Réseautage social et droit canadien en matière de protection des renseignements personnels

Compétence, conservation et divulgation

Christopher Parsons
Candidat au doctorat, Université de Victoria[i]

Mémoire présenté au Comité parlementaire de l'accès à l'information, de la protection des renseignements personnels et de l'éthique
Produit le 23 décembre 2012

Introduction

Depuis l'été 2012, je suis coenquêteur chargé d'un projet visant à examiner comment les sociétés de réseautage social se conforment aux dispositions des lois relatives à la protection de la vie privée. Nous examinons comment les attentes des sites Web et des milieux du réseautage social, dont la raison d'être est la facilitation du partage de renseignements personnels des usagers par les usagers, peuvent être conciliées avec les attentes raisonnables de la protection de la vie privée et les régimes canadiens existants qui visent à protéger les données personnelles. Cette recherche est financée par le programme de contributions du Commissariat à la protection de la vie privée du Canada. Le commissaire n'ayant pas droit de regard sur l'utilisation de ces fonds, les faits présentés au comité proviennent du travail de chercheurs indépendants et ne reflètent pas nécessairement le point du vue du commissaire.

Dans le présent mémoire, je souligne certaines de nos analyses des politiques et dispositions relatives à la protection de la vie privée de 20 sites de réseautage social relativement à la capacité des Canadiens d'accéder à leurs renseignements personnels qui sont stockés sur ces sites. Ces analyses nous aident à comprendre dans quelle mesure les entreprises fournissant ces services sont conscientes de leurs obligations juridiques et de la conservation de renseignements personnels. De plus, elles nous permettent de déterminer l'accès concret qu'ont les Canadiens aux profils établis par ces entreprises et leurs associés. Ensemble, ces analyses révèlent dans quelle mesure les sociétés de réseautage social comprennent les renseignements personnels des Canadiens, les conditions du partage des données et la facilité avec laquelle les Canadiens ont accès aux renseignements qu'ils fournissent à ces services. En guise de conclusion, je proposerai quelques façons d'encourager ces sociétés à se conformer davantage aux lois canadiennes en matière de protection de la vie privée.

Méthodologie

Dans le cadre de notre recherche, nous avons examiné une foule de services de réseautage social, et pas seulement des services bien connus comme Facebook et Twitter, qui font déjà l'objet d'une grande attention publique et réglementaire relativement à leurs pratiques concernant les renseignements personnels. Le choix des sites de réseautage social a porté sur les sites déjà adoptés par les Canadiens. Par suite d'un sondage du marché qui a évalué la popularité relative des réseaux sociaux, nous avons examiné les services suivants : Blogger (Google); Club Penguin; Facebook; Flickr (Yahoo!); Foursquare; Google+; Instagram (tout de suite après son acquisition par Facebook); LinkedIn; LiveJournal; MySpace; Nexopia; Ping (Apple); Plenty of Fish; Reddit; Tumblr; Wikimedia Foundation; Wordpress.com; World of Warcraft (Blizzard); YouTube (Google) et Zynga.

Nous avons centré notre attention sur les sociétés qui offrent des réseaux sociaux (p. ex. Twitter), et non sur celles qui offrent des applications servant à communiquer *avec* les réseaux sociaux (p. ex. Tweetdeck, une application qui permet aux particuliers d'afficher ou de lire des messages sur Twitter). Ainsi, nous avons examiné les politiques des réseaux sociaux en matière de protection de la vie privée et vérifié l'accès aux renseignements qu'ils recueillent au sujet des Canadiens; nous ne l'avons pas fait pour les applications dont se servent les Canadiens pour accéder aux services de ces entreprises.

Les éléments du projet dont il s'agit ici reposent principalement sur l'analyse documentaire. Notre équipe a analysé la teneur d'un échantillon de déclarations sur la protection de la vie privée et de politiques de divulgation de données d'entreprise et procédé à un examen juridique, politique, éducationnel et gouvernemental de ces politiques. Après avoir évalué les déclarations, nous avons constitué un modèle à partir des réseaux sociaux à l'étude et des pratiques de divulgation relatives communes découvertes durant notre évaluation initiale. Ce modèle nous a aidés à concevoir un cadre comparatif pour identifier et différencier les déclarations relatives à la protection de la vie privée et les accords de divulgation liés aux services de réseautage social à l'étude.

Notre analyse documentaire a été complétée par une analyse de l'observation de l'article 4.9 de l'annexe 1 de la loi canadienne de protection de la vie privée, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Nous avons présenté des demandes d'accès à l'information lorsque des membres de l'équipe de recherche avaient déjà des liens avec un réseau; seuls les services suivants ont fait l'objet d'un examen relatif à l'observation de l'article 4.9 de l'annexe 1 : Twitter; Facebook; LiveJournal; Ping (Apple); Tumblr; Google Domains Services; Wordpress.com; Flickr; Google+/Google Services (services non liés au domaine); LinkedIn.

On trouvera ci-dessous une description de certaines des principales constatations tirées de l'analyse des politiques des services de réseautage social en matière de protection de la vie privée; je traiterai ensuite des constatations relatives à nos demandes d'accès aux renseignements.

Politiques en matière de protection de la vie privée : compétence

Durant notre recherche, nous avons examiné les principaux réseaux sociaux utilisés au Canada et les avons analysés sous différents angles : la teneur et la visibilité de la politique; les procédures applicables à l'objet des données (en ce qui concerne l'exercice des droits relatifs à la protection de la vie privée); les demandes relatives à la définition et à la saisie de renseignements personnels identifiables (RPI); la divulgation de RPI à d'autres organisations, dont celles chargées de l'application des lois; les engagements en matière de sécurité; les engagements en matière de droits d'accès et de correction. Dans la présente section, nous examinons la mesure dans laquelle les demandes relatives ou les renvois aux politiques de protection de la vie privée sont conformes aux divers régimes juridiques nationaux et internationaux. Cette analyse donne un aperçu de ce à quoi les sociétés de réseautage social (SRS) ont explicitement accepté d'être juridiquement assujetties.

Nombre des SRS que nous avons examinées ont dit se conformer à au moins certains des régimes juridiques de protection de la vie privée nationaux ou internationaux. Cependant, des SRS comme Flickr, Instagram, Meetup, Noxopia, Reddit, Wikimedia Foundation et Wordpress, notamment, n'ont pas dit qu'elles se conformaient à un régime national ou international particulier. Cela étant dit, je tiens à souligner que lorsque nous avons communiqué avec Instagram, celle-ci a bien amorcé un dialogue à propos de l'observation des lois canadiennes de protection de la vie privée, mais elle ne s'y est jamais conformée.

En dépit les importants engagements pris par le Commissariat à la protection de la vie privée du Canada avec des réseaux sociaux étrangers comme Facebook, seul le Club Penguin, un des membres de notre groupe cible, a dit qu'il se conformait au droit canadien de protection de la vie privée. Le Club Penguin est une société canadienne qui a été achetée par Disney[ii]. La plupart des autres réseaux sociaux, notamment Blizzard[iii], Facebook[iv], Google[v], LinkedIn[vi], LiveJournal[vii], MySpace[viii], Twitter[ix] et Zynga[x], soulignent qu'ils se conforment à certaines lois américaines, comme la Child Online Privacy Protection Act (COPPA). Comme elles disent se conformer à la COPPA, ces sociétés évitent sciemment de recueillir les renseignements personnels d'enfants de moins de 13 ans; cependant, cela ne signifie pas qu'elles évitent de recueillir des renseignements *concernant* des enfants de moins de 13 ans : les parents, les enseignants et d'autres personnes qui ont des relations avec des enfants et des adolescents peuvent rendre publics des renseignements concernant ces enfants. Les mécanismes dont se servent ces réseaux pour éviter de recueillir des RPI d'enfants de moins de 13 ans sont souvent rudimentaires, ne faisant que prévenir la création d'un compte si l'intéressé choisit un âge inférieur à 13 ans lorsqu'il demande une ouverture de compte. En conséquence, beaucoup de RPI à propos de ces enfants peuvent être recueillis dans ces sites. De plus, les RPI à propos d'enfants sont recueillis lorsque ces enfants sont en mesure de choisir l'âge de 13 ans ou plus lorsqu'ils font une demande d'ouverture de compte Facebook ou Twitter.

D'autres sociétés, dont Google, Facebook, LinkedIn, LiveJournal, MySpace, Ping d'Apple, Twitter, Blizzard[xi] et Zynga, disent se conformer à U.S.-E.U. Safe Harbour et aussi au U.S.-Swiss Safe Harbour Framework. Fait à remarquer, entre le moment où nous avons examiné les politiques de ces sociétés en matière de protection de la vie privée et où nous avons rédigé le présent mémoire, MySpace a modifié son engagement envers l'accord U.S.-E.U. Safe Harbour. Sa politique se lit maintenant comme suit :

> Lorsqu'un membre se trouvant dans l'Union européenne choisit d'afficher des renseignements personnels qui seront rendus publics, ce membre doit veiller à ce que ces renseignements soient conformes à toutes les lois de protection des données applicables. Myspace n'est pas responsable, en vertu des lois de protection des données applicables de l'UE, des renseignements personnels affichés par les membres.

Les conditions qui ont causé ce changement sont encore inconnues, mais il reste qu'elles ont vu le jour au moment où l'Europe a débattu le principe du « droit à l'oubli », auquel les sociétés de réseautage social se sont largement opposées. Foursquare a adopté les principes de sphère de sécurité et informe explicitement ses visiteurs internationaux que « les gouvernements fédéraux et ceux des États, les tribunaux, les organismes chargés de l'application de la loi ou les organismes de réglementation pourraient être en mesure d'obtenir la divulgation de vos renseignements personnels aux termes des lois américaines applicables. Votre utilisation du présent site ou service ou la communication par vous de vos renseignements personnels constitueront votre consentement au transfert de vos renseignements personnels à l'extérieur de votre pays, dont les États-Unis, qui pourrait avoir des règles de protection des données différentes de celles en vigueur dans votre pays[xii] ». Cela fait effectivement de la loi américaine la loi par excellence à laquelle ces réseaux acceptent de se conformer.

Lorsque des gens se plaignent au sujet de la façon dont un de ces réseaux recueille, conserve ou traite les données personnelles, le réseau en cause cherche souvent à restreindre les instances qui peuvent être saisies des plaintes. Fréquemment, les politiques de protection de la vie privée ou les conditions de service précisent quelles instances ou quels tribunaux seront saisis des plaintes. Exception faite de Yahoo![xiii], de Nexopia[xiv] et de Plenty of Fish (un réseau social canadien de rencontre[xv]), qui reconnaissent les tribunaux canadiens, toutes les plaintes doivent être présentées à un tribunal fédéral américain ou aux tribunaux d'État de la Californie ou de New York. Seule Zynga, une société de jeux en ligne, reconnaît explicitement les instances européennes, déclarant que les citoyens non américains « accepteraient de se soumettre à la juridiction des tribunaux en matière de renseignements personnels du Luxembourg[xvi] ».

Ainsi, de façon générale, qu'a-t-on constaté? On a constaté que certaines grandes sociétés de réseautage social hésitent à adopter ou à mettre en œuvre les lois européennes ou canadiennes en matière de protection des données. Pareille hésitation peut être attribuable à des raisons économiques, comme éviter d'embaucher des avocats dans divers pays; à des raisons linguistiques, comme le fait de vouloir se défendre dans une langue que comprennent et emploient couramment les fondateurs; ou à d'autres raisons commerciales. Plus particulièrement, dans cette dernière catégorie, de grandes sociétés de réseautage social pourraient craindre que l'observation des lois sur la protection des données ou de la vie privée dans l'UE et au Canada ne nuise aux pratiques auxquelles ont recours les sociétés pour tirer des avantages commerciaux de la collecte, du traitement et de la conservation de renseignements personnels identifiables, ou ne les interdise. Ayant parlé des questions de compétence concernant les réseaux, je traiterai maintenant de la durée pendant laquelle les données sont stockées par certains de ces réseaux.

Politiques de protection de la vie privée : conservation des données

Un simple examen de la façon dont les sociétés de réseautage social disent conserver les données est révélateur. Après avoir supprimé des informations sur un compte, Google admet ne pas immédiatement détruire les données et ne pas retirer les données de ses systèmes de sauvegarde[xvii]. Pareil aveu est inquiétant compte tenu des problèmes de conservation à long terme relatifs aux données de Street View data où les périodes de conservation restent ambiguës[xviii]. Alors que Facebook déclare prendre normalement un mois pour supprimer les données — une partie des renseignements restant dans les registres de sauvegarde jusqu'à 90 jours — la destruction réelle des données, comme les photos téléchargées sur le site, a longtemps été discutable[xix]. Des sociétés comme Yahoo! et Foursquare offrent des engagements semblables à ceux de Facebook. Foursquare souligne aussi que même après la destruction de renseignements des abonnés « il est possible que des copies de ces renseignements soient toujours accessibles ailleurs, s'ils ont été partagés avec d'autres, distribués conformément aux critères de protection de la vie privée, copiés ou stockés par d'autres usagers[xx] ». Tumblr déclare la même chose, informant les abonnés que même si les données de leurs comptes sont détruites, les activités publiques, comme l'affichage de messages « j'aime » ou le partage, resteront stockées sur des serveurs et seront accessibles au public[xxi].

Pour d'autres services, la « suppression » des données des abonnés peut largement se

résumer à la dissimulation des renseignements pour le public. LiveJournal, par exemple, reconnaît que, si les abonnées peuvent détruire leurs comptes et l'information les concernant, il peut s'écouler un certain temps avant les données soient vraiment détruites, et la société peut choisir de conserver les informations le temps voulu pour protéger ses intérêts commerciaux, se conformer à des ordonnances des tribunaux, etc[xxii]. Cet emploi du terme « etc. » laisse la porte ouverte à toutes les motivations possibles pour conserver les données en contravention avec la demande de l'abonné. Chez Meetup, on se réserve le droit de conserver des renseignements dont un usager a demandé la suppression si la conservation est nécessaire pour régler un différend, résoudre un problème ou appliquer les conditions de service. Quoi qu'il soit, la société assure que « vos renseignements ne sont jamais complètement supprimés de nos bases de données en raison de contraintes techniques ou juridiques (par exemple, nous n'enlèverons pas vos renseignements de nos banques de sauvegarde)[xxiii] ». Nexopia offre des critères semblables à ceux de Meetup en ce qui concerne la suppression de renseignements personnels, en stipulant que les abonnés ne devraient pas s'attendre à ce que leurs renseignements personnels soient complètement retirés de ses systèmes après une demande de destruction[xxiv].

Compte tenu que nombre de ces services servent de plateformes permettant à des développeurs externes de saisir, de traiter et de conserver les données produites par les usagers, il est possible que les données « supprimées » d'une plateforme (p. ex. Facebook, Twitter, LinkedIn, Foursquare) soient conservées indéfiniment par des tiers, laissant la plateforme incapable de faire respecter la demande de suppression de l'usager par le tiers. Des sociétés comme Club Penguin, Yahoo!, Google et Apple se réservent le droit de partager des renseignements recueillis on donnés au sein de leur organisation, et la plupart des réseaux sociaux comprennent des dispositions en vertu desquelles ils « peuvent » (et ne manquent pas de le faire) partager des renseignements avec des sociétés d'analyse et des annonceurs associés. En fait, lorsque nous avons examiné les services de réseautage social utilisant Ghostery, un outil servant à identifier les outils de surveillance de sites Web, nous avons constaté que tous les services, exception faite de Facebook et de Google, utilisaient des services analytiques et publicitaires de tiers. Facebook et Google, évidemment, ont leurs propres services analytiques et publicitaires en aval et n'ont pas besoin de recourir à ceux de tiers.

Que peut-on en conclure? Simplement que ces sociétés offrent rarement des façons fiables de supprimer des renseignements une fois que ceux-ci ont été ajoutés à leurs services de réseautage social. En conséquence, les personnes qui trouvent leurs renseignements personnels dans ces réseaux – qu'elles les y aient mis elles-mêmes ou qu'un tiers l'ait fait – ont une capacité limitée de les retirer. Ainsi, bien qu'elles aient conçu des systèmes complexes pour miner les données pour la publicité, la lutte contre la violation du droit d'auteur et nuire aux moyens de prévention, les sociétés qui fournissent ces services ne se sont pas encore dotées d'outils plus que rudimentaires afin de permettre aux usagers d'enlever en toute confiance leurs données des serveurs et des systèmes des sociétés.

Importantes découvertes sur l'accès

Nous avons, en outre, demandé aux diverses SRS de nous fournir les dossiers complets de l'information qu'elles détiennent sur les membres de notre équipe de recherche. De toutes les sociétés avec lesquelles nous avons communiqué, seules Facebook, Twitter, Google,

Instagram, LinkedIn ou Tumblr ont répondu d'une manière ou d'une autre. Ces sociétés ont choisi de fournir des informations incomplètes, refusé de fournir toute information ou fourni uniquement l'information de base donnée par les abonnés.

Facebook offre certes aux usagers la possibilité d'autotélécharger leurs propres renseignements, mais cette possibilité est largement le résultat des pressions exercées par la campagne publique « Europe c. Facebook ». Cette initiative visait à améliorer la « transparence » de Facebook pour ses usagers, aussi bien qu'à accroître le « contrôle » des renseignements personnels des usagers sur la plateforme de Facebook, notamment ceux se trouvant à l'extérieur de la compétence juridique des États-Unis[xxv]. Europe c. Facebook a servi de fondement au rapport du commissaire de la protection des données de l'Irlande sur les principes de collecte et de conservation des données, menant à un changement majeur de la politique d'utilisation des données de Facebook, dont l'établissement de l'outil d'autotéléchargement[xxvi].

Bien que l'outil d'autotéléchargement donne accès aux abonnés à certaines des données que Facebook recueille, utilise et traite, une bonne partie des données – notamment les métadonnées – restent inaccessibles aux usagers. Des tests d'analyse de réseaux réalisés par Privacy International révèlent davantage de données recueillies par Facebook sur les usagers que celles auxquelles ont accès les usagers à l'aide de l'outil de téléchargement. Parmi les données recueillies sur les usagers de Facebook qui sont exclues de l'outil de téléchargement, on compte : les données d'entrée en communication des usagers; l'adresse IP et le fournisseur d'accès Internet; le contenu affiché dans d'autres pages d'usager; les métadonnées liées aux vidéos; les données d'information sur les messages d'usager « j'aime »; l'information des fureteurs; l'information concernant l'interaction des usagers avec les publicités; l'information recueillie par « retraçage de conservation »; l'information qui indique une relation avec d'autres usagers; l'information sur les images auxquelles les usagers étaient liés, mais ne le sont plus; « l'information de suivi » que Facebook recueille sur l'interaction des usagers avec d'autres sites Web; les compilations de recherches par la fonction « recherche » de Facebook; l'information sur les réglages du fil de nouvelles; l'information sur les « click-flows » et les visites d'usager aux pages individuelles de la plateforme; l'information sur l'utilisation de données personnelles dans la fonction « recherche d'amis »; la divulgation des utilisations des données des usagers dans les processus « d'assortiment » liés au ciblage de publicités ou à la reconnaissance des visages; l'information sur l'utilisation des images pour le nouvel outil de « reconnaissance des visages » de Facebook ou de toutes autres données biométriques pouvant être utilisées pour identifier des usagers; les données que Facebook recueille sur les usagers (p. ex. les numéros de téléphone) lorsque d'autres usagers du réseau « synchronisent » un appareil (p. ex. un iPhone) avec l'information recueillie par Facebook; l'information recueillie sur les relations des usagers avec d'autres usagers (amis, frères, etc.); l'information sur les « invitations » à des groupes, à des événements ou à des pages que des usagers ont envoyés à des amis de leur réseau[xxvii].

Twitter, de même, donne accès à certaines informations, mais retient une quantité considérable de métadonnées. La divulgation par Twitter de RPI repose grandement sur la confirmation de l'identité. Les abonnés demandent d'abord une copie de tous leurs renseignements. On leur demande ensuite d'ouvrir un ticket chez Twitter, après quoi on leur demande d'envoyer ce qui suit : une déclaration autorisant la divulgation des

informations demandées; une déclaration renfermant le numéro du ticket; un document renfermant le code d'usager de l'abonné; l'adresse électronique que Twitter a dans les dossiers relatifs au compte; une copie numérisée de la carte d'identité avec photo délivrée par le gouvernement. Après la communication de ces informations, Twitter fournit une copie téléchargeable des renseignements de l'usager. Toutes les informations renferment un condensé pour veiller à ce que les données fournies correspondent aux données stockées dans la base de données de Twitter. Le problème, toutefois, c'est que Twitter ne fournit pas toutes les métadonnées à l'usager. Les cinq lignes suivantes montrent l'information fournie à l'usager pour un seul tweet :

> code d'usager : 14087212
> créé le : Thu Mar 06 06:03:10 +0000 2008
> créé via : le web
> numéro de statut : 767404918
> texte : apprenons-en sur Twitter

Comparons des cinq lignes avec la liste de tous les champs et de toutes les métadonnées qui sont associés avec un tweet de 2010 – 59 ou 60 lignes d'informations : le numéro d'identification du tweet; le texte du tweet; la date de création du tweet; le numéro d'identification du tweet auquel on répond; le nom de l'écran et le numéro d'identification de celui à qui on répond; la question de savoir si le tweet a été ajouté aux favoris; la question de savoir si le tweet a été limité à 140 caractères; le code d'usager de l'auteur; le nom d'usager de l'auteur; le nom d'écran de l'auteur; la biographie de l'auteur; l'URL de l'auteur; le lieu où se trouve l'auteur; l'information de rendu du tweet; la date de création du compte; la question de savoir si le compte permet les contributions; le nombre de tweets que l'usager a ajoutés à ses favoris; le nombre d'usagers que suit l'auteur; le fuseau horaire de l'usager et le décalage horaire; le nombre de tweets affichés par l'usager; la langue de l'usager; la question de savoir si le compte de l'usager est protégé ou non; le nombre d'usagers suivant le compte de l'auteur; la question de savoir si l'usager a activé la géolocalisation; localisation de numéros d'identification; le numéro d'identification de contribution de l'usager, s'il en a un; l'URL pour obtenir un polygone détaillé pour la localisation; les noms imprimables du lieu; le lieu associé au tweet; genre de lieu (p. ex. un quartier ou une ville); le pays où se trouve le lieu; CSS pour le lieu; l'application qui a envoyé le tweet[xxviii]. L'hésitation de Twitter à fournir toutes les métadonnées a poussé un citoyen canadien à porter plainte au Commissariat à la vie privée du Canada; l'affaire n'a pas encore été résolue[xxix].

À l'instar de Facebook et de Twitter, Google offre un service de téléchargement par l'entremise du « Data Liberation Front ». Après avoir demandé des données en remplissant un formulaire automatisé à l'aide de l'outil fourni – qui oblige les usagers à demander des données discrètes à d'importants services de Google plutôt qu'un téléchargement de toutes les informations liées à un compte Google – les données sont fournies dans une grande variété de formats, selon le genre de données. L'information sur les contacts est formatée de manière à incorporer les programmes de carnets d'adresses, les discussions sur Google+ et les « +1s » sont fournis strictement en HTML, et la page du profil est en JSON. Cela permet certes un meilleur formatage lisible par machine des données que celui offert par certains autres services, mais on n'y trouve toujours pas toutes les métadonnées : l'adresse IP n'y est pas, le lieu (le cas échéant) n'y est pas, etc[xxx].

De façon générale, les métadonnées constituent, en soi, du contenu. Elles peuvent renfermer de l'information de géolocalisation, de l'information sur les réseaux sociaux et les habitudes de communication en général qui ne sont pas attestées dans une seule déclaration, des tweets ou des messages sur Facebook. Elles peuvent révéler l'activité d'un usager dans tout réseau social et les moments où il exerce cette activité, aussi bien l'affluence relative fondée sur les appareils utilisés pour communiquer avec le réseau social, le niveau technique fondé sur les logiciels employés par l'usager et elles peuvent être utilisées en conjonction avec les métadonnées d'autres usagers à des fins de minage de données commerciales. En conséquence, compte tenu que les métadonnées constituent souvent de l'information personnelle, ces sociétés ne rendent pas pleinement compte des données personnelles associées produites par les usagers.

LinkedIn, Instagram et Tumblr ont tous répondu lorsque nous avons demandé accès à nos renseignements personnels. Malheureusement, les données n'ont pas été fournies. LinkedIn et Instagram ont toutes deux engagé une discussion avec nous - LinkedIn a ouvert un ticket et Instagram a négocié la fourniture d'informations – mais aucune des deux ne nous a jamais donné les informations personnelles que leur réseau avait recueillies, utilisées ou traitées sur nous. Le personnel du contentieux de Tumblr a déclaré que la société « ne fournira pas les informations que vous avez demandées. Tumblr est une société établie aux États-Unis ayant son siège social à New York. Elle n'a pas de bureau officiel au Canada et, par conséquent, elle n'est pas assujettie à la LPRPDE ni au Commissariat à la protection de la vie privée du Canada ». Par la suite, après que nous eûmes expliqué de nouveau les obligations de la société en vertu de la LPRPDE, la société a réitéré : « Nous vous remercions de l'intérêt que vous portez à une discussion juridique sur la portée de la LPRPDE, mais nous tenons à vous dire que notre avis n'a pas changé[xxxi]. » L'obligation énoncée de s'adresser aux tribunaux de New York est intéressante, compte tenu que la politique de Tumblr en matière de protection de la vie privée reconnaît uniquement le Code civil de la Californie (art. 1798.83-1798.84) et confirme que les habitants de la Californie sont en droit de demander des informations relativement aux catégories de données des usagers que la société partage avec des sociétés affiliées et des tiers[xxxii].

En plus des difficultés rencontrées dans l'accès à leurs données personnelles, les abonnés à ces services peuvent être aux prises avec des problèmes lorsqu'ils alertent une société de réseautage social au sujet de leurs préoccupations quant à la façon dont la société retient, traite ou divulgue leurs renseignements personnels. De toutes les sociétés de notre échantillon, seules trois - Plenty of Fish, Reddit et World of Warcraft – ont publié l'information de contact des agents de la protection de la vie privée. La plupart des autres sociétés avaient des formulaires de contact ou des processus de résolution plutôt ambigus. Peu de sociétés avaient des processus de résolution ou de traitement des plaintes clairs. Cela étant dit, deux services, LiveJournal et MySpace, reconnaissent le caractère unique des usagers de l'UE, la première offrant une adresse postale dans l'UE pour les plaintes, et la seconde, invitant les Européens à présenter leurs questions à l'aide du formulaire en ligne de la société ou par la poste. Tumblr se démarque aussi, son adresse postale publiée étant destinée uniquement aux habitants de la Californie[xxxiii]. Seule Instagram ne disposait d'aucun mécanisme de traitement des plaintes. Cependant, une recherche plus poussée a révélé que son personnel était disposé à discuter, voire à agir, relativement à des préoccupations liés aux renseignements personnels. Les processus d'Instagram en matière

de traitement de ce genre de demandes pourraient changer avec le temps, compte tenu de son acquisition récente par Facebook.

En somme, que peut-on dire au sujet des abonnés et de leur accès aux renseignements personnels que ces services conservent? D'abord, on peut dire qu'il peut être incroyablement difficile d'accéder à ses renseignements personnels. Exception faite de la divulgation limitée d'informations faite par Facebook, Twitter et Google, l'accès à l'ensemble de vos informations nécessiterait une plainte officielle au Commissariat à la protection de la vie privée du Canada. Le fait de devoir recourir à un ombudsman gouvernemental pour obtenir le retrait de renseignements personnels semble être une obligation exagérée. De plus, même lorsque des données ont été fournies, leur nombre était limité puisque, dans les faits, il manquait toutes les métadonnées liées aux communications avec les réseaux sociaux. Par ailleurs, des sociétés comme Tumblr exposent explicitement leur rejet de toute loi non américaine. Enfin, le simple fait de tenter de porter plainte à propos des services – ou de communiquer avec un agent de la protection de la vie privée au sujet de la façon dont les renseignements personnels sont recueillis et téléchargés par un abonné – est difficile, compte tenu de l'absence relative de mécanismes de traitement des plaintes efficaces. Pareil niveau élevé de friction dans l'accès à ses renseignements personnels en dit long sur les pratiques de ces sociétés, compte tenu que ces dernières prétendent promouvoir un partage (relativement) sans friction des renseignements personnels. Tout se passe comme si, lorsque des abonnés veulent savoir quels sont tous les renseignements personnels qui sont stockés dans les serveurs d'une société de média social, la société complique la tâche des usagers voulant accéder à leurs renseignements personnels, allant même parfois jusqu'à leur interdire l'accès. La situation est si tendue qu'il semble que la *seule* façon pour les abonnés de savoir quels renseignements personnels recueillent les sociétés consiste à recourir à un ombudsman national, ce que peu de citoyens ont envie de faire.

Conclusion

Dans le présent mémoire, nous avons présenté les facteurs qui, comme le reconnaissent explicitement les sociétés de réseautage social, influent juridiquement sur les aspects de leurs services liés à la protection de la vie privée et de la conservation des données. Qui plus est, lorsque nous avons examiné l'observation de la divulgation de données relativement aux données recueillies sur les Canadiens, nous avons constaté que les sociétés présentent des carences, voire qu'elles sont carrément négligentes. En somme, la présente étude révèle que ces sociétés ne prêtent aucune attention au Canada et à ses lois sur la protection de la vie privée.

Sur le plan juridique, peu de sociétés reconnaissent le besoin de se conformer spécifiquement aux lois canadiennes, ce qui pourrait contribuer à leur piètre comportement. En outre, en ce qui concerne la destruction de données, l'article 4.5.3 de la LPRPDE prévoit : « On devrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées. Les organisations doivent élaborer des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels. » Compte tenu des vagues engagements en matière de destruction de données qu'offrent la plupart de ces sociétés, les politiques de conservation et de destruction de données qu'elles ont conçues ne renferment pas de directives claires quant à la suppression

de données. Une ligne de conduite est nécessaire à cet égard; les sociétés doivent savoir à quoi ressemble un bon modèle de destruction de données et quel régime serait conforme aux lois canadiennes. En ce qui concerne la loi canadienne sur la protection de la vie privée, lorsque les sociétés nous ont fourni les données personnelles que nous avions demandées, elles en ont omis un certain nombre; les métadonnées *doivent* être reconnues comme étant des renseignements personnels identifiables, sinon les Canadiens ignoreront toujours toute l'étendue des données que recueillent les réseaux sociaux et comment ils les utilisent.

Le comité devrait, idéalement, songer à des façons de renforcer les lois canadiennes en matière de protection de la vie privée de manière à forcer les sociétés étrangères à respecter nos lois lorsqu'elles conçoivent et déploient leurs services. Il ne s'agit pas de renforcer les lois au point de nuire à l'innovation. Il s'agit plutôt d'encourager un développement rapide conforme aux lois canadiennes sur la protection de la vie privée. Il pourrait suffire d'imposer des sanctions administratives aux sociétés qui violent sciemment nos lois sur la protection de la vie privée, ou alors ces sociétés pourraient être tenues de faire une déclaration claire quant aux processus de conservation et de destruction des données offrant un mode défini de retrait des données hébergées par les services de réseautage social. Les métadonnées recueillies par ces services pourraient être considérées comme des renseignements personnels identifiables et, ainsi, justifier les efforts déployés par les Canadiens pour accéder à toutes les informations que ces services recueillent à leur égard. En rehaussant la stature relative du pays aux yeux des SRS, on pourrait favoriser l'émergence d'une série d'options de services plus respectueuses de la protection de la vie privée – et qui refléteraient mieux la façon dont ces systèmes devraient fonctionner – , révélant une fois de plus la capacité du Canada d'influer sur le développement d'outils populaires et très utilisés de manière constructive touchant non seulement les Canadiens, mais encore l'ensemble des usagers de ces services dans le monde.

CITATIONS

[i] L'auteur tient à remercier Joyce Parsons de son aide à la rédaction du présent mémoire.
[ii] « Club Penguin Privacy Policy », modifié la dernière fois le 11 janvier 2012, http://www.clubpenguin.com/privacy.htm.
[iii] « Blizzard Entertainment® Online Privacy Policy », modifié la dernière fois le 25 mars 2011, http://us.blizzard.com/en-us/company/about/privacy.html.
[iv] « Facebook Data Use Policy », modifié la dernière fois le 8 juin 2012, http://www.facebook.com/full_data_use_policy.
[v] « Google Privacy Policy », modifié la dernière fois le 27 juillet 2012, http://www.google.ca/intl/en/policies/privacy/.
[vi] « LinkedIn Privacy Policy », mis à jour la dernière fois le 16 juin 2011, http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv.
[vii] « LiveJournal Privacy Policy », modifié la dernière fois le 12 décembre 2010, http://www.livejournal.com/legal/privacy.bml.
[viii] « MySpace Privacy Policy », mis à jour la dernière fois le 1er octobre 2012,
[viii] http://www.myspace.com/Help/Privacy.
[ix] « Twitter Privacy Policy », modifié la dernière fois le 17 mai 2012, http://twitter.com/privacy.
[x] « Zynga Privacy Policy », modifié la dernière fois le 30 septembre 2011, http://company.zynga.com/privacy/policy.

[xi] « Blizzard Entertainment® Online Privacy Policy »,
[xii] https://foursquare.com/legal/privacy.
[xiii] « Yahoo! Privacy Policy », modifié la dernière fois le 23 avril 2010, http://info.yahoo.com/privacy/ca/yahoo/.
[xiv] "Nexopia Privacy Policy," modifié la dernière fois le 2 novembre 2009, http://www.nexopia.com/privacy.
[xv] « Plenty of fish Terms of Use Agreement », mis à jour la dernière fois le 2 novembre 2011, http://www.pof.com/terms.aspx.
[xvi] « Zynga Privacy Policy », modifié la dernière fois le 30 septembre 2011, http://company.zynga.com/privacy/policy.
[xvii] « Google Privacy Policy », modifié la dernière fois le 27 juillet 2012, http://www.google.ca/intl/en/policies/privacy/.
[xviii] Vinograd, Cassandra et Raphael Satter. 2012. « Google: Didn't delete Street View data after all », *Yahoo! News*, 27 juillet. Consulté le 17 octobre 2012. http://news.yahoo.com/google-didnt-delete-street-view-data-175540701--finance.html.
[xix] Cheng, Jacqui. 2012. « Three years later, deleting your photos on Facebook now actually works », *Ars Technica*, 16 août. Consulté le 17 octobre 2012. http://arstechnica.com/business/2012/08/facebook-finally-changes-photo-deletion-policy-after-3-years-of-reporting/.
[xx] « Foursquare Labs, Inc. Privacy Policy », mis à jour la dernière fois le 13 juillet 2012. https://foursquare.com/legal/privacy.
[xxi] « Tumblr Privacy Policy », mis à jour la dernière fois le 22 mars. http://www.tumblr.com/policy/en/privacy.
[xxii] « LiveJournal Privacy Policy », mis à jour la dernière fois le 12 décembre. http://www.livejournal.com/legal/privacy.bml.
[xxiii] « Meetup Privacy Policy Statement », mis à jour la dernière fois le 23 mai. http://www.meetup.com/privacy/.
[xxiv] « Nexopia Privacy Policy », mis à jour la dernière fois le 2 novembre 2009. http://www.nexopia.com/privacy.
[xxv] « Our Group », Europe c. Facebook, consulté le 13 novembre 2012 http://europe-v-facebook.org/FAQ_ENG.pdf.
[xxvi] « Facebook told to stop indefinitely holding users' advertising data », Charles Arthur, The Guardian, 21 décembre 2011, http://www.guardian.co.uk/technology/2011/dec/21/facebook-advertising-data?newsfeed=true.
[xxvii] « Facebook's information access feature still violates European law », Simon Davies, Privacy International, 22 octobre 2001. https://www.privacyinternational.org/blog/facebooks-information-access-feature-still-violates-european-law.
[xxviii] Pour voir cette information dans un format visuel, se reporter à : Christopher Parsons. (2010). « Twitter, Mobile Browsers, and Metadata Privacy », *Technology, Thoughts, and Trinkets* (blogue). Publié le 22 avril 2010. Consulté la dernière fois le 13 novembre 2012, http://www.christopher-parsons.com/blog/technology/twitter-mobile-browsers-and-metadata-privacy/.
[xxix] Fondé sur la correspondance personnelle entre Christopher Parsons et le plaignant.
[xxx] Jusqu'à maintenant, aucune analyse de l'ensemble du trafic des métadonnées de Google n'a été réalisée. Pour ce faire, il faudrait recourir à une « attaque de l'homme du milieu »

afin de décrypter les données transmises entre Google et un ordinateur client. Pareille attaque dépasse la portée de notre projet de recherche.

[xxxi] Michael Sussmann, correspondance électronique personnelle avec Christopher Parsons.

[xxxii] « Tumblr Privacy Policy », mis à jour la dernière fois le 22 mars. http://www.tumblr.com/policy/en/privacy.

[xxxiii] « Tumblr Privacy Policy », mis à jour la dernière fois le 22 mars. http://www.tumblr.com/policy/en/privacy.