



Commissariat
à la protection de
la vie privée du Canada

Office of the
Privacy Commissioner
of Canada

Rencontre de deux mondes : les univers du droit et de la technologie de l'information (TI)

L'identité en ligne : entre la vie privée et les profils virtuels

Jennifer Stoddart
Commissaire à la protection de la vie privée du Canada

Février 2008

Table des matières

Introduction	1
Profils virtuels : survol préliminaire.....	1
Profil intentionnel ou actif	1
Profil involontaire ou passif	2
<i>Destinataires potentiels des renseignements contenus dans un profil</i>	3
<i>Courtiers en données</i>	3
<i>Marketing</i>	3
<i>Vol d'identité</i>	4
<i>Enquêtes et surveillance</i>	4
Rencontre entre le monde virtuel et le monde réel : impacts potentiels.....	5
Préoccupations au sujet de la protection de la vie privée	6
Gérer l'identité en ligne	6
Initiatives du CPVP	7
Conclusion	8

Introduction

La grande croissance des sites de réseaux sociaux en ligne, comme Facebook et MySpace, a mené un très grand nombre de gens à découvrir le concept du profil virtuel. Dans bien des cas, la création d'un profil en ligne est la première étape (et une condition préalable) vers la participation active dans un réseau social en ligne. En général, l'utilisateur doit fournir certains renseignements personnels pour adhérer à de tels services (une adresse de courriel valide, par exemple). Lorsqu'il crée son profil virtuel, cependant, il peut généralement effectuer de nombreux choix personnels : il peut, par exemple, choisir d'adhérer à un service précis, choisir quels renseignements fournir ou non et choisir la langue utilisée pour fournir ces renseignements. Le profil virtuel est, dans une certaine mesure, un véhicule d'expression créative, qui permet à une personne de personnaliser son profil afin de refléter les façons précises dont elle souhaite se présenter en ligne. On pourrait soutenir que les membres des services de réseaux sociaux en ligne apprennent comment gérer leur identité en ligne. Est-ce bien le cas?

Bien que bon nombre de Canadiens ne choisissent pas d'adhérer à un site de réseau social ou de créer un profil virtuel intentionnel, ils pourraient être surpris d'apprendre qu'ils possèdent probablement un profil virtuel involontaire ou passif, qui correspond probablement très peu au genre de profil qu'ils créeraient eux-mêmes. Le profil « intentionnel » soigneusement composé sur un site de réseau social ne représente souvent que la pointe de l'iceberg de l'identité en ligne d'une personne. Peu de gens se font une idée juste de la quantité de renseignements les concernant qui se retrouve en ligne ou des façons dont ces renseignements peuvent contribuer à leur identité virtuelle. Il est encore plus surprenant de constater la portée potentielle de ce profil virtuel involontaire sur l'existence non virtuelle, hors ligne, de la personne. Ce document étudie la portée potentielle d'un profil virtuel, détecte quelques-uns des enjeux liés à la vie privée soulevés par de tels profils et offre des suggestions pour renforcer notre capacité de contrôler notre identité en ligne, et, donc, hors ligne.

Profils virtuels : survol préliminaire

Profil intentionnel ou actif

Un profil intentionnel en ligne peut prendre de nombreuses formes. Le profil des sites de réseaux sociaux, à certains égards, n'est qu'une façon personnelle de présenter le genre de renseignements biographiques que les personnes fournissent souvent pour des raisons professionnelles, comme le font les membres du corps professoral d'une université ou les avocats d'un cabinet.

Dans tous les cas, l'information est soigneusement choisie et présentée pour des destinataires précis; dans le cas de l'outil de réseau social, le créateur du profil peut également avoir un certain contrôle sur les destinataires du profil achevé. Le contrôle du créateur sur le contenu et la présentation du profil est l'élément qui définit un profil intentionnel.

Profil involontaire ou passif

Le profil involontaire d'une personne est constitué de l'ensemble des informations personnelles à son sujet que l'on peut trouver en ligne. Les sources de tels renseignements peuvent être disparates et, dans bien des cas, l'information pourra s'être retrouvée en ligne sans la participation de la personne concernée. La variété de tels renseignements est illimitée : un nom ajouté à une pétition, des coordonnées obtenues de services d'annuaires en ligne, un commentaire publié sur le blogue de quelqu'un, un nom figurant sur la liste des donateurs à une cause précise, la légende sous une photo prise lors d'une réunion d'anciens du secondaire, etc.

Les éléments du profil peuvent être involontaires pour plusieurs raisons. Il se peut que les renseignements n'aient pas été obtenus auprès des personnes concernées, et que ces personnes n'aient pas été consultées avant leur publication en ligne. Par ailleurs, des renseignements recueillis hors ligne pourraient être publiés en ligne sans que la personne ne sache qu'ils étaient destinés à une diffusion inconditionnelle en ligne. On pourrait considérer que des renseignements d'abord publiés en ligne de façon intentionnelle font partie du profil involontaire, compte tenu de la durée de leur période d'affichage en ligne. Les pages en antémémoire font en sorte que même les renseignements qui ont été effacés par leur auteur peuvent demeurer accessibles en ligne et peuvent être récupérés au moyen d'outils de recherche en ligne longtemps après la soi-disant suppression.

Le profil involontaire d'une personne est donc une combinaison de toutes les sortes d'informations personnelles que l'on trouve en ligne à son sujet. Pour avoir une meilleure idée des renseignements disponibles, on peut procéder à une simple recherche du nom d'une personne à l'aide de n'importe lequel des principaux moteurs de recherche. Le résultat sera probablement composé d'une vaste gamme de renseignements, présentés sans souci d'actualité, d'exactitude ou de contexte. Pris à la pièce, la plupart de ces résultats peuvent sembler inoffensifs. Lorsqu'on les considère tous ensemble, cependant, le profil involontaire apparaît, avec ou sans l'aide, la connaissance ou le consentement de la personne concernée.

Un profil passif contient une couche additionnelle. Les divers types de dispositifs de suivi font en sorte que les activités en ligne d'une personne laissent une trace qui peut être d'un grand intérêt pour d'autres. Bien que les personnes aient bien

peu de chance de voir cette couche de leur profil virtuel de façon concrète, il est fort probable qu'elle leur soit communiquée par l'entremise d'activités de marketing ciblées en fonction des choix qu'elles ont faits lors d'activités en ligne, comme la visite de sites Web et les recherches effectuées.

Destinataires potentiels des renseignements contenus dans un profil

Il est peu probable qu'une personne moyenne comprenne bien de quoi a l'air son profil virtuel complet, mais certains destinataires potentiels le savent tout à fait. Prendre conscience de l'éventail des destinataires potentiels et des raisons qui motivent leur intérêt pour ce qui peut sembler être de l'information personnelle inoffensive peut aider les personnes à exercer un contrôle sur leurs identités en ligne.

Courtiers en données

Vu la mine d'information disponible en ligne, l'existence d'organisations dont les activités consistent à assembler et à vendre les renseignements personnels n'est pas surprenante. Les plus importants courtiers en données détiennent des milliards de collections de documents. Ce genre d'« accès superposé » à de l'information personnelle autrement disponible soulève d'intéressantes questions quant à la notion de ce que constitue l'information « accessible au public ». Cela soulève également des inquiétudes quant au respect du principe du consentement fondé sur le but, puisque la collecte et la communication ultérieure iront, dans la plupart des cas, bien au-delà de la collecte, de l'utilisation ou de la communication envisagée au départ par la personne concernée.

Marketing

Tel que mentionné ci-dessus, plusieurs éléments du profil en ligne d'une personne représentent un intérêt du point de vue du marketing. En effet, c'est la valeur perçue de tels renseignements qui soutient de nombreux services et activités soi-disant « gratuits » en ligne, comme les sites de réseaux sociaux, les services de courriel sur le Web et les moteurs de recherche. Bien que ce genre de renseignements de profil pris dans leur ensemble intéresse depuis longtemps les publicitaires, leur utilisation a pris la forme plus sophistiquée du marketing ciblé. Les intérêts, les goûts, les préférences, et les aversions d'une personne, reflétés tant par les renseignements sur elle qui ont été publiés sur Internet que par les choix qu'elle effectue en ligne, lui sont réfléchis dans une publicité conçue pour être d'autant plus efficace qu'elle a été ciblée, soit pour viser un groupe démographique, soit, parfois, pour viser cette personne en particulier.

Vol d'identité

Il existe également une quantité considérable d'activités criminelles axées sur la collecte, l'utilisation et la communication non autorisées de renseignements personnels en ligne. Le profil virtuel d'une personne peut fournir suffisamment de renseignements pour permettre à un voleur d'identité de se faire passer pour cette personne dans le but de réaliser des activités frauduleuses. Lorsque le profil virtuel accessible est insuffisant pour ces fins, les voleurs d'identité peuvent le compléter d'autres façons, que ce soit en testant les mesures de protection des organisations qui ont la garde de renseignements personnels sensibles (comme les institutions financières) ou en procédant à l'hameçonnage de renseignements personnels directement auprès des personnes concernées.

Enquêtes et surveillance

Internet est également une ressource importante pour les personnes qui s'occupent d'enquêtes ou de surveillance. Certaines auront recours aux services d'un courtier en données afin d'obtenir les renseignements désirés, mais, dans bien des cas, l'utilisation d'un moteur de recherche suffira. Plus simplement, bien des employeurs effectuent, durant le processus de recrutement, une recherche Internet portant sur le nom du candidat. Le candidat ne sera peut-être pas averti qu'une telle recherche sera entreprise, ni informé qu'elle a eu lieu. Ces recherches sont pourtant une pratique courante de bien des employeurs.

Des renseignements en apparence inoffensifs peuvent également servir à une utilisation plus sophistiquée. En vertu de ce que les services de renseignements appellent le « principe de la mosaïque », des éléments d'information qui semblent négligeables en soi peuvent, lorsque réunis, former un tout ayant une valeur. Quoiqu'un tel travail de compilation soit laborieux, le volume de renseignements disponibles dans Internet et la durée de leur accessibilité encouragent la persévérance de telles entreprises. Il faut également noter que l'organisation des données en couches peut faire que des renseignements qui ne seraient pas personnels (car ils ne permettent pas d'identifier une personne en particulier) le deviennent lorsque combinés. Pour les autorités chargées de l'application des lois, l'information offerte sur Internet fournit un moyen de réaliser des activités d'enquête importantes, sans mandat¹. Or, si ce travail est effectué par les autorités chargées de l'application des lois, ces dernières n'ont pas le monopole de telles activités d'enquête. Le secteur privé s'adonne à des activités similaires, tant dans les domaines où le secteur public lui a délégué une telle autorité que dans le contexte d'activités d'enquête plus générales du secteur privé.

¹ L'utilisation d'Internet comme outil d'enquête (et, dans certains cas, comme solution de rechange à l'obtention d'un mandat) a des conséquences importantes sur le droit à la vie privée prévu par l'article 8 de la *Charte*.

Rencontre entre le monde virtuel et le monde réel : impacts potentiels

L'examen des destinataires potentiels des renseignements d'un profil virtuel montre clairement que l'identité virtuelle d'une personne peut avoir des impacts dans la vraie vie.

Les Forces canadiennes ont récemment adressé un avertissement à leurs membres et à leurs familles au sujet de la publication de renseignements personnels en ligne, en particulier sur les sites de réseaux sociaux, leur rappelant que ce qui peut sembler inoffensif et sans importance à la personne qui le publie pourrait revêtir un caractère beaucoup plus dangereux entre les mains d'une autre personne, si celle-ci les jumelait à d'autres éléments d'information et avait la volonté de les assembler patiemment².

Dans un autre contexte, des employés ont eu une bien mauvaise surprise lorsque des renseignements qu'ils avaient publiés sur Facebook ont été communiqués à leur employeur par d'anciens collègues. Les employés avaient publié en ligne de l'information douteuse, directement liée à leurs emplois, y compris des photographies des employés portant leur uniforme, prises en contravention directe de leur code de déontologie. Comme l'employeur, l'Agence des services frontaliers du Canada, l'a écrit dans une note de service interne, [traduction] « Même la conduite en dehors des heures de travail devient une question d'ordre professionnel si elle met indûment en péril la réputation ou les programmes de l'Agence³ ». Dans ce cas, la conduite semble avoir été clairement déplacée et les personnes qui ont publié l'information semblent avoir choisi de lier leur conduite à leur lieu de travail et de prendre peu de précautions pour limiter l'accès à ces renseignements. On peut toutefois facilement imaginer des scénarios dans lesquels les faits s'avèreraient pencher moins nettement en faveur de l'employeur.

Une grande proportion des activités en ligne se produisent sans considération des frontières nationales. En fait, la collecte, l'utilisation et la communication d'information en ligne peuvent concerner plusieurs territoires de compétence. Dans une affaire récente, la directrice générale de la Clinique d'intérêt public et de politique d'Internet du Canada est entrée en contact avec un courtier en données en ligne situé aux États-Unis afin de demander son propre profil. Lorsque le profil est arrivé, il s'est avéré être une compilation en grande partie fictive. Non seulement ce profil erroné était fourni contre rémunération à

² « Military warns soldiers not to post info on Facebook », CBC News, 25 février 2008, www.cbc.ca.

³ « Student recruits unfit for service, say former border guards », CBC News, 1^{er} octobre 2007, www.cbc.ca.

quiconque le demandait, mais la personne profilée n'aurait peut-être jamais appris qu'un tel profil existait ou avait été obtenu par d'autres⁴.

Préoccupations au sujet de la protection de la vie privée

L'identité en ligne soulève d'importantes inquiétudes quant à la protection des renseignements personnels. Le fait qu'un profil virtuel continue de se développer même sans contribution consciente de la personne concernée semble indiquer qu'une personne moyenne n'a pas de contrôle sur son identité en ligne. La sphère privée s'en trouve donc réduite et les attentes raisonnables d'une personne en matière de vie privée sont directement remises en question. Comme il est possible de développer un profil virtuel sans jamais être en ligne, il est difficile d'imaginer un refus de participer à ce processus. De plus, les éléments qui s'additionnent pour former un profil en ligne comprennent de nombreuses transactions et interactions de base, essentielles à notre adhésion à la société moderne, comme les services bancaires, le paiement de factures ou l'inscription à des services gouvernementaux. Dans une certaine mesure, nous ne pouvons éviter de laisser une trace identitaire, tant hors ligne qu'en ligne. L'importance croissante de l'identité en ligne dans nos vies signifie également que nous ne pouvons renoncer à notre droit fondamental à la vie privée pour la portion en ligne de notre existence.

Gérer l'identité en ligne

La tâche de gérer son identité en ligne peut sembler intimidante. Pourtant, les personnes peuvent prendre quelques mesures simples afin de protéger leur vie privée en ligne et, du même coup, gérer leur identité en ligne. Nous pouvons, à tout le moins, être maîtres de nos profils intentionnels. En étant conscients de l'intérêt que peut représenter pour d'autres l'information que nous publions sur nous-mêmes en ligne, nous pouvons faire des choix plus éclairés au sujet de la trace identitaire que nous choisissons de créer. Nous savons, par exemple, que certains éléments clés de l'information personnelle fournissent la base requise pour le vol d'identité et ne devraient pas être communiqués dans un contexte non sécurisé (par exemple, numéros d'assurance sociale, date de naissance, adresse et numéro de téléphone). Nous pouvons également nous assurer de savoir comment l'information pourra être diffusée avant de la fournir. Si, par exemple, l'information n'est pas protégée et est accessible au moyen des outils de recherche en ligne, nous pouvons à tout le moins être conscients que des versions en antémémoire de cette information seront disponibles sous forme de résultats de recherche longtemps après sa suppression du site où elle a d'abord été publiée.

⁴ *Lawson c. Accusearch Inc.*, [2007] 4 A.C.F. 314 (C.F.).

Il est également bon de demeurer conscients des objectifs qui motivent la collecte de renseignements personnels en ligne. Dans le cas des sites de réseaux sociaux, par exemple, les utilisateurs peuvent croire que l'objectif de la collecte de leurs renseignements personnels vise à leur permettre de participer pleinement au réseau social qui en résulte. Quoique cet objectif puisse être valide, il n'est pas le seul qui motive la collecte et peut, en fait, n'être qu'un objectif secondaire à la collecte aux fins de marketing. Plusieurs services en ligne offerts à l'utilisateur sans frais apparents sont, en réalité, soutenus commercialement par la valeur des renseignements personnels fournis par les personnes comme condition à l'utilisation du service ou découlant de son utilisation. Comme pour les programmes de fidélisation hors ligne, c'est en comprenant ce qui rend un service viable commercialement que nous pourrions être mieux outillés pour évaluer les avantages et les inconvénients de notre participation et que nous pourrions, dans le cas de bien des activités en ligne, prendre des décisions informées sur l'étendue de notre participation.

Initiatives du CPVP

Le CPVP a pris part à plusieurs activités de sensibilisation du grand public destinées à accroître la conscientisation quant au besoin de protéger les renseignements personnels en ligne, y compris, notamment, dans les environnements en ligne comme les sites de réseaux sociaux. Le CPVP est conscient que l'utilisation des sites de réseaux sociaux est généralisée chez les jeunes Canadiens, même si l'utilisation de tels services par d'autres groupes démographiques a connu une augmentation fulgurante. Les jeunes ont besoin d'outils particuliers afin de les aider à faire des choix éclairés au sujet de l'identité en ligne, et ces outils doivent leur être présentés de façon significative. Dans cette optique, le CPVP a créé un court film vidéo intitulé « Qu'est-ce qu'un ami d'un ami d'un ami a besoin de savoir sur vous? » sur les répercussions sur la protection des renseignements personnels des sites de réseaux sociaux. Le film, accessible sur notre site Web et sur notre poste YouTube, a été visionné plus de 5 000 fois sur YouTube.

Nous avons également préparé un certain nombre d'outils pour aider les gens à se protéger contre le vol d'identité. « L'abc du vol d'identité » et la « Liste de vérification concernant le vol d'identité » ne sont que deux exemples des outils offerts sur notre site Web. Une personne peut grandement améliorer sa protection contre le vol d'identité en prenant quelques mesures simples. Notre objectif est de sensibiliser les gens à un éventail de changements concrets, qui peuvent facilement être mis en application.

Les enjeux liés à la vie privée en ligne évoluent au même rythme que la technologie qui facilite les activités en ligne et que nos utilisations de cette technologie. Le CPVP doit anticiper ces changements pour être en mesure d'informer le public des répercussions sur la protection des renseignements

personnels de nos existences en ligne et pour suggérer des réponses à ces répercussions. Dans le cadre de cet engagement, le CPVP finance un programme des contributions de recherche indépendante dans les secteurs que le CPVP considère comme prioritaires chaque année. Les études déjà réalisées comprennent des travaux novateurs dans le domaine du vol d'identité ainsi qu'un examen exhaustif de l'industrie du courtage en données au Canada.

Conclusion

La transformation sociale qui a eu lieu en une seule génération grâce à Internet est stupéfiante. La quantité de nos activités en ligne augmente et leur étendue gagne en diversité, empruntant des méthodes inimaginables il y a dix ans. Ce changement comporte des bénéfices potentiels immenses quant à la promotion des communautés, à l'amélioration de la communication et à l'appui de la créativité. L'accroissement de la sensibilisation à l'égard de la protection des renseignements personnels n'a pas pour but de nous décourager de profiter du plein potentiel d'Internet. Ce qui compte, c'est que nous acquérions tous les outils nécessaires pour naviguer dans ces nouveaux mondes virtuels, d'une façon qui nous permette de profiter activement du potentiel des activités en ligne, tout en conservant un sentiment de contrôle sur leurs impacts sur nos vies, tant en ligne que hors ligne.

La Commissaire à la protection de la vie privée du Canada, M^{me} Jennifer Stoddart, exprime ses remerciements à M^{me} Kate Wilson, avocate au Commissariat à la protection de la vie privée du Canada, pour sa précieuse et indispensable collaboration dans la publication de ce texte.