cellulaire d'un employé du Commissariat à la protection de la vie privée du Canada a été utilisé (avec son consentement) pour mener des recherches en ligne.
Les recherches ont révélé :

- le véritable nom, au complet, de la personne;
- le nom de son fournisseur de services de télécommunications sans fil;
- deux sites Web personnels et les enregistrements de noms de domaine;
- l'affiliation à une université;
- la participation à des forums de discussion en ligne concernant la radiodiffusion sur Internet, ainsi qu'à des conférences professionnelles et portant sur la sécurité;
- la participation à un groupe d'intérêt local sur les problèmes techniques.

2. Adresse IP – Observations générales sur la fonctionnalité des adresses IP

Il est possible d'obtenir de plus amples renseignements au sujet d'un réseau, d'un appareil ou d'un service à partir d'une adresse IP. Plus précisément, l'adresse IP permet :

« …. même des activités de nature non commerciale sur Internet, comme la consultation de documents sur des pages Web, requièrent la transmission de données sur l'adresse IP, ce qui permet d'identifier l'objet de la consultation ».

- de déterminer le propriétaire et l'exploitant du réseau. Une recherche dans la base de données WHOIS à partir de l'adresse IP peut fournir une foule de renseignements sur la personne[4] (ce qui pourrait mener à la découverte de ses affiliations organisationnelles) ou l'organisation à qui l'adresse a été attribuée, y compris le nom, le numéro de téléphone et l'adresse municipale[5];
- d'effectuer une recherche inversée (établir une correspondance entre l'adresse IP et le nom de domaine auquel elle est associée) pour obtenir un nom d'ordinateur[6], ce qui fournit souvent des indices quant à l'emplacement logique et géographique;
- d'utiliser *traceroute* (un outil de diagnostic informatique qui montre l'acheminement des paquets de données sur un réseau IP) pour établir le chemin logique vers l'ordinateur, ce qui fournit souvent des indices quant à l'emplacement logique et géographique;
- de déterminer l'emplacement géographique de l'ordinateur, avec différents degrés d'exactitude. Selon l'outil de recherche utilisé[7], il est possible d'obtenir le pays, la province ou l'État, la ville, la latitude/longitude, l'indicatif régional du numéro de téléphone et une carte géographique;
- d'effectuer une recherche sur Internet à partir de l'adresse IP ou du nom de l'ordinateur. Une telle recherche pourrait révéler les activités poste-à-poste (p. ex. le partage de fichiers), les entrées dans les fichiers journaux du serveur Web, ou une partie des activités sur le Web d'une personne (p. ex. révision de pages Wikipédia). Ces bribes de l'historique des activités en ligne d'une personne peuvent permettre d'établir son allégeance politique, son état de santé, son orientation sexuelle, son appartenance religieuse, ainsi qu'une foule d'autres caractéristiques, préoccupations et intérêts personnels;
- de trouver de l'information sur les adresses courriel utilisées à partir d'une adresse IP donnée, ce qui pourrait donner lieu à d'autres demandes de renseignements sur les abonnés.

Selon Electronic Frontier Canada[8], même des activités de nature non commerciale sur Internet, comme la consultation de documents sur des pages Web, requièrent la transmission de données sur l'adresse IP, ce qui permet d'identifier l'objet de la consultation.

Les constatations du Commissariat…

Pour illustrer ce processus, un simple test a été réalisé au moyen de l'adresse IP du serveur mandataire du Commissariat à la protection de la vie privée du Canada.

Une recherche sur WHOIS a révélé que l'adresse IP était attribuée à Travaux publics et Services gouvernementaux Canada (TPSGC) et associée à l'adresse 350 CDKE (il s'agit du Centre de données King Edward), Ottawa (Ontario) K1A 0S5. Le point de contact technique était identifié, et son nom complet, son adresse de courriel et son numéro de téléphone étaient fournis.

Plus de 240 résultats ont été obtenus en utilisant l'adresse IP comme terme de recherche. Ces résultats ont indiqué que les personnes travaillant à partir de cette adresse IP avaient consulté des sites concernant notamment :

- la formation sur l'optimisation des moteurs de recherche;
- le monde de la publicité et du marketing au Canada;
- la gouvernance du Web;
- la gestion de l'identité;
- les questions de vie privée;
- des conseils juridiques sur le droit des assurances et les litiges pour lésions corporelles;
- un certain groupe religieux;
- le conditionnement physique;
- le partage de photos en ligne;
- l'historique des révisions d'une page Wikipédia;
- certains artistes, ce qui a permis de révéler un éventail de noms d'utilisateurs.

3. Adresse IP – Renseignements sur les personnes

Il est à noter que les renseignements ci-dessus ont été tirés de l'activité en ligne à partir d'un ensemble d'ordinateurs, et non d'un poste de travail individuel. Cela dit, le procédé utilisé pour obtenir ces résultats peut être appliqué à un abonné résidentiel. Les renseignements précis pouvant être obtenus dépendent du niveau d'activité en ligne des abonnés et de la façon dont les sites Web consultés traitent les adresses IP (autrement dit, laissent-elles les moteurs de recherche les répertorier?).

Afin de montrer ce qu'une simple adresse IP permet de découvrir au sujet d'une personne, une analyse similaire a été entreprise à l'aide d'une adresse IP plus représentative d'un abonné individuel.

Les constatations du Commissariat…

Le Commissariat s'est penché sur des collaborateurs actifs de Wikipédia et a effectué des recherches à partir des adresses IP indiquées sur ce site. Celles-ci permettent souvent d'établir un profil détaillé des collaborateurs.

Par exemple, l'adresse IP d'un certain collaborateur de Wikipédia[9] a révélé que cette personne :

- avait révisé des centaines de pages Wikipédia au sujet d'émissions de télévision nord-américaines ou étrangères. Cet intérêt à l'égard des émissions de télévision était vaste et circonscrit, mais des précisions ne sont pas fournies ici pour des raisons de confidentialité;
- avait révisé des douzaines de pages Wikipédia sur des sujets liés à l'histoire;
- avait participé à un groupe de discussion au sujet d'une chaîne de télévision;
- avait consulté un site consacré aux préférences sexuelles, puis effectué une recherche en ligne pour un type de personne particulier.

Aux fins des recherches menées par le Commissariat, les renseignements susmentionnés ont été obtenus à partir d'une simple adresse IP. Toutefois, ces exemples donnent un aperçu du type de portrait que les organismes d'application de la loi pourraient brosser d'un individu sans qu'il soit nécessaire d'obtenir une autorisation judiciaire au préalable, comme l'ont proposé les divers projets de loi déposés au cours de la dernière décennie.

L'affaire Petraeus – Montrer ce que les renseignements de base sur les abonnés *ont* révélé et les conséquences qui en ont découlé

Un autre exemple des renseignements qu'il est possible d'obtenir en se servant d'une adresse IP comme point de départ d'une enquête est l'affaire *Petraeus* aux États-Unis, qui a été largement médiatisée. Il s'agissait au départ d'une enquête sur des courriels de harcèlement qui a mené à la révélation d'une aventure extraconjugale du directeur de la CIA, David Petraeus, et à d'autres détails compromettants, et qui s'est terminée par la démission de ce dernier[10].

Selon les renseignements qui peuvent être obtenus au moyen des sources médiatiques publiques, la séquence des événements semble être la suivante :

a) Une personne reçoit des courriels de harcèlement « anonymes » et demande au FBI d'enquêter. Des copies des courriels sont transmises au FBI;
b) Même si les messages ont été envoyés d'un service de dépersonnalisation, les adresses IP à partir desquelles ils ont été transmis figuraient dans l'en-tête des courriels;
c) Puisqu'il connaissait les adresses IP sources, le FBI a été en mesure d'identifier l'organisation à laquelle elles avaient été attribuées (en règle générale, un ou des fournisseurs de services de télécommunication);
d) Sur réception d'assignations administratives[11], qui sont émises par les autorités chargées de l'application de la loi sans surveillance judiciaire, le ou les fournisseurs de services de télécommunication ont ensuite transmis les renseignements sur l'abonné correspondant aux adresses IP utilisées pour accéder au

« …le FBI a pu obtenir ces renseignements au moyen d'assignations administratives, ou peut-être de lettres de sécurité nationale; dans le cas de ces deux documents, aucune approbation judiciaire indépendante n'est requise au préalable. Au Canada, dans le cadre de propositions législatives présentées dans le passé par le gouvernement fédéral, des renseignements semblables pourraient être obtenus sans approbation judiciaire indépendante préalable ».

compte de courriel d'origine, ainsi qu'à tout autre compte de courriel consulté à partir des mêmes adresses IP. Il semblerait que Google a donné au FBI de l'information sur chaque adresse IP utilisée pour avoir accès au compte[12];

e) Le fournisseur de services Internet (FSI) a associé les adresses IP à divers endroits, y compris des hôtels;
f) En connaissant les lieux physiques à partir desquels ont été envoyés les courriels, le FBI a pu obtenir la liste des gens qui se trouvaient dans ces endroits au moment de l'envoi des messages en présentant une assignation administrative[13];
g) Un nom revenait constamment dans la liste des personnes présentes pendant les périodes où les messages ont été envoyés, si bien que cette personne est devenue le suspect le plus probable;
h) C'est alors que le FBI a demandé et obtenu un mandat pour avoir accès au contenu du compte de courriel anonyme.

Le FBI a pu obtenir les renseignements suivants sans avoir à demander de mandat :

a) Les adresses IP à partir desquelles ont été envoyés les courriels de harcèlement;
b) Les noms des fournisseurs de services de télécommunication à qui ces adresses ont été attribuées;
c) Les renseignements sur l'abonné correspondant au compte de courriel utilisé pour envoyer les courriels, ainsi que des renseignements sur d'autres comptes de courriel consultés à partir des mêmes adresses IP;
d) Les organisations – dans le présent cas, les hôtels – auxquelles le fournisseur de services de télécommunication avait attribué les adresses IP;
e) Les listes des personnes enregistrées dans ces hôtels au moment de l'envoi des courriels.

Selon plusieurs sources publiques[14], le FBI a pu obtenir ces renseignements au moyen d'assignations administratives[15], ou peut-être de lettres de sécurité nationale; dans le cas de ces deux documents, aucune approbation judiciaire indépendante n'est requise au préalable. Au Canada, dans le cadre de propositions législatives présentées dans le passé par le gouvernement fédéral, des renseignements semblables pourraient être obtenus sans approbation judiciaire indépendante préalable.

« Plus les technologies de l'information sont présentes dans nos vies et constituent un prolongement de notre personne, et plus les renseignements d'un abonné deviennent sensibles et révélateurs ».

Résumé – Ce que tout cela signifie

Comme le démontrent les exemples susmentionnés, le fait de posséder des renseignements sur un abonné, comme des numéros de téléphone et des adresses IP, peut servir de point de départ pour dresser un tableau des activités en ligne de celui-ci, notamment :

- Les services en ligne auxquels il est abonné;
- Ses intérêts personnels, en fonction des sites Web visités;
- Les organisations auxquelles il appartient.

Ces renseignements peuvent aussi donner un aperçu des endroits où la personne est allée (p. ex. en établissant une carte des adresses IP liées aux hôtels, comme dans l'affaire *Petraeus*).

Ils peuvent être sensibles, car ils peuvent permettre de déterminer, entre autres, les penchants d'une personne, ses fréquentations et les endroits où elle voyage. De plus, chacun de ces éléments d'information peut servir à dévoiler davantage de renseignements sur cette personne.

Plus les technologies de l'information sont présentes dans nos vies et constituent un prolongement de notre personne, et plus les renseignements d'un abonné deviennent sensibles et révélateurs.

Le fait d'affirmer que ces données sont comparables à ce qu'on peut trouver dans les pages blanches d'un annuaire téléphonique signifie que l'on se fait une idée erronée de la situation et qu'on sous-estime grossièrement la quantité de renseignements auxquels elles peuvent donner accès.

Ces données sont vraiment plus que de simples renseignements « d'annuaire téléphonique ».

Annexe A

Adresse de protocole Internet

Une adresse de protocole Internet (IP) est un identifiant numérique (adresse logique) attribuée aux appareils connectés à un réseau informatique qui utilise le protocole Internet. Bien que les adresses IP soient représentées sous forme de nombres binaires, elles sont habituellement affichées dans une forme plus facilement lisible par les humains, comme 208.77.188.166. Le protocole Internet doit aussi transmettre des paquets de données entre les réseaux, et les adresses IP précisent les lieux des nœuds sources et de destination dans la topologie du système d'acheminement.

L'adresse IP est attribuée, ou louée, à une personne par un fournisseur de services Internet; elle constitue un élément essentiel de l'accès à Internet comme tel. Les adresses IP indiquent la provenance des données et leur destination. Elles peuvent être statiques ou dynamiques. L'adresse IP statique est attribuée à un appareil relié à un réseau qui doit avoir une adresse permanente attribuée (p. ex. un serveur, un pare-feu, un routeur). D'autre part, une adresse IP dynamique est attribuée à un appareil relié temporairement à un réseau, ce qui est généralement le cas dans l'espace des consommateurs. Il convient de signaler que la durée d'une affectation d'adresse IP peut varier de quelques jours à quelques mois, selon le nombre de facteurs comme la taille du groupe d'adresses IP à la disposition du fournisseur de services Internet (FSI), le nombre d'abonnés et la stabilité relative du réseau.

La plupart des fournisseurs de services de télécommunication imposent des limites quant à la quantité de données un abonné peut télécharger au cours d'une période donnée, selon le forfait qu'il a acheté (p. ex. Rogers permet 20 Go de données par mois pour un forfait d'accès Internet « Lite »). De plus, ils appliquent des frais pour l'utilisation qui dépasse la limite du forfait. À cette fin, les fournisseurs de services de télécommunication doivent pouvoir associer avec précision l'achalandage de téléchargement à un abonné, et cela est possible en conservant un registre de l'adresse ou des adresses IP attribuées à cet abonné pendant cette période. Le temps de conservation de ce registre par le fournisseur de services de télécommunication dépend des exigences législatives ou réglementaires pertinentes ou de ses pratiques d'affaires particulières[16].

Adresse électronique

Une adresse électronique désigne une boîte aux lettres informatique où sont transmis des messages électroniques. Elle se présente généralement comme suit : jdupont@exemple.org. Elle comporte deux parties : avant le signe @, il s'agit de la *partie locale* et après le signe @, du *nom de domaine* où sera acheminé le message électronique.

La partie locale de l'adresse est souvent le nom d'utilisateur du destinataire (jdupont). C'est certainement le cas au gouvernement du Canada et dans la plupart des entreprises, qui généralement adoptent une convention standard pour les adresses électroniques (c.-à-d. prénom.nomdefamille@).

Toutefois, la partie locale de l'adresse peut aussi être un pseudonyme. Bien que certains fournisseurs de services de courriel sur le Web (p. ex. Gmail de Google et Hotmail de Microsoft) exigent que l'abonné entre un nom, une adresse et ainsi de suite au moment de créer un compte de courriel, ils ne vérifient pas nécessairement si l'information est vraie. La partie du nom de domaine de l'adresse indiquera le type d'organisation à laquelle appartient l'utilisateur (p. ex. @priv.gc.ca) ou le fournisseur de services de courriel (p. ex. @rogers.com, @gmail.com).

Les adresses électroniques peuvent être liées à des comptes particuliers; elles peuvent aussi être des adresses générales. Une personne peut avoir plus d'une adresse électronique, par exemple, une adresse pour un forum Web, une deuxième pour les achats en ligne et, enfin, une troisième pour la correspondance personnelle. En fait, cela est recommandé sur le plan de la sécurité et de la protection des renseignements personnels.

Identifiant du fournisseur de services locaux

L'identifiant du fournisseur de services locaux, appelé parfois « identité du fournisseur de services locaux » (IFSL), est un numéro unique attribué aux fournisseurs de services afin que les propriétaires de commutateurs de télécommunication et les fournisseurs de services de télécommunication puissent avoir des relations financières pour le transport de trafic. Le nombre identifie l'entreprise qui « possède » le compte associé au trafic. Il est alors possible d'identifier l'abonné qui utilise un service particulier (p. ex. un abonné de Rogers qui utilise un cellulaire Rogers sur le réseau d'AT&T) afin que l'utilisation du service (dans ce cas, le réseau d'AT&T) soit facturée à la bonne personne.

Notes de fin de document

[1] CBC News, *Opposition jumps on surveillance bill confusion*, daté du 20 février, 2012.
[2] Christopher Parsons, *The Anatomy of Lawful Access Phone Records*, publié sur le blogue *Technology, Thoughts and Trinkets* le 21 novembre 2011. Voir aussi *The Issues Surrounding Subscriber Information in Bill C-30*, publié le 28 février 2012.

[3] Une recherche fondée sur un élément des renseignements de base sur l'abonné, comme le numéro de téléphone ou l'adresse de courriel, peut donner accès à des dossiers financiers ou médicaux si la séquence de mots recherchée y figure et que les dossiers ont été indexés par un moteur de recherche.

[4] À mesure que de plus en plus de personnes enregistreront leur propre nom de domaine (p.ex. jeandupont.com), une recherche sur WHOIS à partir de l'adresse IP pourra révéler directement le nom et l'adresse d'une personne, ainsi que d'autres renseignements, sans devoir passer par le fournisseur de services.

[5] À l'origine, WHOIS a été conçu pour permettre aux administrateurs de système de trouver de l'information sur d'autres adresses IP ou administrateurs de noms de domaine (un peu comme les Pages blanches). Pour un exemple du type d'information que révèle une interrogation de WHOIS, voir http://en.wikipedia.org/wiki/WHOIS#Data_Returned.Voir aussi http://whatismyipaddress.com.

[6] Un nom d'ordinateur sert à identifier ou repérer un ordinateur sur un réseau. Les noms des ordinateurs doivent être uniques afin que les ordinateurs puissent être identifiés avec précision à des fins de communication.

[7] Il existe plusieurs outils permettant de trouver des adresses IP et d'autres renseignements connexes, dont IP Lookup, IP Tools, et WHOIS.

[8] Renseignements tirés d'une présentation conjointe d'Electronic Frontier Canada/Electronic Freedom Foundation datée du 17 décembre 2002, en réponse à un document de consultation du ministère de la Justice publié le 25 août 2002.

[9] Il existe deux façons d'apporter une contribution à Wikipédia. On peut soit se créer un compte puis s'y connecter avant d'apporter sa contribution, ou collaborer de façon anonyme. Dans ce deuxième cas, Wikipédia enregistre l'adresse IP de l'ordinateur utilisé pour accéder à Wikipédia. Aux fins de la présente recherche, le Commissariat a cliqué sur l'onglet « Modifications récentes » (à gauche sur la page d'accueil), puis a examiné une série d'entrées comportant des adresses IP. En cliquant sur l'adresse IP, le Commissariat a pu voir les contributions apportées par un utilisateur donné. Le Commissariat a ensuite choisi un utilisateur ayant un haut taux d'activités. Au bas de la page figurent des outils comme WHOIS, traceroute et geolocate, qui permettent d'obtenir plus de renseignements au sujet de l'utilisateur.

[10] L'affaire *Petraeus* a fait l'objet d'une vaste couverture médiatique, notamment :

a) NBC News, R. Engel, « Petraeus' biographer Paula Broadwell under FBI investigation over access to his e-mail, law enforcement officials say », daté du 9 novembre 2012, consulté le 5 décembre 2012.

b) WIRED Magazine (édition en ligne), K. Zetter, « Email Location Data Led FBI to Uncover Top Spy's Affair », daté du 12 novembre 2012, consulté le 5 décembre 2012.

c) USA Today, D. Leinwand Leger et Y. Alcindor, « Petraeus and Broadwell used common e-mail trick », daté du 13 novembre 2012, consulté le 5 décembre 2012.

d) T. Klosowski, « How CIA Director David Petraeus's Emails Were Traced (And How to Protect Yourself) », daté du 13 novembre 2012, consulté le 5 décembre 2012.

e) American Civil Liberties Union (ACLU), C. Sogohian, « Surveillance and Security Lessons from the Petraeus Scandal », daté du 13 novembre 2012, consulté le 5 décembre 2012.

f) BBC, « How email trail aided Petraeus case », daté du 14 novembre 2012, consulté le 5 décembre 2012.

g) J. Sanchez, « Collateral damage of our surveillance state », Reuters (édition américaine), daté du 15 novembre 2012, consulté le 17 décembre 2012.

h) Bruce Schneier, « E-mail Security in the Wake of Petraeus », billet sur le blogue Schneier on Security, daté du 19 novembre 2012, consulté le 17 décembre 2012.

[11] Voir, par exemple, J. Sanchez, « Collateral damage of our surveillance state », Reuters (édition américaine), daté du

15 novembre 2012, consulté le 17 décembre 2012. Voir aussi M. Ambinder, « What the heck, FBI? », The Week, daté du 13 novembre 2012, consulté le 17 décembre 2012.

[12] USA Today, D. Leinwand Leger et Y. Alcindor, « Petraeus and Broadwell used common e-mail trick », daté du 13 novembre 2012, consulté le 5 décembre 2012.

[13] A. Leonard, « Paula Broadwell's big mistake », Salon, 16 novembre 2012, consulté le 28 janvier 2013.

[14] Voir, par exemple, J. Sanchez, « Collateral damage of our surveillance state », Reuters (édition américaine), daté du 15 novembre 2012, consulté le 17 décembre 2012. Voir aussi M. Ambinder, « What the heck, FBI? », The Week, daté du 13 novembre 2012, consulté le 17 décembre 2012.

[15] Il existe divers types d'assignation reconnus par le droit américain. Les trois plus courants sont les suivants : assignation administrative (c.-à-d. une assignation provenant d'un organisme gouvernemental qui détient le pouvoir d'en délivrer), assignation à comparaître au procès (parfois appelée assignation d'un juge administratif) et assignation du grand jury. Une assignation administrative est probablement ce que le FBI utilisait pour obtenir certains renseignements préliminaires dans l'affaire *Petraeus*. Voir, par exemple, R. Rothacker et D. Ingram, « Identity of second woman emerges in Petraeus' downfall », Reuters, 12 décembre 2012 (consulté 14 janvier 2013). Dans l'article, on cite sans le nommer un fonctionnaire du gouvernement américain qui a déclaré que l'enquête du FBI sur les courriels était assez simple et ne nécessitait pas l'obtention d'ordonnance de la cour pour surveiller les comptes de courriel des personnes touchées, y compris le compte de courriel personnel de David Petraeus. Voir aussi A. Leonard, « Paula Broadwell's big mistake », Salon, 16 novembre 2012, consulté le 14 janvier 2013.

[16] Les fournisseurs de courriel Web comme Google, Yahoo et Microsoft conservent les enregistrements des connexions (généralement pendant plus d'un an), qui indiquent les adresses IP à partir desquelles un consommateur s'est connecté. Voir l'American Civil Liberties Union (ACLU), C. Sogohian, « Surveillance and Security Lessons from the Petraeus Scandal », daté du 13 novembre 2012, consulté le 5 décembre 2012.

Vous pouvez trouver cette publication en ligne à l'adresse suivante :

http://www.priv.gc.ca/information/research-recherche/2013/ip_201305_f.asp