



Commissariat
à la protection de
la vie privée du Canada

Office of the
Privacy Commissioner
of Canada

**CONSULTATIONS DE 2010
SUR LA PROTECTION DE
LA VIE PRIVÉE DES
CONSOMMATEURS**

**2010 CONSUMER
PRIVACY
CONSULTATIONS**



ÉBAUCHE

Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne, et l'informatique dans les nuages

À DES FINS DE COMMENTAIRES

Table des matières

Avant-propos	1
Sommaire	2
Préambule	4
Le monde de Louise et David	5
I. Introduction	5
I.I. Protection de la vie privée au Canada	6
I.II Nouvelles technologies, anciennes questions	6
I.III Est-ce que les outils dont nous disposons actuellement seront suffisants pour protéger la vie privée à l’avenir?	8
Suivi, profilage et ciblage en ligne	11
II. Qu’est-ce que le suivi, le profilage et le ciblage en ligne?	12
II.I Ce que nous avons appris	13
II.II Points de vue des Canadiens	15
II.III Questions générales liées à la protection de la vie privée	17
II.IV LPRPDE — Principes de la protection de la vie privée	25
Informatique dans les nuages	39
III. En quoi consiste l’informatique dans les nuages?	39
III.I Ce que nous avons appris	40
III.II LPRPDE — Principes de la protection de la vie privée	42
Sommaire des questions à commenter	53
Suivi, profilage et ciblage en ligne	53
Informatique dans les nuages	54
Conclusion	55
Notes en fin de texte	56

Avant-propos

Au début de 2010, le Commissariat à la protection de la vie privée a amorcé un processus de consultation sur le suivi, le profilage et le ciblage en ligne, et l'informatique dans les nuages. Notre objectif était de souligner les tendances technologiques en évolution et de sensibiliser le public et les intervenants aux incidences du monde virtuel sur la protection de la vie privée. Je crois que les consultations étaient un premier pas positif vers la réalisation de cet objectif.

Au nom du Commissariat, j'aimerais remercier les associations, les organisations, les défenseurs d'intérêts, les universitaires et les personnes qui ont pris le temps de nous présenter des observations écrites ou qui ont participé aux événements publics. Nous leur savons gré de l'intérêt qu'ils portent à ces questions de politiques publiques importantes et sommes heureux de connaître leurs points de vue sur le sujet.

J'aimerais également remercier les employés du Commissariat pour leurs efforts assidus et leur dévouement dans ce dossier. Je tiens tout particulièrement à souligner le travail de l'ancienne commissaire adjointe à la protection de la vie privée (LPRPDE), Elizabeth Denham, le directeur, Recherche, sensibilisation et engagement, Colin McKay, la directrice, Politiques et affaires parlementaires, Ann Goldsmith, l'analyste principale de la recherche, Melanie Millar-Chapman, pour le leadership dont ils ont fait preuve tout au long de ce processus. J'aimerais également remercier l'analyste de la recherche, Barbara Bucknell, qui a rédigé le présent document.

La présente ébauche de rapport sur les consultations vise à résumer ce que nous avons entendu, ce que nous croyons et les sujets pour lesquels nous aimerions obtenir davantage de commentaires de l'industrie, des consommateurs ou d'autres intervenants, et les aspects sur lesquels nous voulons axer nos futurs travaux. Nous espérons poursuivre le dialogue amorcé au printemps dernier et nous accueillerons avec plaisir tout commentaire additionnel sur le présent rapport.

La commissaire à la protection de la vie
privée du Canada,

Jennifer Stoddart

Octobre 2010

Sommaire

Au printemps 2010, le Commissariat à la protection de la vie privée du Canada a tenu des consultations sur le suivi, le profilage et le ciblage en ligne, et l'informatique dans les nuages. En tout, le Commissariat a reçu 32 observations écrites et organisé 3 événements publics à Toronto, Montréal et Calgary, auxquels ont pris part des représentants d'autres commissariats à la protection de la vie privée, des représentants de l'industrie, des universitaires, des défenseurs d'intérêts et des membres du public.

En ce qui a trait au suivi, au profilage et au ciblage en ligne, les mémoires portaient principalement sur la publicité comportementale : en quoi celle-ci consiste-t-elle, quels sont les avantages et les risques qu'elle présente et quelles mesures d'autoréglementation sont en vigueur. Bon nombre de répondants et de participants ont soulevé diverses questions relatives à la protection de la vie privée en ce qui concerne le suivi, le profilage et le ciblage en ligne. Pour ce qui est des préoccupations générales liées à la protection de la vie privée, le manque de distinction claire entre les domaines public et privé et les répercussions que cela entraîne sur la réputation étaient perçus comme une question importante. Les activités des enfants en ligne et la nécessité d'intégrer la protection de la vie privée aux programmes de citoyenneté numérique étaient également au nombre des préoccupations soulevées.

Les consultations offraient également l'occasion d'examiner la pratique du suivi, du profilage et du ciblage en ligne dans le cadre de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). La plupart des participants de l'industrie considéraient que la LPRPDE pouvait répondre à l'environnement technologique changeant, mais bon nombre de répondants et de participants ont mentionné certains défis liés à l'application de la *Loi*. On a souligné que la définition de « renseignements personnels », la détermination de la forme de consentement appropriée, la limitation de l'utilisation des renseignements personnels, la mise en œuvre de mesures de protection raisonnables, la prestation d'un accès et de mesures de correction et la responsabilisation étaient des questions relatives à la LPRPDE auxquelles il fallait prêter une attention particulière. En général, les gens en savent encore très peu sur le suivi, le profilage et le ciblage en ligne, et la plupart des répondants et des participants convenaient qu'une plus grande transparence s'imposait dans l'intérêt des personnes et pour assurer l'innovation.

Le Commissariat cherche à obtenir des commentaires précis de la part d'intervenants sur la distinction entre les domaines public et privé, les activités des enfants en ligne, le consentement valable et d'autres utilisations du suivi, du profilage, et du ciblage en ligne. Il propose également de mener des activités particulières sur le suivi, le profilage et le ciblage en ligne, notamment des activités de recherche et de sensibilisation.

Le Commissariat en a appris davantage sur les différentes caractéristiques et les modèles de l'informatique dans les nuages. Il a entendu parler des avantages et des risques que cette technologie présente pour les entreprises et les consommateurs. Comme il a été mentionné précédemment, la plupart des répondants et des participants considéraient que la LPRPDE pouvait répondre aux problèmes liés à l'informatique dans les nuages, mais d'autres suggéraient que des mesures additionnelles s'imposaient. La plupart des questions relatives à la LPRPDE concernaient les champs de compétences et l'accès des tiers aux renseignements personnels, les mesures de protection, les nouvelles utilisations des renseignements personnels, leur conservation et leur accès.

Le Commissariat cherche à obtenir des commentaires précis d'intervenants sur la protection des renseignements personnels dans le contexte de l'informatique dans les nuages. Il propose également de mener certaines activités, principalement dans le but sensibiliser les personnes et les petites et moyennes entreprises aux questions liées à la protection de la vie privée dans le cadre de l'informatique dans les nuages.

La date limite pour la présentation d'observations sur le sujet a été repoussée au **10 décembre 2010**.

Préambule

Pour préparer les discussions dans le cadre des consultations de 2010 sur la protection de la vie privée des consommateurs tenues par le Commissariat à la protection de la vie privée du Canada, nous avons élaboré des scénarios illustrant des activités de la vie quotidienne des Canadiens. Le but était de rendre plus concrets les concepts souvent techniques et abstraits du suivi et du profilage en ligne ainsi que de l'informatique dans les nuages pour les Canadiens. Nous souhaitons ainsi que les particuliers, les représentants de l'industrie et les défenseurs de la protection des renseignements personnels amorcent un dialogue sur la façon dont les activités quotidiennes en ligne influent sur la vie privée des Canadiens et ce qui est fait et ce qu'il faudrait faire pour protéger ces renseignements. Ces scénarios seront utilisés tout au long du rapport.

Remarque : Les noms de marque de sites populaires sont utilisés dans le présent rapport pour simplifier sa lecture. Il n'est nullement question ici de commenter les pratiques sur la protection des renseignements personnels de ces sites ou de formuler des suggestions à cet égard.

Le monde de Louise et David

Louise est une étudiante postsecondaire branchée de 21 ans, qui aime rencontrer de gens et essayer de nouvelles choses. Elle est active en ligne, où elle fait à peu près tout : acheter des vêtements à la mode et des billets de spectacle, garder le contact avec ses amis et afficher des mises à jour et des photos d'elle sur sa page Facebook. Comme elle termine ses études cette année, Louise a commencé à se chercher un emploi. Elle paie sa scolarité en fabriquant des bijoux et en les vendant en ligne. Elle collectionne également des bandes dessinées et fait partie d'un réseau international d'amateurs de bandes dessinées. Louise a un jeune frère, David, âgé de 9 ans. David aime les jeux en ligne. Il s'y inscrit lui-même, mais utilise la carte de crédit de sa sœur pour effectuer des achats.

Parfois, Louise se demande ce que ces entreprises en ligne font des renseignements qu'elle leur donne. Elle a déjà entendu l'expression « protection des renseignements personnels en ligne », mais elle ne sait pas trop ce que cela signifie. Elle a déjà remarqué un lien vers une politique sur la protection des renseignements personnels sur un site Web. Elle a suivi le lien, essayé de lire la politique, mais cela l'a ennuyée. Il ne semblait s'agir que de jargon juridique. Elle a cessé de lire et poursuivi ses activités.

I. Introduction

Louise et David sont des Canadiens typiques. Ils comptent parmi les millions de Canadiens qui utilisent Internet tous les jours pour faire des achats, discuter, jouer à des jeux ou, comme Louise, faire des affaires. Ils perçoivent les avantages de la vie virtuelle et, comme ils sont jeunes, ils ont intégré l'univers virtuel à leur monde réel. Ils ne se rappellent pas l'époque où l'on utilisait des dossiers papier, des machines à écrire et des cartes routières en papier, et où l'on faisait la file pour acheter des billets de cinéma. Ils vivent une existence sur demande et disposent d'un accès instantané à un vaste éventail de renseignements : ce que leurs amis font, où ils peuvent trouver la meilleure affaire et qui est la petite amie de leur vedette de rock préférée. Ils mènent leur vie sociale en ligne, téléchargent leurs photos, vidéos et opinions et ont le sentiment de faire partie d'une communauté planétaire. Éventuellement, s'ils sont assez âgés, ils paient leurs factures, présentent des demandes de crédit ou gèrent des entreprises. Ils peuvent se procurer des chansons, des vidéos, des films, des livres, des vêtements, des journaux et des jeux avec un seul clic de la souris, le plus souvent gratuitement, du moins sur le plan monétaire. Les Canadiens de tous âges comprennent l'utilité de la technologie (le côté pratique, la connectivité et la créativité) et l'adoptent avec enthousiasme.

Cependant, cela ne signifie pas que les Canadiens comme Louise ne se demandent jamais ce qui se cache derrière leurs activités sur le Web. Où les renseignements sont-ils acheminés? Qui les examine? Louise cherche des réponses à ces questions, mais elle constate que les renseignements sont difficiles à trouver ou qu'ils sont confus et plus complexes qu'elle ne le croyait. Louise croit peut-être qu'il lui manque une vue d'ensemble. Mais où peut-elle aller pour en savoir davantage? Elle se dit que la technologie est si facile à utiliser, alors pourquoi faut-il que ce soit si ardu de comprendre la façon dont ses renseignements personnels sont utilisés?

I.I. Protection de la vie privée au Canada

Heureusement pour Louise, il existe au Canada des lois sur le traitement des renseignements personnels ainsi qu'un commissariat qui aide à assurer le respect de ces règles. Le mandat du Commissariat à la protection de la vie privée du Canada est de surveiller le respect de la *Loi sur la protection des renseignements personnels*, qui porte sur les pratiques de traitement des renseignements personnels utilisées par les ministères et les organismes fédéraux, et de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), la loi fédérale sur la protection des renseignements personnels dans le secteur privé. La LPRPDE vise les organisations qui recueillent, utilisent et communiquent des renseignements personnels dans le cadre de leurs activités commerciales (sauf s'il existe une loi provinciale essentiellement similaireⁱ). Elle vise également les renseignements personnels des clients et des employés des entreprises fédérales. De façon générale, la LPRPDE régit les pratiques de traitement des renseignements personnels des organisations du secteur privé qui effectuent des activités de suivi, de ciblage et de profilage en ligne, et qui ont recours à l'informatique dans les nuages.

Le Commissariat a pour mission de protéger et de promouvoir le droit des personnes à la vie privée. Pour ce faire, le Commissariat cherche des occasions de promouvoir la sensibilisation et l'éducation du public à l'égard des droits et des obligations en matière de protection de la vie privée en nouant le dialogue avec des institutions et des organismes du gouvernement fédéral, le secteur privé, un vaste éventail d'intervenants concernés et le public en général. Si Louise le voulait, elle pourrait se rendre sur notre site Web et téléphoner au Commissariat pour poser des questions ou déposer une plainte si elle était préoccupée par les agissements d'une des entreprises avec lesquelles elle fait affaire. Parmi ses nombreuses fonctions, le Commissariat mène des enquêtes sur les plaintes, répond aux demandes de renseignements de particuliers, de parlementaires et d'organisations qui souhaitent obtenir de l'information et de l'orientation, noue de façon proactive des liens avec des intervenants, fournit au public des documents de sensibilisation et d'orientation, surveille les tendances et collabore avec des intervenants du domaine de la protection de la vie privée d'autres administrations, au Canada et à l'étranger, au traitement de questions liées à la protection des renseignements personnels à l'échelle mondiale qui découlent d'une circulation transfrontière accrue de l'information.

I.II Nouvelles technologies, anciennes questions

L'évolution des technologies au cours de la deuxième moitié du XX^e siècle a incité bon nombre de pays à élaborer des lois sur la protection des renseignements personnels. On s'inquiétait des effets potentiels de l'évolution rapide des technologies sur la protection de la vie privée. À mesure que les ordinateurs et les bases de données gagnaient en puissance, des universitaires, des décideurs, des gouvernements et des organisations internationales ont commencé à s'interroger sur les meilleures façons de protéger la vie privée des gens. Dans le secteur privé canadien, on a élaboré un code d'autoréglementation dans les années 1990 qui était principalement fondé sur les pratiques équitables en matière de renseignements décrites dans les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* émises en 1980 par l'OCDE. En 2000, on a promulgué la LPRPDE, loi qui intégrait le code d'autoréglementation. Les pratiques équitables en matière de renseignements qui figurent à l'annexe 1 de la LPRPDE sont les suivantes : responsabilité, détermination des fins de la collecte des renseignements, consentement, limitation de la collecte, limitation de l'utilisation, de la communication et de la conservation, exactitude, mesures de sécurité, transparence et accès aux renseignements personnels.

La majorité des problèmes sur lesquels le Commissariat s'est penché au cours des premières années de la mise en œuvre de la LPRPDE concernait les pratiques de protection des renseignements personnels des organisations traditionnelles, comme les institutions financières, les entreprises de télécommunications, les agences d'évaluation du crédit et les entreprises de transportⁱⁱ, et avaient trait aux activités opérationnelles quotidiennes. Parmi ces problèmes figuraient notamment la définition de « renseignements personnels » et la détermination du type de consentement approprié. D'autres problèmes portaient parfois sur les répercussions de la technologie sur le traitement de questions liées aux renseignements personnels, comme le fait de déterminer si les témoins sont des renseignements personnelsⁱⁱⁱ. La façon dont le Commissariat a abordé ces problèmes a fourni le cadre à partir duquel nous examinons les pratiques de protection de la vie privée des modèles opérationnels en évolution et les effets des nouvelles technologies sur certaines pratiques. Cela a fonctionné jusqu'à maintenant parce que la loi est fondée sur des principes et qu'elle est neutre sur le plan technologique.

La technologie a changé, et la façon dont nous interagissons avec cette dernière aussi. Quand la LPRPDE est entrée en vigueur en janvier 2001, les sites Web de réseautage social, les sites d'échange de vidéos et le microblogage n'existaient pas. Le Web était en expansion, et les entreprises commençaient à faire des affaires en ligne, les téléphones cellulaires n'étaient pas très courants, mais ils gagnaient en popularité, les caméras de surveillance étaient de plus en plus présentes, et la biométrie commençait à prendre forme. Il existait certains forums sur Internet où des personnes pouvaient communiquer entre elles, mais les communications en ligne étaient principalement à sens unique, soit du site Web vers la personne.

De nos jours, les gens jouent un rôle différent dans le partage de renseignements personnels. Dans les premières années de la mise en œuvre de la LPRPDE, une personne comme Louise devait, presque dans tous les cas, quitter son domicile pour prendre part à des activités commerciales. Maintenant, elle peut mener la plupart de ses activités commerciales, voire assumer des tâches professionnelles, depuis son domicile. La multiplication des occasions d'échange de renseignements personnels en ligne sur soi-même et sur d'autres personnes à un public souvent invisible fait qu'il est de plus en plus ardu d'établir une distinction entre nos vies publiques et privées d'une part, et nos vies professionnelles et personnelles, d'autre part. Parler de nous-mêmes ou d'autres personnes n'est pas une nouvelle activité, mais le fait de le faire en ligne signifie que cela est consigné de façon permanente, et l'industrie trouve de plus en plus de façons de tirer parti de cette situation.

Cette évolution a des répercussions sur la protection des renseignements personnels. Le Commissariat est responsable envers les Canadiens et le Parlement de suivre de près les nouvelles questions liées à la protection de la vie privée et de prendre des mesures proactives pour les informer de ces questions. La rapidité avec laquelle la technologie évolue fait qu'il est encore plus important que le Commissariat comprenne bien les nouvelles tendances. Nous devons être informés des répercussions potentielles de la technologie sur la protection de la vie privée et du rôle changeant que jouent les personnes dans la création et la diffusion de renseignements personnels.

I.III Est-ce que les outils dont nous disposons actuellement seront suffisants pour protéger la vie privée à l'avenir?

En ce qui a trait à la protection des renseignements personnels, le Canada a joué un rôle de chef de file en fournissant un cadre qui protège la vie privée des personnes et appuie les organisations à cet égard. À mesure que la technologie et l'économie numérique évoluent, il est important de veiller à ce que l'équilibre entre les besoins des entreprises et les droits des personnes à la vie privée soit maintenu et renforcé, au besoin. Jusqu'à maintenant, la LPRPDE s'est avérée efficace et a su s'adapter à des technologies et à des modèles opérationnels qui n'existaient pas au moment de son entrée en vigueur. On a également constaté que la LPRPDE s'appliquait à des organisations étrangères qui ont un lien réel et considérable avec le Canada, fait important puisque l'essentiel des activités en ligne font fi des frontières géographiques. Il est toutefois important de veiller à ce que les Canadiens puissent continuer de jouir de leur droit à la vie privée tout en tirant profit des nouvelles tendances et technologies. Il importe également que l'innovation se poursuive pour permettre aux industries de prospérer.

Consultations de 2010

Par conséquent, le Commissariat a décidé de consulter les Canadiens sur des questions qui, selon lui, pourraient compromettre la protection de la vie privée des consommateurs, à l'heure actuelle et dans un avenir rapproché^{iv}. Comme nous l'avons indiqué dans nos [observations](#) présentées dans le cadre de la consultation du gouvernement du Canada sur la stratégie numérique, nous sommes à l'aube d'une convergence des technologies qui entraînera une surveillance exhaustive des données des personnes^v. Cette consultation auprès des consommateurs visait à en apprendre davantage sur certaines pratiques de l'industrie, à examiner les répercussions de ces dernières sur la protection de la vie privée et à déterminer les mesures de protection de la vie privée auxquelles s'attendent les Canadiens relativement à ces pratiques. La consultation avait également pour objet de favoriser un débat sur les répercussions des progrès technologiques sur la protection des renseignements personnels et d'orienter le prochain processus d'examen de la LPRPDE.

Nous avons choisi d'aborder le suivi, le profilage et le ciblage en ligne, et l'informatique dans les nuages, car nous considérons que ces tendances sont susceptibles d'avoir des répercussions sur la vie privée des Canadiens. À mesure que les gens et les entreprises se tournent vers Internet et tirent profit des nombreux avantages de l'ère numérique, les pratiques qui soutiennent les services que les gens apprécient doivent être entièrement examinées sous l'angle de la protection de la vie privée.

Nous nous sommes également penchés expressément sur les activités en ligne des enfants, comme David. L'âge moyen des enfants qui utilisent Internet semble diminuer^{vi}, et les responsables des politiques publiques doivent accorder une attention particulière aux effets des activités en ligne sur la vie privée des enfants. L'un de nos objectifs est d'attirer l'attention sur cette question. En général, les efforts visent surtout à protéger les enfants contre les prédateurs quand ils sont sur le Web. Toutefois, bon nombre d'experts ont affirmé qu'il fallait accorder davantage d'attention à la protection des renseignements personnels des enfants.

Au cours des dernières années, le Commissariat a examiné les pratiques de protection de la vie privée de sites de réseautage social et abordé des questions liées à la technologie d'imagerie à l'échelle de la rue utilisée pour cartographier les villes du Canada. En 2008 et 2009, nous avons examiné la question de l'inspection approfondie des paquets en enquêtant sur son utilisation, en présentant des mémoires au Conseil de la radiodiffusion et des télécommunications

canadiennes, et en commandant un ensemble d'essais sur la technologie. En décembre 2009, nous avons pris part aux audiences du Comité permanent des transports et des communications du Sénat sur la société numérique, où nous avons abordé les questions de protection des renseignements personnels et de sécurité dans le monde numérique. En réfléchissant à ce que nous avons appris dans le cadre de ces travaux, nous avons décidé que nous devons mobiliser le public et les intervenants et nous renseigner davantage sur l'incidence des activités en ligne sur la protection des renseignements personnels. Plus précisément, l'évolution du Web 2.0 a souligné l'importance de trouver des façons novatrices de joindre le public pour l'aider à naviguer en ligne en toute connaissance de cause.

Nous voulions entendre l'opinion des Canadiens sur la question. Nous voulions parler aux représentants de l'industrie de leurs pratiques et de la façon dont ils perçoivent la protection des renseignements personnels dans le contexte de la technologie et de l'innovation. Nous voulions connaître le point de vue d'universitaires qui réfléchissent à la protection des renseignements personnels, à la technologie et à ce que nous réserve l'avenir, et le point de vue de défenseurs d'intérêts qui jouent un rôle important en s'exprimant au nom des Canadiens sur un sujet qui devient de plus en plus complexe.

Comme la technologie abaisse les frontières dans le domaine du traitement des données, le Commissariat reconnaît que la coopération et le consensus à l'échelle internationale quant aux questions de protection de la vie privée sont essentiels pour contribuer à la protection des renseignements personnels des Canadiens. Bon nombre d'organisations internationales, de décideurs et d'autres autorités de protection des données examinent de façon plus approfondie les principes de protection des renseignements personnels qui constituent le fondement des lois et des efforts d'autoréglementation pour déterminer s'ils permettront de bien répondre aux besoins des citoyens à l'avenir. Certains examinent également plusieurs des questions abordées dans le présent rapport. Nous surveillons leurs efforts, et ils font de même. En effet, nous avons eu l'honneur d'accueillir David Vladeck, directeur du Bureau of Consumer Protection de la Federal Trade Commission (FTC) des États-Unis à notre consultation du 29 avril 2010 à Toronto. La FTC a tenu des [tables rondes](#) sur la protection des renseignements personnels à la fin de 2009 et au début de 2010. Nous avons également eu le plaisir d'accueillir un certain nombre de dirigeants de l'industrie et d'universitaires des États-Unis et de l'Europe à nos événements. Leurs points de vue sur ces questions sont très utiles, car nous nous efforçons de trouver des approches communes à la protection des renseignements personnels.

Nous avons tenu les consultations à plusieurs endroits au pays pour joindre les Canadiens et cibler les régions où bon nombre d'associations ou d'entreprises de l'industrie sont situées. Nous avons diffusé l'événement sur le Web et utilisé nos propres outils de réseautage social pour attirer le plus grand nombre de Canadiens possible^{vii}.

Nous espérons que les consultations et le présent rapport favorisent de nouvelles activités de sensibilisation que le Commissariat pourra mener dans le cadre de son mandat d'éducation du public. La sensibilisation suppose la discussion avec les Canadiens et l'éducation des organisations à l'égard de leurs obligations en matière de protection des renseignements personnels. Les consultations permettront l'élaboration du matériel que nous utiliserons pour mener les activités de sensibilisation. Elles orienteront également nos recherches et nos travaux stratégiques au cours des prochaines années. Elles nous aideront en outre à préparer la contribution du Commissariat au prochain examen parlementaire de la LPRPDE.

Parfois, les consultations ont suscité davantage de questions que de réponses, mais elles ont donné lieu à des discussions stimulantes sur les domaines qui, selon nous, compromettent la

protection des renseignements personnels. La présente ébauche de rapport ne vise pas à présenter des conclusions sur certaines pratiques. Elle vise plutôt à lier les pratiques au cadre de la LPRPDE pour souligner les domaines qui peuvent susciter des préoccupations; elle indique également les domaines qui sont liés à des questions générales concernant la protection des renseignements personnels et qui ne sont pas nécessairement abordés par la loi. Les participants étaient souvent d'accord sur les répercussions liées à la protection des renseignements personnels, mais ils divergeaient quant à la façon de les aborder. Le présent rapport de consultation demande des commentaires précis de l'industrie sur certains sujets. Il indique les domaines pour lesquels nous comptons prendre des mesures, que nous souhaitons examiner davantage et sur lesquels l'industrie et le gouvernement doivent, selon nous, prêter attention. Le rapport n'est pas notre contribution au processus d'examen de la LPRPDE et il ne comporte pas de changements précis que nous aimerons voir apporter à la *Loi*. Nous avons entendu certaines suggestions sur des changements à apporter à la *Loi* et nous en tiendrons compte lorsque nous amorcerons le processus d'examen de la LPRPDE.

Dans certaines sections du rapport, nous avons demandé des renseignements supplémentaires et nous recueillerons vos commentaires jusqu'au **10 décembre 2010**. Le rapport final sera diffusé en 2011.

Suivi, profilage et ciblage en ligne

Louise a acheté un jean griffé dans un magasin^{viii} du centre commercial du coin en payant avec sa carte de crédit. Elle a aussi remis sa carte de fidélité au commis pour qu'il enregistre la transaction.

De retour à la maison, Louise a ouvert une session dans son nouveau compte, sur le site Web du magasin, pour se renseigner davantage sur les vêtements qu'elle a essayés mais qu'elle n'a pas achetés. Dans son empressement à examiner la marchandise du magasin, elle a cliqué rapidement sur le long énoncé de politique sur la protection de la vie privée du site.

Alors qu'elle parcourait le site Web du magasin à la recherche d'un chemisier pour accompagner son nouveau jean, Louise a vu une annonce de bijoux qui lui a vraiment plu et elle a suivi le lien. Louise s'est sentie à l'aise sur le petit site canadien de bijoux parce qu'il lui donnait l'impression de visiter la page d'un ami.

Comme elle aimait les styles de bijoux offerts sur le site, elle a aussi acheté un collier et cliqué sur « j'aime » pour mettre ses amis au courant de cette dernière acquisition. Puis, elle a quitté le site et fait une recherche pour trouver un concert et elle a acheté deux billets. Ensuite, elle a vérifié l'état d'une enchère en ligne à laquelle elle participe pour tenter d'acquérir une nouvelle bande dessinée spécialisée.

Après cela, Louise a mis à jour sa page Facebook pour informer ses amis de ses achats et voir qui d'autre irait au concert. À partir de Facebook, elle a consulté le site de sa librairie en ligne préférée, où elle a acheté un livre que lui a recommandé un autre spécialiste de bandes dessinées.

Lorsque Louise a acheté un jean griffé au centre commercial du coin, le magasin lui a aussi offert d'essayer un gadget logiciel sur son iPhone pour la durée de son magasinage, pour lui indiquer où se trouvent les vêtements qui pourraient l'intéresser en fonction de son sexe et de son âge (21 ans). Louise a opté pour une expérience plus personnelle et a aussi ajouté son adresse de courriel, son numéro de téléphone, ainsi que les styles et les tailles de vêtements qu'elle préfère^{ix}.

Pendant qu'elle se trouvait dans le magasin, Louise a vérifié un service géodépendant populaire; elle a ensuite reçu un message sur son iPhone l'informant que le café situé à côté du magasin offrait une promotion spéciale pour l'heure du lunch avec certains de ses plats favoris — un thé vert chai et un sandwich luzerne et gruyère.

Plus tard dans la soirée, Louise est sortie avec ses amis et a porté ses nouveaux vêtements. Elle et ses amis ont consulté le service géodépendant et ont ensuite reçu des offres de rabais dans des restaurants et des boîtes de nuit situés à proximité. Ils ont retenu une offre et en ont informé d'autres amis. Ils étaient impatients de faire démarrer la soirée.

Le jeune frère de Louise, David, est âgé de 9 ans. Il aime jouer à des jeux en ligne et s'est inscrit lui-même à plusieurs jeux. Les avis qui s'affichent à l'écran l'impatientent et il clique pour les faire disparaître le plus vite possible. Il demande parfois à Louise d'utiliser son adresse de courriel et son numéro de carte de crédit afin de ne pas avoir à faire intervenir ses parents dans le processus de consentement. Louise est satisfaite de cet arrangement, sauf pour les courriels qu'elle reçoit maintenant pour l'informer des offres spéciales liées aux jeux auxquels David s'est inscrit.

Lorsque David s'inscrit à un jeu, il a tendance à remplir tous les champs parce qu'il ne sait pas s'il peut les laisser en blanc; parfois, il invente des renseignements. Il aime bavarder avec d'autres joueurs et, s'il leur fait confiance, il leur révèle des renseignements à son sujet, par exemple l'endroit où il vit et ce qu'il aime faire.

L'un des jeux préféré de David a affiché un avis indiquant que des renseignements « non personnels » seraient recueillis durant la procédure d'ouverture de session et que le consentement pour ce faire avait été obtenu par le biais des conditions de service. Cela est satisfaisant pour David qui ne s'interroge pas davantage parce qu'il n'est pas concerné de toute façon. Cependant, la définition de « renseignements non personnels » dans les conditions de service a trait à l'enregistrement de l'adresse IP de l'ordinateur de David, que certains considèrent comme un renseignement personnel.

II. Qu'est-ce que le suivi, le profilage et le ciblage en ligne?

Qu'est-ce qui se passe quand Louise navigue sur le Web, qu'elle clique sur des publicités, fait des achats et en informe ses amis? Comment l'annonceur ou le courtier en données sait-il que Louise aime les bijoux, par exemple? Les renseignements associés à sa carte de fidélité sont-ils parfois combinés à ses activités en ligne? Qu'en est-il des renseignements qu'elle fournit par l'entremise du logiciel gadget ou de sa page Facebook?

Tout ce que vous faites en ligne est enregistré d'une façon ou d'une autre. On recueille de plus en plus certains de ces renseignements pour les utiliser à des fins commerciales (et pour des programmes gouvernementaux). Les données sont très lucratives, et il est possible de faire de l'argent au moyen des renseignements personnels fournis sur Internet par des personnes comme Louise et David.

De quelle façon le suivi et le profilage fonctionnent-ils?

Si l'on effectue le suivi de Louise en ligne, des données sur ses habitudes de navigation sont recueillies grâce à des indicateurs numériques. Les témoins HTTP et Flash et les pixels invisibles sont actuellement les moyens les plus fréquemment utilisés pour recueillir des renseignements. Les témoins sont de petits fichiers texte placés sur le disque dur de l'ordinateur de Louise quand elle visite des sites Web. Ils servent à recueillir et à emmagasiner des renseignements sur elle en fonction de ses habitudes de navigation et des renseignements qu'elle fournit. Les témoins Flash peuvent être utilisés pour enregistrer des renseignements entre deux sessions, mais ils servent également à effectuer le suivi des sites Web que Louise visite. Les témoins Flash sont souvent utilisés sur les sites Web et avec des témoins traditionnels sur le Web et on peut les utiliser pour recréer des témoins s'ils sont supprimés. Les pixels invisibles sont des petits segments de code qui constituent une méthode pour intégrer une image graphique sur une page Web ou dans un courriel aux fins de transfert de données. Souvent, le pixel invisible est conçu de façon à s'harmoniser avec l'arrière-plan de la page visitée^x. Les pixels invisibles peuvent être utilisés pour comprendre certaines tendances de navigation d'un visiteur donné du site. Ils peuvent également servir à envoyer des témoins ou des applications téléchargeables^{xi}. Louise peut désactiver les témoins ou les supprimer temporairement, mais il est difficile de supprimer ou de refuser les pixels invisibles. Les supertémoins sont un nouveau type de témoin. Ils utilisent de nouveaux emplacements de mémoire intégrés aux navigateurs afin d'enregistrer les renseignements sur l'utilisateur.

Voici quelques types de renseignements recueillis dans les fichiers journaux sur les utilisateurs d'Internet : adresse IP, pages visitées (dans un site donné ou dans plusieurs sites), temps passé sur les pages, publicités consultées, articles lus, achats effectués, termes recherchés ou autres renseignements entrés sur un site, préférences de l'utilisateur, comme la langue et le type de navigateur Web, système d'exploitation et information sur l'emplacement géographique par l'entremise des adresses IP (sur le Web) ou du système de positionnement global (GPS) qui se trouve dans bon nombre d'appareils sans fil.

D'autres données peuvent être recueillies au moyen d'autres technologies, comme l'inspection approfondie des paquets. Les personnes comme Louise fournissent également de façon volontaire bon nombre de renseignements personnels, surtout par l'entremise des sites de réseautage social, comme Facebook, MySpace et LinkedIn, et d'autres services Web populaires, comme Foursquare. Les techniques d'exploration de données sont ensuite utilisées pour découvrir les tendances à partir des données, lesquelles peuvent ensuite servir à différentes fins.

II.1 Ce que nous avons appris

Nous avons reçu 21 observations écrites sur le suivi, le profilage et le ciblage en ligne. Elles portaient principalement sur la publicité comportementale. Les autres utilisations possibles des renseignements ont fait l'objet de discussions dans le cadre des consultations.

Qu'est-ce que la publicité comportementale?

Une bonne part de la publicité en ligne — publicité fondée sur les données démographiques, l'emplacement, le comportement, le contexte ou les intérêts — représente des variations sur le thème de la publicité comportementale.

La publicité comportementale consiste à effectuer le suivi des activités de consommateurs en ligne au fil du temps afin de présenter des annonces ciblant leurs intérêts. Les annonceurs qui ont recours à la publicité comportementale utilisent ces données pour créer des profils d'utilisateurs, déterminer les catégories d'intérêt des utilisateurs et montrer des publicités fondées sur les données démographiques et des hypothèses sur les intérêts. D'un annonceur à l'autre, ces catégories d'intérêts peuvent être générales (p. ex. passionné d'automobiles) ou très précises (p. ex. jeune femme propriétaire d'une Honda ayant de jeunes enfants et habitant en Alberta). L'annonceur utilise les catégories d'intérêts pour choisir et présenter des annonces qui sont considérées comme pertinentes à ces catégories.

Les renseignements sur le comportement en ligne de Louise peuvent être utilisés pour optimiser sa sensibilisation aux produits et services. En raison de la popularité accrue des dispositifs mobiles, les annonceurs se penchent de plus en plus sur l'emplacement afin d'obtenir de nouveaux clients potentiels. On peut connaître l'emplacement d'une personne grâce aux réseaux de téléphones cellulaires, aux points d'accès sans fil, aux liens satellites et aux systèmes de positionnement global, et s'en servir pour offrir des services sur les appareils sans fil. Louise indique également de façon volontaire son emplacement quand elle utilise des services géodépendants, comme les applications qui recommandent des restaurants à proximité ou qui effectuent le suivi d'amis.

Un concept important et distinct de la publicité comportementale est la publicité contextuelle. La FTC, qui [étudie depuis quelque temps les pratiques liées à la publicité en ligne](#), définit la

publicité contextuelle comme un type de publicité axée sur la visite d'un consommateur à une page Web donnée ou une recherche unique qui ne comporte aucune conservation de données sur les activités en ligne du consommateur outre ce qui est nécessaire pour la présentation immédiate d'une annonce ou d'un résultat de recherche^{xii}. On ne considère pas que ce type de publicité compromette la vie privée, comme c'est le cas de la publicité comportementale, car il ne suppose pas la collecte ou la conservation des renseignements sur le comportement de la personne en ligne, soit ses habitudes de navigation, son emplacement ou ses activités sur les sites de réseautage social, au fil du temps. Cependant, quand une personne clique sur une publicité contextuelle, cette activité est suivie et elle peut être utilisée ultérieurement dans une publicité ciblée.

Qui sont les principaux intervenants dans la diffusion des publicités comportementales en ligne?

En général, trois principaux acteurs interviennent dans le modèle de publicité comportemental : les sites Web, les annonceurs et les réseaux de publicité. En bref, les sites Web ont besoin de fonds pour fonctionner, les annonceurs veulent vendre des produits et les réseaux de publicité permettent la diffusion de publicités à un public cible. On n'a pas abordé en détail dans les observations écrites et les discussions de groupe les différents intervenants œuvrant dans le domaine du suivi, du profilage et du ciblage en ligne.

En ce qui a trait à l'univers actuel de la publicité en ligne, l'une des observations écrites que nous avons reçues soulignait qu'au cours des dernières années, le nombre de réseaux de publicité avait diminué. Cela permet à un nombre restreint de très grandes entreprises de publicité d'effectuer de façon globale le suivi des comportements des utilisateurs sur Internet. Bon nombre de ces réseaux sont détenus par les mêmes entités qui fournissent un certain nombre de services Web et qui ont un lien direct avec les utilisateurs.

Avantages et risques

Les associations industrielles qui nous ont transmis leurs observations ont souligné les nombreux avantages de la publicité comportementale. Ils ont fait valoir que bien que les personnes n'aient pas besoin de payer (du moins en argent) pour obtenir certains renseignements et services sur Internet, il faut néanmoins que des revenus soient générés. La publicité est la source principale de revenus pour les entreprises sur le Web. Les annonceurs cherchent la meilleure façon de mettre en marché les produits et les services, et ceux qui paient pour les annonces veulent que leurs produits et services soient connus du plus grand nombre possible de parties intéressées. En citant des études qui indiquent que les gens préfèrent recevoir des renseignements qui les intéressent, les associations ont souligné que la publicité comportementale fournit aux utilisateurs comme Louise des renseignements à caractère commercial pertinents pour eux. Parmi les autres avantages cités, mentionnons l'appui à des événements culturels, sportifs ou autres, la vente de biens et de services et le soutien de l'économie et de l'emploi dans l'industrie de la mise en marché et les industries connexes.

Bon nombre d'associations industrielles, de groupes de défense des intérêts et d'universitaires ont affirmé que le suivi, le profilage et le ciblage en ligne posaient des risques. Des associations clés de l'industrie ont reconnu que près de la moitié des Canadiens qu'elles avaient sondés ont affirmé qu'ils n'étaient pas à l'aise avec l'idée d'être suivis en ligne. Pour les associations de l'industrie qui ont commenté la question, ces pratiques risquent d'ébranler la confiance des consommateurs, surtout parce que la pratique consistant à faire le suivi des personnes est

invisible pour ces dernières. Ces associations ont mentionné les efforts de l'industrie à l'égard de l'autoréglementation et de la sensibilisation des consommateurs comme moyens d'accroître la visibilité de la pratique et de veiller à ce que la vie privée des utilisateurs soit respectée. Ces mesures d'autoréglementation sont abordées de façon plus approfondie ci-dessous.

Les défenseurs du droit à la vie privée ou des intérêts des consommateurs qui ont fourni des observations écrites ou pris part aux consultations ont également mentionné bon nombre de risques liés à cette pratique. Le fait que les gens ne sont pas très sensibilisés au rôle et à l'ampleur de la collecte de données dans la diffusion de publicités fondées sur le comportement ou le suivi des consommateurs et qu'ils ne les comprennent pas bien^{xiii} était une préoccupation clé. Le fait que de telles pratiques compromettent la capacité de la personne de surveiller la diffusion de ses renseignements personnels était également au nombre des préoccupations ou des risques soulevés. On a également mentionné l'utilisation de données potentiellement inexactes influant sur l'expérience en ligne d'utilisateurs et les décisions prises les concernant, souvent sans qu'ils en soient au courant, ce qui nuit à leur capacité de remettre en question l'exactitude des renseignements. Un autre risque important tient au fait que le profilage peut servir à discriminer les personnes, par exemple par l'entremise de structures de prix. Ce qu'il importe de retenir, c'est que ces pratiques menacent l'autonomie des consommateurs. Ces préoccupations sont abordées davantage dans les sections sur les questions générales liées à la protection des renseignements personnels et les principes de la LPRPDE, ci-dessous.

Portée de la publicité comportementale et contexte international

Une présentation indiquait qu'actuellement, la publicité comportementale ne représente que 10 % des revenus de publicité en ligne au Canada. Même si la discussion sur la publicité comportementale portait sur le contexte canadien, on a insisté sur le fait que les pratiques en ligne sont généralement transfrontières. Ainsi, bon nombre de répondants de l'industrie ont indiqué que dans toute discussion sur les pratiques exemplaires au chapitre de la protection de la vie privée, il faut tenir compte des différentes exigences sur le plan international.

Autoréglementation

Nous avons appris qu'un certain nombre d'organisations, dont bon nombre mènent des activités ailleurs qu'au Canada, avaient mis en place des mesures d'autoréglementation. En règle générale, ces mesures visent à fournir des renseignements aux consommateurs sur les activités de publicité comportementale en ligne et les options de retrait dont ils peuvent se prévaloir. Ils sont fondés sur certaines lignes directrices élaborées par des associations américaines comparables et comportent les principes suivants : avis et choix, sensibilisation, transparence, contrôle, sécurité des données, changements importants, données de nature délicate et responsabilisation. Plusieurs organisations ont indiqué dans leur présentation que certains de ces principes, voire tous ces principes, orientaient leurs activités de suivi, de profilage et de ciblage en ligne.

II.II Points de vue des Canadiens

Voici un bref aperçu de certaines enquêtes pertinentes liées aux points de vue sur la protection de la vie privée, dont l'une a été commandée par le Commissariat (nous menons une enquête auprès de personnes tous les deux ans), et d'une enquête menée par Ressources naturelles Canada sur l'information géospatiale. Les auteurs de certaines observations écrites ont mentionné des études précises sur les attitudes des Canadiens à l'égard du suivi en ligne ou de

la publicité comportementale. Deux de ces observations ont été rendues publiques, et les études mentionnées dans les observations sont fournies ci-dessous.

Attitudes générales à l'égard de la protection de la vie privée

Une enquête EKOS réalisée en 2009 pour le compte du Commissariat a révélé que 90 % des Canadiens sont préoccupés par les répercussions des nouvelles technologies. Si les Canadiens ne sont pas conscients de certains risques d'atteinte à leur vie privée, ou s'ils acceptent consciemment de faire des compromis à ce chapitre, ils n'en ont pas moins des attentes élevées en ce qui a trait à la protection de leur vie privée, y compris en ligne, et ils se préoccupent de la façon dont leurs renseignements personnels sont utilisés, notamment dans le contexte de la circulation transfrontière des données.

Les personnes âgées de 45 à 65 ans sont plus susceptibles de s'inquiéter de l'impact des nouvelles technologies sur la vie privée, tandis que les personnes de moins de 25 ans sont moins enclines à exprimer une grande inquiétude à cet égard. De même, les Canadiens de moins de 25 ans sont moins susceptibles de se préoccuper du traitement et du stockage hors frontières de leurs renseignements personnels.

Dans l'ensemble, 98 % des Canadiens croient qu'il est important d'avoir des lois rigoureuses en matière de protection des renseignements personnels^{xiv}.

Attitudes à l'égard du suivi et du ciblage en ligne

Selon une enquête menée en 2009 par le Centre pour la défense de l'intérêt public au sujet du suivi du comportement de consommateurs en ligne, près de 75 % des répondants n'étaient pas très à l'aise ou pas à l'aise du tout avec la publicité fondée sur le suivi. La moitié des répondants étaient au courant des dispositifs et des techniques de suivi. L'étude a montré que les personnes avaient tendance à accepter davantage le suivi en ligne aux fins de service à la clientèle ou de publicité si cela était fait par des entreprises avec lesquelles elles avaient déjà fait affaire^{xv}. Dans une étude menée au nom de l'Association canadienne du marketing en 2009 au sujet de la publicité comportementale, on mentionne que 50 % des Canadiens étaient plutôt mal à l'aise à l'idée que des spécialistes du marketing utilisent des renseignements sur la navigation des consommateurs pour leur présenter des publicités plus pertinentes^{xvi}. Dans une étude qui a fait l'objet d'une discussion dans le cadre des événements tenus à Montréal, on a expliqué que les personnes ont tendance à accepter davantage la publicité comportementale une fois qu'elle leur a été expliquée.

Attitudes à l'égard de la protection des renseignements géoréférencés

En ce qui a trait aux données sur l'emplacement, Ressources naturelles Canada a mené une enquête sur les points de vue des Canadiens à l'égard de la confidentialité et de l'utilisation des données géospatiales. Selon certaines conclusions clés de l'enquête, les Canadiens sont plutôt prudents en ce qui a trait au partage de renseignements liés à leur emplacement, et le contrôle des renseignements partagés et le contexte sont les éléments qui influent le plus sur leur sentiment de confiance à l'égard du partage de ces renseignements. Les Canadiens sont moins à l'aise lorsque les renseignements sont liés à un emplacement en temps réel ou servent à des fins de commercialisation sélective, lorsqu'il n'y a aucun contrôle ou très peu, lorsque les renseignements sont partagés avec le secteur privé ou le grand public, et pour des raisons

associées à l'activité économique. Près de la moitié des répondants ne voient aucun avantage à utiliser la technologie de localisation ou sont incertains des avantages qu'elle procure^{xvii}.

II.III Questions générales liées à la protection de la vie privée

« *Nous vivons notre vie privée en ligne*^{xviii} »

—*La commissaire à la protection de la vie privée du Canada, Jennifer Stoddart*

Grâce aux outils de plus en plus puissants de forage de données, il est possible de dresser le portrait complet d'une personne à partir de ce qu'elle écrit sur elle-même et les autres sur des sites de réseautage social, des capacités de cartographie qui nous montrent, à nous et aux autres, où et comment nous vivons, de l'entretien des contacts avec nos amis, du jumelage de nos préférences aux endroits où nous nous trouvons ainsi que de la surveillance de l'utilisation des choses que nous possédons. En outre, les progrès technologiques permettent le regroupement de fonctions dans un seul dispositif, ou le regroupement de fonctions ou de services dans une seule plateforme. Ce deuxième cas suppose la concentration des renseignements et du pouvoir entre les mains d'organisations de plus en plus restreintes, ce qui constitue un problème de taille pour la protection du marché en ligne.

Les individus sont des consommateurs enthousiastes de la technologie et des participants de la vie sociale sur le Web. Ils tirent profit des outils à leur disposition, mais cela a des conséquences positives ou négatives, certaines d'ordre social, d'autres, économique. Malgré cela, ils utilisent avidement ces outils et échangent ou créent un volume accru de renseignements personnels. Cependant, ils affirment toujours que la protection de la vie privée est importante pour eux. Cela semble contradictoire, mais est-ce vraiment le cas?

Dans bon nombre des observations écrites et des discussions en table ronde, on a soulevé des questions générales liées à la protection de la vie privée ainsi que des questions ayant précisément trait à la portée et aux principes de la LPRPDE. Dans la présente section, on abordera certaines des questions générales liées à la protection de la vie privée en ce qui concerne le suivi, le profilage et le ciblage en ligne. Certains des commentaires présentés dans cette section se rapportent à des questions liées plus généralement au phénomène des personnes qui passent de plus en plus de temps en ligne et échangent un plus gros volume de renseignements personnels (les leurs et ceux des autres) avec la communauté en ligne. Les questions soulevées dans la présente section ont pour but de déterminer si la technologie influence notre comportement et, le cas échéant, dans quelle mesure. Nous tenons également compte des observateurs, soit d'autres personnes, des annonceurs, des chercheurs, des spécialistes du marketing et le gouvernement, qui utilisent ces renseignements pour différentes raisons, ce qui a des répercussions sur la protection de notre vie privée, dont certaines ne sont pas explicitement comprises dans la portée de la LPRPDE.

Ce que nous avons entendu — l'absence de démarcation claire entre les domaines public et privé et les répercussions sur notre réputation

Qui est Louise?

Dans le cadre des consultations tenues à Toronto et à Montréal, bon nombre de discussions portaient sur la façon dont la nature sociale de l'expérience en ligne actuelle a des répercussions profondes sur la protection de la vie privée. Selon certaines des observations écrites que nous avons reçues et certains commentaires que nous avons entendus, les

concepts traditionnels d'espace public et d'espace privé changent compte tenu de la prévalence des technologies de communication mobiles et de la popularité accrue du réseautage social. Le réseautage social fournit aux personnes les mécanismes nécessaires pour rendre leur vie privée publique, et cela contribue à l'évolution des attentes face à la protection des renseignements personnels. En retour, certains exploitants de sites de réseautage social invoquent cette évolution pour justifier une plus grande ouverture et un échange plus libre de renseignements. L'utilisation des téléphones cellulaires et l'accès accru aux applications géodépendantes font que la vie privée est de plus en plus publique.

On a discuté du « public invisible », soit les personnes à qui Louise croit s'adresser. Cela a une incidence importante sur le type et le volume de renseignements communiqués. Les enfants et les jeunes adultes ont une perception très différente du public auquel ils s'adressent en ligne. Lorsqu'ils sont en ligne, les jeunes enfants comme David s'attendent à ce que « le public » soit composé d'autres enfants. Ils ne s'attendent pas à ce que les adultes fassent partie de ce public, même s'ils savent que ces derniers peuvent voir l'information. Les jeunes adultes sont enclins à afficher des renseignements qui renforcent l'image qu'ils veulent montrer au public. Cela explique l'affichage de certains renseignements sociaux par des jeunes qui ressentent le besoin d'être populaires.

On a mentionné que les gens ont de la difficulté à visualiser leur public quand ils téléchargent des renseignements sur eux-mêmes ou d'autres personnes. Ils sont seuls devant un écran, et, comme il s'agit d'une activité solitaire, il est facile de se méprendre sur la composition du public. Les gens se comportent différemment, et les normes sociales sont remises en question. Par exemple, en ce qui a trait à la question du suivi et de la technologie fondée sur les données géographiques, non seulement les entreprises (et par extension les organismes gouvernementaux) peuvent suivre les personnes, mais les personnes peuvent se suivre les unes les autres. Puisque la capacité de le faire existe, le suivi des autres devient acceptable sur le plan social, voire une activité sociale^{xix}.

On a également discuté de l'effet de la pression exercée par les pairs et des relations de pouvoir sur les personnes comme Louise et David, et de la façon dont cela nuit aux mesures de protection de la vie privée normalisées, comme le consentement. Les gens se sentent obligés d'utiliser beaucoup de ces services, car ils croient que s'ils s'en abstiennent, ils se retrouveront seuls. Certains participants aux consultations ont indiqué que la vie sociale dépend grandement de l'utilisation des technologies de l'information. Par ailleurs, à cause des technologies, nos liens avec les autres peuvent être cartographiés. Il en résulte notamment que les personnes sont stéréotypées en fonction de qui sont leurs amis. Nous aborderons à nouveau l'utilisation du marketing dans les médias sociaux ultérieurement dans le présent document.

Quand les obstacles sont éliminés mais que les perceptions ne sont pas rajustées en conséquence, et que les personnes affichent des renseignements en ligne comme si elles écrivaient dans leur journal intime, cela compromet véritablement leur réputation. En plus des risques pour les personnes, on a mentionné dans un des groupes de discussion à Montréal que le réseautage social peut compromettre la réputation d'entreprises. Les entreprises peuvent communiquer de façon inadéquate des renseignements, et des organisations entières peuvent être discréditées.

On a tenu des discussions sur la gestion de l'identité en ligne, soit la capacité de contrôler les renseignements sur soi-même. On a mentionné que bon nombre des conséquences associées au fait d'avoir une vie sociale en ligne pourraient être atténuées si la technologie permettait aux

gens d'être plus prudents dans leurs activités. Un participant a indiqué qu'une grande partie de l'architecture technologique en ligne est publique par défaut et privée moyennant certains efforts^{xx}. D'autres se demandaient pourquoi Louise n'obtenait pas plus d'avantages pour avoir fourni des renseignements personnels et potentiellement mis en cause sa réputation.

On a discuté du fait que la protection des renseignements personnels doit être intégrée d'emblée aux systèmes et aux pratiques et des paramètres par défaut qui devraient exister sur Internet à cet égard. On a reconnu que le fait de régler les problèmes après l'adoption des pratiques peut avoir des conséquences pour les personnes et les organisations.

Bon nombre de participants ont mentionné que l'industrie de la publicité comportementale en est à ses débuts et que la technologie évolue rapidement. Dans un sens, pour ce qui est de la protection des renseignements personnels, les organisations tentent d'harmoniser leurs politiques à cet égard avec leurs pratiques opérationnelles. Par conséquent, il y a certains risques pour les personnes et les organisations. Pour Louise, cela signifie habituellement que ses renseignements personnels sont recueillis et utilisés à des fins qu'elle ignore totalement. Pour les entreprises, cela signifie que la confiance entre l'organisation et la personne est compromise en raison de l'invisibilité des pratiques et de l'utilisation potentiellement inadéquate des renseignements.

Observations du Commissariat

Le Commissariat convient que les concepts traditionnels de l'espace public et de l'espace privé sont en train de changer. Les Canadiens continuent de considérer la protection de la vie privée comme importante, mais ils veulent également participer à la vie en ligne. Les deux ne sont pas incompatibles, mais nous croyons qu'il faut en faire davantage pour protéger la vie privée afin que les personnes comme Louise puissent faire confiance à ceux qui leur offrent des produits, des services et des endroits où mener leur vie sociale.

Le Commissariat convient que la pratique consistant à élaborer des profils et à tirer des conclusions en fonction des renseignements que les personnes affichent sur les sites de réseautage social comporte une multitude de risques d'atteinte à la vie privée des personnes (et probablement à d'autres droits fondamentaux). Même si les personnes affichent en ligne des renseignements sur elles-mêmes et leurs amis, cela ne veut pas nécessairement dire qu'elles veulent que des entités inconnues utilisent ces renseignements comme elles l'entendent. Dans les discussions que nous avons tenues à Montréal, on a mentionné que lorsque les gens se trouvent sur un site de réseautage social, ils ont tendance à croire qu'ils sont entre amis et qu'ils n'agissent pas à titre de « consommateurs ». La distinction entre nos interactions sociales et notre « rôle » de consommateurs s'estompe. On essaie de faire de nous des consommateurs à temps plein.

La recherche sur les perceptions que les personnes ont de leur public et de la divergence possible entre leurs impressions et la réalité à cet égard en est encore à ses premiers balbutiements. Comme l'a mentionné la chercheuse danah boyd, la façon dont les gens communiquent et interagissent en ligne est complexifiée par le fait que les réseaux sociaux possèdent en particulier certaines propriétés qui modifient la dynamique sociale, soit la persistance, la possibilité de faire des recherches, la possibilité de faire des copies exactes et les publics invisibles^{xxi}. En ce qui a trait aux activités de réseautage social, certaines recherches laissent entendre que les personnes établissent une distinction en ce qui concerne leur public cible et souhaitent prendre des mesures de contrôle^{xxii}. La difficulté associée à l'exercice du

contrôle s'explique par l'architecture des sites. Quand les mesures de protection de la vie privée sont difficiles à trouver ou à comprendre sur un site Web, la capacité de la personne d'assurer un certain contrôle est amenuisée. Si le site est populaire et que la personne souhaite vraiment faire partie de la communauté, elle risque d'être plus conciliante afin de se joindre au site.

Le Commissariat remet en question le point de vue selon lequel les renseignements qui sont affichés en ligne volontairement peuvent être utilisés à toutes sortes de fins. Certaines recherches montrent que certaines personnes se créent intentionnellement une fausse identité en ligne et affichent des renseignements à l'appui, habituellement pour se donner de l'importance^{xxiii}. Leur intention n'est peut-être pas toujours de s'afficher publiquement. Par exemple, une personne peut vouloir entretenir une présence professionnelle en ligne, mais il se peut qu'elle souhaite également disposer d'un espace social distinct où échanger avec ses amis à l'extérieur du contexte professionnel. Établir une distinction entre ces deux environnements et la maintenir n'est ni évident ni facile.

De plus, au Canada, les renseignements personnels qui figurent dans le domaine public ne peuvent pas nécessairement être utilisés à différentes fins. Par exemple, la LPRPDE indique que certains renseignements personnels auxquels le public a accès (comme il est défini dans le [Règlement précisant les renseignements auxquels le public a accès](#), découlant de la LPRPDE) peuvent être recueillis, utilisés et communiqués sans le consentement de la personne; cependant, les fins pour lesquelles les renseignements peuvent être recueillis, utilisés ou communiqués sont limitées.

Le Commissariat considère que les dommages causés à la réputation des personnes dans la vraie vie est l'exemple par excellence des conséquences du flou apparent entre les existences publique et privée. Des personnes (comme des enseignants, des politiciens et des hauts gradés de la police) ont perdu leur emploi, ont été humiliés publiquement ou ont perdu des avantages en raison de renseignements qu'elles avaient affichés en ligne. Les données affichées en ligne sont consignées de façon permanente. Les renseignements qui ternissent la réputation d'une personne peuvent ne jamais s'effacer. De plus, en raison de la popularité accrue des applications géodépendantes, le fait de dire aux gens où vous êtes signifie que vous leur dites également où vous n'êtes pas, ce qui peut compromettre la sécurité de votre domicile.

Il y a également des répercussions liées à l'exactitude des profils élaborés par les explorateurs de données. On a fait grand cas de l'utilisation des profils de réseaux sociaux pour déterminer l'employabilité d'une personne ou pour accepter sa candidature dans un établissement d'enseignement postsecondaire. Cependant, le suivi et le profilage des habitudes de navigation en ligne entraînent également des conséquences très préoccupantes compte tenu du fait qu'ils sont presque invisibles. Si ces pratiques n'étaient utilisées que pour le marketing ciblé, les risques d'inexactitude pourraient sembler minimes (quoique cela puisse être problématique si certaines personnes ne reçoivent pas les mêmes avantages que d'autres). Si les profils étaient utilisés de façon plus générale, comme pour accorder des prêts, évaluer les risques d'assurance ou déterminer les risques à la sécurité nationale, les conséquences imprévues pourraient être plus graves. Il existe également d'autres questions de politiques publiques potentiellement graves qui n'ont pas trait à la protection de la vie privée, comme les obstacles à la liberté d'expression.

Le concept de « tort » semble être utilisé par certains pour distinguer les pratiques qui devraient nécessiter le consentement de celles qui ne le devraient pas. Il importe toutefois de mentionner que la LPRPDE ne comporte pas un tel concept. Elle exige plutôt que les fins soient

« acceptables », que la personne en soit informée et qu'on ait obtenu le consentement de cette dernière (le type de consentement peut varier). Les situations dans lesquelles le consentement n'est pas requis sont peu nombreuses. Les questions liées au consentement sont abordées en détail ultérieurement dans le présent rapport.

Dans le cadre de ses priorités stratégiques, le Commissariat a suivi les progrès réalisés dans le secteur de la gestion de l'identité^{xxiv}. La gestion de l'identité peut être utile, car elle fournit aux utilisateurs des moyens plus efficaces de contrôler leurs renseignements personnels, mais elle a également des répercussions sur la protection de la vie privée en ce sens que, si elle n'est pas effectuée adéquatement, il peut être plus facile de lier les données à des identités distinctes. Nous nous intéressons aux idées sur l'« identité numérique » formulées par Kim Cameron^{xxv} et d'autres personnes. Les identités numériques doivent être souples pour correspondre parfois à l'identité naturelle et véritable et pour être parfois complètement distinctes. Les identités devraient permettre à tous de mener une vie publique et privée, en fonction du contexte. Les identités devraient également permettre de vérifier la véracité d'une allégation (âge légal pour consommer de l'alcool) tout en respectant le principe de la communication minimale (p. ex. ne pas révéler la date de naissance). Nous suivons les efforts visant à élaborer des métasystèmes d'identité qui permettent la création et la gestion efficaces d'identités différentes.

Le Commissariat est d'avis que les considérations relatives à la protection de la vie privée devraient être une composante essentielle de la conception de toute technologie ou de l'utilisation des technologies. Selon nos [observations](#) présentées récemment au gouvernement du Canada en vue de la Stratégie sur l'économie numérique, nous sommes d'avis que des mesures supplémentaires pourraient être prises afin d'éviter les problèmes relatifs à la protection de la vie privée ou d'atténuer les effets des nouvelles technologies sur la protection de la vie privée en faisant de la protection de la vie privée une partie intégrante du développement de l'économie numérique. D'autres autorités de protection des données ailleurs au Canada et dans le monde réclament que les lois sur la protection des données obligent que l'on tienne compte de la protection de la vie privée à l'étape de la conception des produits. La commissaire à l'information et à la protection de la vie privée de l'Ontario, Ann Cavoukian, défend depuis longtemps ce concept.

Le Commissariat croit également que la protection des renseignements personnels doit faire partie intégrante des processus et des modèles opérationnels fondés sur la technologie grâce à l'analyse minutieuse des activités des entreprises. Les évaluations des facteurs relatifs à la vie privée (EFVP) sont un outil pratique que le secteur privé devrait être encouragé à utiliser, car le fait de prêter une attention accrue à de telles analyses pourrait prévenir les problèmes.

Il serait probablement déraisonnable de s'attendre à ce que Louise et David lisent les énoncés relatifs aux répercussions sur la protection de la vie privée des nombreux services et pratiques opérationnelles en ligne, les comprennent et y consentent en l'absence de mesures de protection de la vie privée solides. La connaissance et le consentement sont des éléments clés de la LPRPDE, mais les organisations doivent tenir davantage compte d'autres principes et les intégrer aux technologies et aux modèles opérationnels.

Questions à commenter — Distinctions entre les domaines public et privé, et réputation:

- **Le Commissariat aimerait tenir d'autres discussions avec les intervenants sur la gestion de l'identité en ligne.**
- **Le Commissariat met l'industrie au défi de trouver des façons et des moyens de favoriser l'expiration des données et souhaite tenir d'autres discussions à cet égard. La LPRPDE indique clairement que les renseignements personnels ne doivent pas être conservés pour toujours.**

Mesures proposées

- **Le Commissariat continuera de surveiller et de financer les recherches sur les répercussions de l'évolution des perceptions de l'espace public et de l'espace privé (ainsi que sur la difficulté d'assurer une présence en ligne sur le plan professionnel et personnel) par l'entremise de son Programme des contributions.**
- **Le Commissariat mènera des recherches sur l'opinion publique à l'égard des perceptions des Canadiens relativement à la distinction entre les domaines public et privé^{xxvi}.**
- **Le Commissariat mènera des activités de sensibilisation et élaborera des pratiques exemplaires pour les organisations afin de soutenir la capacité des personnes de mener comme elles l'entendent une vie privée ou publique.**
- **Le Commissariat poursuivra ses efforts de sensibilisation du public axés sur les Canadiens.**
- **Le Commissariat collaborera avec Industrie Canada pour déterminer la meilleure façon d'intégrer aux pratiques du secteur privé l'utilisation des EFVP et les principes de la protection de la vie privée à l'étape de la conception des produits.**
- **Le Commissariat surveillera les travaux de nos collègues d'autres pays qui abordent ces questions et s'en inspirera, dans la mesure du possible.**

Ce que nous avons entendu — Il faut prêter une attention particulière aux enfants

Dans le cadre des consultations, on a mentionné que la distinction entre les domaines public et privé est encore plus importante pour les enfants, qui utilisent Internet de plus en plus jeunes et fournissent leurs renseignements personnels sur des sites Web sans savoir vraiment comment les renseignements seront utilisés et pour quelle raison. Les enfants comme David jouent principalement sur des sites commerciaux, qui semblent combiner le divertissement et le divertissement éducatif, où les jeux auxquels les enfants jouent, par exemple, sont un moyen de recueillir des renseignements sur ces enfants, soit la façon dont ils jouent, ce qu'ils aiment et la façon dont ils pensent. Bon nombre de ces sites ne font pas que recueillir des renseignements sur les enfants; en effet, comme dans le cas de Louise et de David, David utilise les renseignements de la carte de crédit de Louise pour s'inscrire aux jeux, et le site recueille ainsi

les renseignements de David, mais également ceux de sa sœur. Par ailleurs, certains sites demandent également aux enfants de divulguer des renseignements sur leurs parents.

Bon nombre de personnes ont signalé qu'il y avait un manque flagrant de transparence dans la façon dont les renseignements personnels sont recueillis ou utilisés; les parents qui souhaitent en apprendre davantage sur les pratiques de protection des renseignements personnels d'un site donné pourraient donc avoir de la difficulté. On a également discuté de la perception des enfants à l'égard de la protection de la vie privée. Les enfants croient qu'ils « discutent » uniquement avec des amis; ils ne sont pas conscients du « public invisible ». Ils considèrent que, si des adultes ont vu leurs renseignements ou les ont utilisés de façon inappropriée selon eux, c'est l'adulte qui a tort et qui devrait prendre des mesures correctives. On a également mentionné que les enfants ne comprennent pas le marketing avant d'atteindre un certain âge. Ils ne savent pas quand on leur présente ou non des publicités. Cela est un fait important, car les enfants qui utilisent Internet sont de plus en plus jeunes. Un participant de la consultation sur les enfants a indiqué qu'il fallait adopter une loi contre l'exploitation des enfants à des fins commerciales. Dans le cadre des discussions, l'Association canadienne du marketing a mentionné ses lignes directrices en rapport à la publicité destinée aux enfants. Cependant, un participant a signalé que bon nombre des pratiques en ligne ne respectent pas ces lignes directrices.

Observations du Commissariat

Le Commissariat partage les importantes préoccupations soulevées en ce qui a trait aux activités des enfants en ligne. Un changement à la LPRPDE qui permettrait d'aborder les préoccupations concernant quelques-unes des pratiques liées à la protection de la vie privée de certains sites Web destinés aux enfants est présentement à l'étude. Bien que le changement ne s'applique pas précisément aux enfants, il faudrait raisonnablement s'attendre à ce que le consentement, pour être considéré comme valide, soit fourni par une personne qui comprend la nature, l'objet et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels visés par le consentement. La LPRPDE requiert déjà le consentement valable, et on s'attend à ce qu'une telle modification améliore et clarifie cette exigence. Le Commissariat appuie le changement proposé à la LPRPDE concernant le consentement et la compréhension.

Conformément à notre position relative à la façon dont les technologies et les services sont créés, le Commissariat considère que des normes de base doivent être élaborées pour aider les parents et les éducateurs à s'assurer que les renseignements personnels des enfants sont protégés. Il faut mettre en œuvre un cadre qui permettra de mieux informer les parents et les éducateurs et qui, ultimement, protégera mieux les renseignements personnels d'enfants comme David. Nous savons que les spécialistes du marketing sont tenus de respecter certaines lignes directrices concernant la publicité destinée aux enfants, mais la publicité comportementale n'en fait pas partie.

Questions à commenter — Il faut prêter une attention particulière aux enfants

- **Le Commissariat aimerait recevoir des commentaires sur ce que pourraient être les normes de base concernant la protection des renseignements personnels des enfants et la façon dont elles pourraient être élaborées. Le Commissariat aimerait également obtenir des points de vue sur le type de cadre qu'il faudrait mettre en œuvre.**

Ce que nous avons entendu — La citoyenneté numérique est primordiale

Certains répondants ont affirmé que toutes les parties — les utilisateurs de tous âges, les entreprises et les organismes de réglementation — doivent être davantage sensibilisés à la façon dont leurs activités en ligne et hors ligne peuvent influencer sur leur existence. Généralement, les participants étaient d'avis qu'il faut en faire plus pour mieux informer les utilisateurs sur la protection de la vie privée en ligne et qu'il faut trouver des façons novatrices et créatives de le faire.

Observations du Commissariat

Le Commissariat est d'accord avec ce point de vue et considère que la protection de la vie privée devrait faire partie du programme de citoyenneté numérique pour veiller à ce que les personnes participant à l'environnement en ligne se comportent de façon à respecter nos droits, nos valeurs et nos règles d'éthique, et à soutenir l'interaction constructive et la confiance. Le Commissariat convient qu'il faut trouver des façons plus efficaces de sensibiliser les personnes pour les aider à comprendre les conséquences de leurs gestes. Dans nos propres travaux auprès des jeunes, nous avons constaté que les outils et les ressources pédagogiques suscitaient un grand intérêt et étaient en demande.

Comme nous l'avons toutefois mentionné dans nos [observations](#) présentées dans le cadre de la consultation du gouvernement du Canada sur la Stratégie sur l'économie numérique, les jeunes ne doivent pas être le seul point de mire. Les développeurs, chefs d'entreprise et utilisateurs de tous âges doivent bien connaître les principes relatifs à la protection de la vie privée si nous voulons protéger le marché en ligne du Canada.

Mesures proposées

- **Le Commissariat s'efforcera d'axer ses activités de protection de la vie privée en ligne sur les Canadiens adultes, qui peuvent être de nouveaux utilisateurs de l'environnement en ligne.**
- **Le Commissariat poursuivra le dialogue avec la communauté technique sur la façon d'intégrer les principes contenus dans la LPRPDE aux interfaces-utilisateurs et aux technologies connexes.**

-
- **Le Commissariat, dans le cadre de ses activités de sensibilisation du public, continuera de s'adresser aux jeunes et de trouver des façons novatrices et créatives de s'y prendre. Le Commissariat continuera de trouver des façons de collaborer avec ses homologues provinciaux et territoriaux dans le cadre de telles activités.**

II.IV LPRPDE — Principes de la protection de la vie privée

Dans le cadre des consultations, nous avons constaté que les plus importants enjeux liés aux principes de protection de la vie privée établis dans la LPRPDE pour l'industrie, les personnes et le Commissariat semblent découler du suivi, du profilage et du ciblage en ligne. La définition des renseignements personnels, la détermination des types adéquats de consentement et la perte de contrôle de ses propres renseignements personnels, voilà les questions fondamentales auxquelles il faut prêter attention si nous voulons mieux protéger la vie privée des Canadiens de tous âges.

Ce que nous avons entendu : LPRPDE — souplesse et neutralité

Bon nombre des personnes et organisations qui ont fourni des observations écrites ou pris part aux consultations ont indiqué que la LPRPDE présente les forces suivantes : elle est neutre sur le plan technologique, axée sur des principes et donc souple. C'est un point de vue que le Commissariat a appuyé et il continue de le faire. Selon nous, la LPRPDE a été un instrument dynamique et efficace qui a renforcé le droit des Canadiens à la vie privée. Néanmoins, il existe certaines questions liées à la portée de la protection des renseignements personnels et aux principes équitables à la base de la LPRPDE que nous avons soulevées dans les observations écrites et dans le cadre des consultations et qui doivent faire l'objet d'un examen minutieux. Elles sont abordées ci-dessous.

Définition des renseignements personnels

Le fait de déterminer si les données recueillies, utilisées ou communiquées sont des renseignements personnels est une étape fondamentale pour définir la portée de l'application de la LPRPDE dans la situation en question.

Nous avons constaté des divergences dans la manière dont les différents répondants décrivent les renseignements recueillis quand les activités en ligne des personnes sont suivies.

- Deux des 21 observations écrites (dont l'une provenait d'une association) établissaient une distinction entre les données recueillies par l'entremise de publicités ou les renseignements non signalétiques, et les renseignements personnels ou les renseignements permettant d'identifier une personne.
- Une autre association se demandait si les données sur la navigation et les adresses IP étaient des renseignements personnels.
- Un répondant a indiqué qu'il s'adonnait à la pratique de la publicité axée sur les intérêts, mais que cela ne supposait pas la collecte, l'utilisation ou la communication de renseignements personnels.
- Dans une autre observation écrite, on mentionnait la distinction faite par bon nombre d'entreprises en ligne, qui utilisent souvent l'expression « renseignements permettant

d'identifier une personne » tandis qu'au Canada, l'expression utilisée est « renseignements personnels ».

- Les variations d'ordre terminologique ont été reflétées dans les discussions en table ronde au cours des consultations. Dans une des discussions, on a utilisé l'expression renseignements « confidentiels », et sa signification est semblable à celle de « renseignements permettant d'identifier une personne ».

Outre les divergences terminologiques, il semble que les répondants et les participants étaient nombreux (sans être unanimes) à dire que le suivi, le profilage et le ciblage en ligne touchent la protection de la vie privée.

Observations du Commissariat

Actuellement, dans la LPRPDE, on entend par renseignement personnel « tout renseignement *concernant* un individu *identifiable*, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail » (c'est nous qui soulignons).

La LPRPDE ne définit pas les « renseignements permettant d'identifier une personne », les « renseignements non signalétiques » et les « renseignements confidentiels ». L'expression « renseignements permettant d'identifier une personne » est utilisée dans d'autres administrations et elle se rapporte habituellement à un ensemble restreint de renseignements qui peuvent être utilisés pour identifier précisément une personne. Voici quelques exemples : le nom, l'adresse, le numéro d'identification national ou le numéro de permis de conduire d'une personne donnée. En comparaison, le concept de renseignement personnel établi dans la LPRPDE a été interprété par les tribunaux et le Commissariat de façon à s'appliquer de façon plus générale.

En 2008, le Commissariat a diffusé un document d'[interprétation](#) qui fournissait des interprétations générales de l'expression « renseignement personnel » par des tribunaux et résumait la position adoptée par le Commissariat dans différentes plaintes liées à la LPRPDE dans le cadre desquelles on débattait la question des renseignements personnels.

Habituellement, le Commissariat adopte une approche générale et contextuelle pour déterminer si un renseignement est personnel ou non. Il importe de mentionner une conclusion de 2003 selon laquelle les renseignements emmagasinés par les témoins temporaires et permanents constituent des renseignements personnels^{xxvii}. Le Commissariat a également déterminé qu'une adresse du protocole Internet (IP) est un renseignement personnel si on peut l'associer à une personne identifiable^{xxviii}.

Parmi d'autres exemples dignes de mention, on retrouve une enquête sur la collecte et l'utilisation de renseignements du système de positionnement global placé dans les véhicules d'une entreprise, qui en est arrivée à la conclusion que ces renseignements étaient des renseignements personnels puisqu'un lien pouvait être établi entre les renseignements recueillis et les employés qui conduisent les véhicules. On a mentionné que les employés sont identifiables même s'ils ne sont pas identifiés à tout moment par tous les utilisateurs du système^{xxix}. Les renseignements recueillis au moyen de l'identification par radiofréquence (IRF) pour effectuer le suivi de valises, de produits de détail et d'achats personnels, et de trouver ces derniers, peuvent être considérés comme des renseignements personnels de toute personne identifiable associée à ces éléments^{xxx}.

Qu'est-ce que cela signifie pour les données recueillies au moyen du suivi en ligne?

Le Commissariat est préoccupé par les divergences relatives à la terminologie utilisée dans les observations et les discussions. On semble tenter d'insister sur le fait que les renseignements recueillis sont anonymes (non signalétiques ou non confidentiels), probablement parce qu'ils ne permettent pas d'identifier la personne par son nom (certains répondants considèrent qu'il s'agit de renseignements permettant d'identifier une personne). Cependant, il est de plus en plus difficile de faire en sorte que les renseignements demeurent entièrement anonymes en raison des progrès technologiques.

Certains répondants aimeraient que le Commissariat fournisse une orientation afin de déterminer le moment où des renseignements découlant d'un suivi deviennent des renseignements concernant une personne identifiable. Sans mener d'enquête, il ne serait pas opportun que le Commissariat indique de façon définitive que toutes les données recueillies en ligne sont ou ne sont pas des renseignements personnels. Nous interprétons habituellement les renseignements personnels de façon globale. Dans certains cas, nous avons déterminé que, par exemple, les adresses IP constituent des renseignements personnels, notamment quand elles sont associées aux activités en ligne d'une personne. Nous avons également conclu que les témoins étaient des renseignements personnels. Nous reconnaissons qu'il existe des zones grises et qu'il faut toujours tenir compte du contexte, mais les exemples de conclusions du Commissariat présentés ci-dessus montrent que les renseignements recueillis par l'entremise du suivi, du profilage et du ciblage en ligne ont déjà été considérés comme des renseignements personnels, et les organisations devraient en tenir compte dans l'élaboration de leurs pratiques.

Nous constatons que la FTC a adopté une approche globale dans son document intitulé [Self-Regulatory Principles for Online Behavioral Advertising](#), appliquant la portée non seulement aux renseignements permettant d'identifier une personne mais également à ceux qui ne le permettent pas, mentionnant que la notion traditionnelle de ce qu'englobent ces types de renseignements devient de moins en moins importante et ne devrait donc pas, en soi, servir à déterminer les mesures de protection pour les données des consommateurs. Elle poursuit en soulignant qu'elle et d'autres intervenants reconnaissent depuis longtemps que ces renseignements peuvent poser problème sur le plan de la protection de la vie privée^{xxxii}. En ce qui a trait à la publicité comportementale, le Groupe de travail Article 29 de l'Union européenne a récemment fourni une [opinion](#) sur la pratique, mentionnant que les méthodes (utilisées en publicité comportementale) « impliquent souvent le traitement de données à caractère personnel, telles qu'elles sont définies à l'article 2 de la directive 95/46/CE^{xxxii} ».

Nous croyons donc que l'approche globale et contextuelle que le Commissariat a déjà utilisé par le passé pour définir les données ne sera pas incompatible avec les points de vue des organismes de réglementation internationaux à cet égard.

Mesure proposée

- **Le Commissariat mettra à jour, au besoin, son document d'interprétation relativement aux renseignements personnels.**

Consentement, consentement valable et transparence

Nous avons entendu beaucoup de discussions sur le type de consentement approprié pour le suivi, le profilage et le ciblage en ligne, et presque tous les participants ont convenu que la transparence est essentielle à cette pratique. En général, les entreprises et les associations industrielles étaient plutôt en faveur du consentement négatif en ce qui a trait à la publicité comportementale, et l'une d'entre elles a indiqué qu'il faudrait donner un consentement positif quand il s'agit de renseignements de nature délicate. Cependant, une autre association privilégiait le consentement positif pour la publicité comportementale, que les renseignements soient de nature délicate ou non.

Bon nombre d'associations ont mentionné que des mesures d'autoréglementation sont prises pour régler le problème de la transparence. Parmi les stratégies potentielles pour aborder la question du consentement, on a mentionné que les réseaux de publicité et les sites Web pourraient insérer des liens évidents au sujet des pratiques de publicité. Nous avons entendu parler des différentes façons d'assurer la transparence (et le consentement négatif) en plaçant une icône spéciale (icône « i ») sur laquelle on pourrait cliquer pour obtenir immédiatement de l'information^{xxxiii}. Nous avons également pris connaissance de différentes initiatives de sensibilisation, notamment un site qui fournit aux personnes des renseignements sur la protection de la vie privée en ligne. Certains sites Web commencent à offrir aux utilisateurs la possibilité de gérer les intérêts qu'un annonceur ou un réseau de publicité a pu associer à ses habitudes de navigation. On convenait que les personnes ne devraient pas à avoir à chercher des renseignements. On convenait également que les renseignements doivent être faciles à comprendre, mais suffisamment détaillés; cependant, on a affirmé que la pratique est en elle-même relativement complexe et difficile à expliquer.

Les personnes qui étaient plus critiques à l'égard des pratiques se demandaient si l'obligation énoncée dans la LPRPDE selon laquelle le consentement doit être valable était respectée, car les descriptions des pratiques, s'il y en a, sont souvent peu détaillées. Une personne se demandait si tous les renseignements recueillis étaient nécessaires aux fins de la publicité.

Observations du Commissariat

Il est difficile de déterminer si une donnée constitue ou non un renseignement personnel, et la question du consentement est également complexe. Nous constatons que bon nombre d'associations industrielles déploient des efforts pour intégrer la transparence et les autres pratiques équitables en matière de renseignements à l'orientation qu'elles fournissent à leurs membres. Voici la façon dont le Commissariat a abordé les questions du consentement, du consentement valable et de la transparence par le passé, et les problèmes que posent le suivi, le profilage et le ciblage en ligne par rapport au consentement.

Qu'est-ce que le Commissariat a dit par le passé au sujet du consentement?

En 2004, le Commissariat a diffusé une [fiche d'information](#) sur le consentement, qui demeure pour l'essentiel notre interprétation des exigences liées à la connaissance et au consentement établies dans la LPRPDE. Nous avons appliqué ce raisonnement à divers types de pratiques et déterminé le type de consentement approprié dans différentes situations.

La LPRPDE stipule que la collecte, l'utilisation ou la communication de renseignements personnels doivent se faire au su de l'intéressé et avec son consentement, sauf dans les situations où cela est inapproprié^{xxxiv}. Il y est également indiqué que le type de consentement peut varier selon les circonstances et la nature des renseignements. Pour déterminer le type de consentement à utiliser, les organisations doivent déterminer s'il s'agit de renseignements sensibles. Certains renseignements (comme les dossiers médicaux et les dossiers sur le revenu) sont presque toujours considérés comme sensibles, mais tous les renseignements peuvent être de cette nature, selon le contexte. Elle indique qu'il faut obtenir le consentement de la personne quand les renseignements sont susceptibles d'être considérés comme sensibles et que le consentement implicite est généralement suffisant quand les renseignements sont moins sensibles. Enfin, la *Loi* indique qu'en ce qui concerne l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes.

Le Commissariat a toujours considéré que le consentement positif (explicite) était la méthode de consentement privilégiée, mais que le consentement négatif peut être acceptable dans certaines situations.

Qu'est-ce que le consentement négatif?

L'organisation offre à une personne comme Louise l'occasion d'exprimer son désaccord envers une utilisation proposée. À moins que la personne ne prenne des mesures pour exprimer un consentement négatif à l'égard de l'utilisation prévue — c'est-à-dire, à moins qu'elle ne la refuse — l'organisation présume que le consentement a été donné et utilise l'information aux fins déterminées. Louise devrait être clairement informée qu'en omettant d'exprimer son refus, elle consent à ce que les renseignements personnels la concernant soient utilisés aux fins proposées.

Le Commissariat a eu l'occasion d'examiner le refus du consentement sous plusieurs angles. Cette option sert habituellement dans le cadre de l'utilisation ou de la communication de renseignements personnels à des fins secondaires de marketing. Les fins secondaires s'ajoutent à celles pour lesquelles l'information doit être recueillie au départ. Le Commissariat estime que pour recourir à un mécanisme de consentement négatif, par exemple pour obtenir un consentement pour l'utilisation de renseignements personnels à des fins secondaires de marketing, l'organisation doit répondre aux exigences suivantes :

- Il faut démontrer que les renseignements personnels ne sont pas sensibles compte tenu de leur nature et du contexte.
- La situation prévoyant le partage d'information doit être limitée et clairement définie selon la nature des renseignements personnels devant être utilisés ou communiqués ainsi que la portée de l'utilisation ou de la communication prévue.
- Les objectifs de l'organisation doivent être limités et nettement définis, et énoncés d'une manière claire et facile à comprendre.
- En règle générale, l'organisation devrait obtenir au moment de la collecte le consentement de la personne concernée pour utiliser ou communiquer les renseignements personnels.
- L'organisation doit mettre en place un mécanisme pratique pour le refus ou le retrait du consentement relativement à l'utilisation de renseignements personnels à des fins

secondaires. Le refus devrait prendre effet immédiatement et avant toute utilisation ou communication d'information aux nouvelles fins proposées^{xxxv}.

Notre position concernant le consentement positif par rapport au consentement négatif et les critères que nous avons élaborés, surtout en ce qui a trait au marketing, découlent de nos expériences avec les organisations traditionnelles. Cela a quelque peu évolué à la suite de notre examen de l'utilisation faite par les sites de réseautage social des renseignements personnels des utilisateurs pour la publicité^{xxxvi}. Nous avons tenu compte du rôle que joue la publicité dans le modèle opérationnel de ces sites et des renseignements qui sont considérés ou non comme sensibles dans ce contexte.

Le suivi, le profilage et le ciblage en ligne constituent un environnement très complexe dans lequel il faut déterminer le type de consentement approprié. Tout d'abord, la façon dont les données sont recueillies et utilisées est en grande partie invisible pour la plupart des utilisateurs, surtout pour les enfants. Il y a beaucoup d'intervenants (comme les sites Web et les réseaux de publicité), et l'utilisateur peut ne pas les connaître. Même Louise, qui s'y connaît relativement bien en matière de pratiques de suivi en ligne, est susceptible de ne pas savoir qui recueille ses données. Si elle est curieuse de connaître les types de renseignements recueillis et le type de profil qu'on lui attribue, il est probable qu'elle aura de la difficulté à savoir qui détient ses renseignements. Les questions liées à la responsabilité, à l'exactitude et à l'accès seront abordées ultérieurement dans le présent rapport.

La transparence et le consentement valable sont des questions importantes qui ont suscité beaucoup de discussions dans le cadre des consultations. Il est peut-être difficile de bien saisir la distinction entre « consentement positif » et « consentement négatif », mais une question à laquelle il faut absolument prêter attention est le *caractère valable*. Est-ce que les fins et les pratiques sont suffisamment claires pour que le consommateur fournisse un consentement valable? Il s'agit d'une question d'équité et d'une exigence aux termes de la loi. Et il s'agit selon nous d'un domaine qui nécessite davantage attention.

La LPRPDE exige que les organisations doivent être transparentes au sujet de leurs politiques et pratiques. Les renseignements fournis aux consommateurs sur le suivi et le ciblage en ligne sont, bien souvent, trop complexes ou constituent du jargon juridique. Souvent, les personnes ne souhaitent pas lire les avis concernant la protection de la vie privée, lesquels n'offrent la plupart du temps que deux choix : les accepter ou les refuser. Même s'ils sont bien écrits et faciles à comprendre, il faudrait trouver des façons d'encourager les gens à les lire. Nous avons entendu parler de progrès positifs concernant l'information transmise aux consommateurs au sujet du suivi et du profilage en ligne et de la publicité comportementale. Dans le cadre des consultations, on a discuté de l'icône « i », qu'il faudrait ajouter à la plupart des publicités en ligne qui font appel aux données comportementales, afin de renseigner les consommateurs sur la publicité comportementale et ce qui survient quand ils visitent un site Web donné. On a également discuté de la possibilité de mieux rédiger les politiques sur la protection de la vie privée et de les rendre plus accessibles (avis multiples, information sur la protection de la vie privée semblable à l'étiquetage nutritionnel); il s'agit de quelques exemples qui pourraient mieux renseigner les consommateurs. Le consentement valable est encore plus difficile à obtenir dans l'environnement des télécommunications sans fil. L'écran est petit et il est difficile de fournir aux utilisateurs les détails nécessaires.

La LPRPDE oblige également que les fins pour lesquelles les renseignements personnels sont recueillis, utilisés et communiqués soient déterminées, généralement au moment de la collecte.

En ce qui a trait à la publicité comportementale, lorsque des renseignements sont fournis à côté de la publicité, cela se fait après que les renseignements ont été recueillis et utilisés d'une façon donnée. Nous sommes encouragés par l'adoption de façons novatrices de mieux informer les gens et croyons que l'icône « i » constitue un pas dans la bonne direction, mais le consentement négatif peut ne pas convenir à bon nombre d'utilisateurs.

D'aucuns diront que l'utilisateur sera constamment interrompu si on lui demande son consentement chaque fois qu'il ouvre une session. Dans le cadre des consultations, on a discuté des témoins : les utilisateurs peuvent décider de bloquer ou de supprimer les témoins, puis de refuser les publicités en cliquant dessus (si ces dernières permettent qu'un utilisateur les refuse). On ne peut toutefois pas s'en remettre uniquement aux témoins et à la capacité des personnes à utiliser les outils qui leur sont offerts en matière de protection de la vie privée. Par exemple, les témoins Flash ne sont habituellement pas visibles aux utilisateurs, et les options pour les contrôler ou les supprimer sont habituellement inexistantes ou très difficiles à trouver. Les témoins Flash peuvent être utilisés pour recréer des témoins Web quand ces derniers sont supprimés. Les supertémoins sont souvent invisibles pour l'utilisateur, à qui, bien souvent, on ne fournit pas les outils pour contrôler les renseignements emmagasinés. Les navigateurs offrent certains outils pour que les utilisateurs puissent contrôler la collecte de leurs activités de navigation, mais ils sont limités puisque, généralement, ils suppriment certains types de témoins, mais pas d'autres. Afin de supprimer l'ensemble des différents types de témoins et des renseignements emmagasinés sur le Web, les utilisateurs doivent installer et utiliser des applications complémentaires spéciales. Est-il raisonnable de s'attendre à ce que l'utilisateur moyen agisse de la sorte? Et est-ce que l'utilisateur moyen doit s'attendre raisonnablement à prendre de telles mesures uniquement pour prévenir le suivi et le profilage? Une association industrielle a affirmé qu'il faudrait fournir en un seul clic des renseignements sur la publicité comportementale et l'occasion de refuser ce type de publicité (au moyen d'un témoin permanent). Si cette solution fonctionne comme prévu et qu'elle est mise en œuvre globalement, elle pourrait permettre de répondre à certaines des préoccupations liées à la convivialité pour les utilisateurs.

Pour déterminer le type de consentement approprié, il faut également déterminer si les renseignements sont de nature délicate. Cette question comporte des zones grises. Un renseignement de nature délicate pour certains peut ne pas l'être pour d'autres, et un renseignement peut être de nature délicate dans un contexte donné, mais pas dans un autre. Le problème lorsqu'on essaie de déterminer si un renseignement est de nature délicate en ligne, c'est que l'environnement ne fournit pas de contexte.

Certaines des personnes qui ont soumis des commentaires font valoir que la vie privée pourrait être mieux protégée si l'on prêtait attention à l'utilisation des renseignements. Il faudrait se demander si l'utilisation en question est nuisible ou non pour la personne. Ce ne sont pas toutes les utilisations qui sont nuisibles; bon nombre de personnes pourraient convenir que le fait de recevoir des publicités axées sur leurs intérêts n'est pas un affront à la dignité, mais considérer que l'utilisation des activités en ligne pour évaluer leur cote de crédit est nuisible. Cependant, le concept de tort n'est pas établi dans la LPRPDE. La *Loi* met l'accent sur la collecte, l'utilisation ou la communication de renseignements personnels à des fins *acceptables*. Il est obligatoire d'informer la personne de ces fins et d'obtenir son consentement. Si l'on ne s'intéresse qu'à l'utilisation finale, on fait également fi du fait que bon nombre de personnes sont réticentes à l'idée d'être « suivies » quand elles sont en ligne.

Existe-t-il une approche pratique à l'évaluation de la nature délicate des renseignements et à la détermination du type de consentement approprié?

Certaines entreprises limitent déjà leurs activités de suivi et n'utilisent pas certains renseignements qui sont généralement considérés comme étant de nature délicate (comme les renseignements sur la santé). Le Commissariat croit qu'il s'agit là d'une approche utile et pratique.

Nous avons également entendu des propos sur un registre d'interdiction de suivi. C'est une idée qui fait du chemin aux États-Unis et qui nous intéresse. Elle offre aux personnes un moyen pratique de protéger leurs activités de navigation, mais elle est également liée à des questions techniques et propres aux administrations. Pour qu'elle se réalise, il faudrait également que les personnes aient une connaissance raisonnable de la façon dont le suivi est effectué et des fins pour lesquelles les renseignements sont utilisés, et qu'elles prennent des mesures actives pour s'inscrire au registre.

Un changement proposé à la LPRPDE ferait en sorte que le consentement ne serait considéré comme valide que s'il est raisonnable de croire que la personne comprend la nature, l'objet et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles elle a consenti. Cette modification pourrait améliorer et clarifier l'obligation du consentement valable et aborder certaines préoccupations liées au suivi, au profilage et au ciblage d'enfants en ligne, surtout ceux qui sont trop jeunes pour comprendre la publicité. Cela entraînerait toutefois des répercussions sur le caractère approprié de l'utilisation du consentement négatif pour le suivi et le ciblage d'enfants.

Fait intéressant concernant les services géodépendants, nous croyons comprendre que le milieu canadien de la publicité sur les appareils sans fil semble être conscient des préoccupations des Canadiens concernant le fait que les autres peuvent savoir où ils se trouvent et de leur méfiance à l'égard de la réception de publicités en fonction de cela. On nous a mentionné que les dispositifs personnels (comme les téléphones cellulaires) devaient être « privés » et précisé que l'on demande aux utilisateurs leur consentement positif avant de leur présenter des publicités fondées sur l'emplacement. Nous considérons qu'il s'agit d'une approche positive et appropriée.

Fins appropriées

Au moins un répondant se demandait si le suivi était approprié en soi. Il s'agit d'une question importante. La LPRPDE comporte une disposition selon laquelle une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances^{xxxvii}. Nous n'indiquerons pas si, selon nous, le profilage et le ciblage sont appropriés en soi, mais nous insistons sur le fait que les entreprises doivent tenir compte de cette disposition, surtout en raison du malaise que provoquent chez bon nombre de personnes le suivi, le profilage et le ciblage. Il se peut qu'elles apprécient certains des services qu'elles reçoivent mais, malgré cela, il faut les informer et leur permettre de décider elles-mêmes ce qu'elles veulent et ce qu'elles ne veulent pas.

Questions à commenter — Consentement, consentement valable et transparence

- **Le Commissariat continuera de collaborer avec l'industrie pour élaborer la meilleure approche possible pour veiller à ce que les personnes fournissent un consentement valable à des pratiques opérationnelles légitimes. Il s'agit d'un domaine dans lequel la technologie peut être utile. Par conséquent, nous aimerions recevoir des commentaires sur la meilleure façon de réaliser cet objectif.**
- **Le Commissariat continuera d'axer ses activités de sensibilisation sur les personnes afin de les aider à mieux se protéger en ligne. Pour ce faire, on examinera la meilleure façon d'aider les personnes à prêter attention aux explications sur la protection de la vie privée qui leur sont fournies. Le Commissariat aimerait recevoir des commentaires sur la meilleure façon de réaliser cet objectif.**

Mesures proposées

- **Le Commissariat appuiera ou mènera des recherches sur les innovations en matière d'explication du droit à la vie privée et examinera le bien-fondé de la promotion de certains types d'explication.**
- **Le Commissariat, en collaboration avec ses homologues provinciaux et territoriaux, continuera de trouver des façons d'aider à informer les parents de la nécessité de protéger les renseignements personnels de leur famille en ligne.**

Limites de l'utilisation ou de la communication

Même si la majorité des observations écrites que nous avons reçues concernaient la publicité comportementale, certaines discussions ont été tenues dans le cadre des consultations sur les autres utilisations possibles des renseignements liés au profil et le peu de contrôle à l'égard des renseignements personnels que les utilisateurs comme Louise auraient. Des préoccupations ont été soulevées au sujet des utilisations que les personnes connaissent, soit l'utilisation des données dans un réseau social pour mener des évaluations psychologiques, évaluer la solvabilité ou appliquer la loi, pour ne nommer que ces quelques exemples. Généralement, les gens considéraient que le recours au suivi et au profilage pour leur présenter des publicités pertinentes était une chose, mais que l'utilisation de telles données ou de renseignements liés au réseautage social pour d'autres motifs inconnus était déconcertante. Certains s'inquiétaient du fait que, comme les pratiques sont pour la plupart invisibles pour les utilisateurs, la capacité d'entreposer des données pendant une période indéterminée existe et que, la technologie de traitement des données pour de nouveaux usages évoluant, la possibilité de trouver de nouvelles utilisations peut être très attrayante. Des données pourraient également être vendues, et les gens pourraient ne jamais en être au courant. Cependant, certains représentants de

l'industrie ont affirmé qu'aux termes de la LPRPDE, il existait des exigences selon lesquelles il fallait demander le consentement pour les nouveaux usages de renseignements, et que la loi protège les personnes et leur offre des recours quand les renseignements sont utilisés de façon inappropriée.

Certains ont mentionné qu'en tant que société, nous devrions être préoccupés par le volume de données recueillies par de grandes sociétés. Dans le cadre de certaines discussions, on a affirmé que les lois étaient déraisonnablement permissives en ce qui a trait à la collecte de renseignements par les entreprises privées — lesquelles semblaient en savoir plus sur nous que nous en savons nous-mêmes — et à l'application de la loi. On a soulevé l'argument selon lequel les autorités chargées de l'application de la loi doivent obtenir un mandat pour accéder à des renseignements sur nous, mais des lois permettent aux entreprises privées de divulguer des renseignements à la police à notre insu et sans notre consentement — et ces données sont de plus en plus parlantes.

Observations du Commissariat

Nous avons reçu 21 observations écrites, mais nous aurions aimé recevoir une rétroaction d'un plus vaste éventail d'organisations. Il nous aurait été utile d'obtenir leurs points de vue sur la publicité comportementale et sur certaines autres utilisations des renseignements recueillis par l'entremise du profilage.

Par exemple, nous savons qu'aux États-Unis, les profils élaborés en fonction des activités des personnes sur les sites de médias sociaux sont utilisés non seulement pour cibler les consommateurs et leur offrir de nouveaux produits et services, mais également pour prendre des décisions concernant l'octroi de prêts^{xxxviii}. Dans le cadre de ce processus, appelé surveillance des médias sociaux, on fait appel aux renseignements figurant sur les sites de réseautage social comme Facebook et Twitter, aux commentaires affichés sur des sites comme Amazon et aux revues sur des sites comme Yelp ou aux entrées de blogue pour élaborer des graphiques sociaux. Compte tenu de l'expansion du marketing personnalisé et des recherches qui montrent l'influence qu'exercent les amis sur les décisions d'achat, les explorateurs de données ont formulé l'hypothèse selon laquelle les renseignements sur les comportements de vos amis peuvent être utilisés pour mieux prévoir votre comportement. En d'autres mots, les renseignements personnels d'autrui deviennent vos propres renseignements personnels et, sans votre consentement et à votre insu, ces derniers influenceront sur les décisions prises à votre égard^{xxxix}.

On a mentionné que lorsque les gens indiquent où ils se trouvent par l'entremise de services géodépendants, ils montrent où ils ne sont pas. Certains ont allégué que le secteur de l'assurance pourrait augmenter les primes ou refuser les demandes de clients qui utilisent des services tels Loopt et Foursquare, qui indiquent où ces clients se trouvent.

Mises à part des discussions générales tenues à ce sujet dans le cadre des consultations, peu de renseignements ont été fournis sur l'ampleur de l'utilisation de ces données sociales au Canada. Ces renseignements sont-ils utilisés à d'autres fins au Canada? Qu'en est-il de la combinaison de renseignements figurant dans les bases de données hors ligne, comme les renseignements recueillis grâce à des cartes de fidélité et des coupons remis en ligne pour des magasins traditionnels? Nous n'avons pas même obtenu un aperçu complet de l'environnement

de la publicité comportementale^{xl}. Nous sommes préoccupés par le fait que nous ignorons certains aspects importants de cette pratique et d'autres pratiques qui n'ont pas fait l'objet de discussions approfondies dans le cadre des consultations, notamment le jeu en ligne. Le Commissariat est d'avis que, dans l'intérêt des Canadiens, il faut tenir une discussion publique sur l'état de certaines pratiques, l'orientation qu'elles pourraient prendre et le fait que le public les accepte ou non.

Le Commissariat convient qu'il est essentiel que les utilisateurs puissent contrôler leurs renseignements personnels. Selon nous, des pratiques plus transparentes et des dispositions plus claires sur le consentement feront en sorte que les utilisateurs comme Louise auront un plus grand contrôle. Nous considérons également que l'amélioration de l'architecture pourrait fournir de meilleures mesures de protection de base. Nous sommes d'accord avec le participant qui a affirmé que la LPRPDE doit obliger les organisations à obtenir le consentement des utilisateurs pour chaque nouvelle utilisation des renseignements personnels. Cependant, si l'on ne s'appuie que sur les plaintes qui nous sont présentées dans de tels cas, des pratiques douteuses pourraient passer inaperçues.

Certains répondants ont également suggéré que le Commissariat prête attention à l'utilisation du suivi et du profilage en ligne par le gouvernement. Le Commissariat est au courant des utilisations possibles de ces renseignements à des fins gouvernementales et partage les nombreuses préoccupations soulevées à cet égard dans le cadre des consultations.

Questions à commenter – Autres utilisations et modes de communication

- **Le Commissariat aimerait obtenir des points de vue et des commentaires supplémentaires sur les pratiques actuelles et futures de suivi et de profilage en ligne (à l'exception de la publicité comportementale) au Canada.**

Mesures proposées

- **Le Commissariat incite les associations de l'industrie à continuer de collaborer avec leurs membres afin de leur rappeler que l'obtention du consentement pour les nouvelles utilisations est un facteur essentiel de la protection de la vie privée aux termes de la LPRPDE. Le Commissariat fera part de nos points de vue aux associations, au besoin.**
- **En ce qui a trait à l'utilisation par le gouvernement des renseignements en ligne, le Commissariat continuera de surveiller les progrès dans ce domaine et fera part de nos préoccupations aux parties pertinentes.**

Mesures de protection et conservation

Des préoccupations étroitement liées aux utilisations secondaires des renseignements personnels ont été soulevées, au sujet des mesures de protection et de la conservation des renseignements. Les participants qui étaient préoccupés par les utilisations secondaires des renseignements personnels ont affirmé que les questions de sécurité et la capacité d'entreposer des données pendant une période indéterminée étaient des facteurs qui peuvent contribuer aux

utilisations inadéquates ou aux multiples utilisations. Les associations de l'industrie reconnaissent l'importance des mesures de protection et de conservation des renseignements, et les modèles d'autoréglementation que bon nombre d'entre elles ont mis en œuvre comportent des exigences liées à la sécurité des données et à la conservation limitée.

Nous avons également entendu dans le cadre des discussions que, dans l'environnement numérique, les données peuvent perdurer, qu'il est moins dispendieux d'entreposer des données que de les supprimer et qu'il pourrait y avoir des façons potentielles d'utiliser les données de manière très attrayante. Certains ont affirmé que la suppression des données en ligne est ardue, voire impossible.

Observations du Commissariat

Le Commissariat convient que les mesures de protection et la conservation sont des questions importantes, et nous sommes heureux que l'industrie les ait intégrées à ses modèles d'autoréglementation, car elles sont également comprises dans la LPRPDE, que ses membres doivent respecter. Plus les modèles d'autoréglementation ressembleront aux lois que les entreprises œuvrant à l'échelle internationale doivent respecter, plus il sera facile pour les organisations d'être raisonnablement certaines que leurs pratiques satisfont aux différentes exigences réglementaires d'autres pays.

La cybersécurité est une préoccupation sérieuse qui ne cesse de croître. Il existe un certain nombre de facteurs qui contribuent à ce problème, notamment le volume accru de données électroniques entreposées et traitées, la complexité croissante du matériel et des logiciels informatiques et l'omniprésence des dispositifs informatiques, qui sont souvent portables (téléphones intelligents, assistants numériques, ordinateurs portables). Le Commissariat est heureux que le gouvernement du Canada ait apporté des modifications pour que le signalement des atteintes soit obligatoire, car cela pourrait renforcer les exigences de sécurité.

Nous partageons la préoccupation selon laquelle l'existence indéfinie des données en ligne pourrait avoir des répercussions sur la réputation des personnes et donner lieu à des utilisations inadéquates. Nous sommes également d'avis qu'il s'agit d'un problème qui nécessite des solutions techniques afin de satisfaire aux exigences stratégiques et législatives qui consistent à ne pas conserver les renseignements personnels indéfiniment. On a abordé ce sujet dans le présent rapport dans la section sur l'absence de distinction claire entre les domaines public et privé et la réputation.

Mesures proposées

- **Le Commissariat encourage l'industrie à élaborer des approches techniques afin d'aborder les problèmes liés à la conservation.**
- **Le Commissariat encourage le CRTC à élaborer une directive de référence relativement à la protection des renseignements personnels qui combinerait les règlements actuels visant la publicité radiodiffusée et en ligne, et les mesures de protection pour assurer la confidentialité des renseignements des consommateurs.**
- **Le Commissariat collaborera avec Industrie Canada pour élaborer une directive sur l'élimination des données.**

Accès à l'information, correction et exactitude

Pour atténuer les préoccupations liées à la réputation, il faudrait que les gens puissent accéder à leurs propres renseignements personnels et être en mesure de les corriger. Cependant, bon nombre de participants ont mentionné que les personnes ont souvent du mal à savoir qui détient leurs renseignements personnels (outre les organisations à qui elles ont donné directement leurs renseignements), la façon dont ils sont utilisés et la manière dont elles peuvent corriger les erreurs. Ce problème est aggravé par le fait que les renseignements sont souvent détenus dans un autre pays (on aborde ce sujet en détail dans la section sur l'informatique dans les nuages). Comme le suivi et le profilage sont en grande partie invisibles pour la plupart des utilisateurs, ces derniers sont susceptibles d'ignorer la situation et, donc, d'avoir peu à dire sur la façon dont leurs renseignements sont recueillis, utilisés ou communiqués.

Nous avons entendu parler de certaines techniques novatrices élaborées par des organisations qui offrent une myriade de services Web aux utilisateurs comme Louise pour qu'ils connaissent les renseignements que ces organisations détiennent sur eux. Certaines préoccupations ont été soulevées quant au fait que des données inexactes pourraient être utilisées pour prendre des décisions à l'égard de personnes, ce qui pourrait entraîner différentes conséquences, en fonction de la façon dont les données sont utilisées.

Observations du Commissariat

Le Commissariat est d'accord avec le fait que la capacité d'accéder à ses propres renseignements personnels et de les corriger est un élément clé du contrôle de ses renseignements personnels. Nous sommes conscients que l'accès et la correction peuvent être plus ardues pour les personnes et les organisations dans l'environnement en ligne. Néanmoins, nous considérons que la technologie pourrait fournir certaines réponses concernant la façon de satisfaire à ces exigences aux termes de la LPRPDE.

Mesure proposée

- **Le Commissariat encourage l'industrie à trouver des façons novatrices de respecter les dispositions sur l'accès aux renseignements, la correction et l'exactitude afin de satisfaire aux exigences de la LPRPDE.**

Responsabilité

La responsabilité englobe toutes ces questions. Les associations de l'industrie qui ont fourni des observations écrites ont reconnu qu'il s'agit d'un sujet qu'il faut aborder. Qui effectue le suivi, où les personnes doivent-elles se rendre pour examiner leurs profils et les corriger, qui protège leurs renseignements personnels, à qui doivent-elles s'adresser pour retirer leur consentement, et qui s'occupe d'elles quand elles présentent une plainte? Certains travaux sont effectués dans ce domaine afin d'accroître la transparence des pratiques et d'offrir aux gens davantage de renseignements sur le suivi, le profilage et le ciblage en ligne.

Observations du Commissariat

Le Commissariat convient que la responsabilité est essentielle pour garantir que les renseignements personnels d'utilisateurs comme Louise et David ne sont pas utilisés à des fins malveillantes et que ces derniers sont informés et qu'ils ont fourni un consentement valable concernant la façon dont leurs renseignements personnels sont recueillis et utilisés.

Nous reconnaissons les efforts que certaines organisations et les associations de l'industrie ou leurs membres déploient pour être responsables des activités de suivi, de profilage et de ciblage en ligne et nous les encourageons à continuer de prêter attention à cette composante importante de la protection de la vie privée.

Informatique dans les nuages

Le commerce de bijoux de Louise marche si bien que sa liste de clients augmente et qu'elle a récemment étendu sa gamme de produits. À mesure que sa petite entreprise prend de l'expansion, Louise se rend compte qu'elle devrait commencer à traiter ses documents électroniques de manière plus professionnelle. Toutefois, elle sent qu'elle aura besoin d'aide : elle n'est pas une experte en informatique et n'a pas beaucoup de temps à consacrer aux détails d'ordre technique. Elle entend beaucoup parler dernièrement des avantages de l'informatique dans les nuages et se demande si elle ne trouverait pas là les outils commerciaux dont elle a besoin.

Bien qu'elle ne s'en rende pas compte, Louise utilise déjà des services dans les nuages : elle se sert de Gmail pour sa communication d'affaires et de Flickr pour stocker les photos de ses créations, et elle accède à son compte commercial sur le Web, par l'entremise des solutions Internet de son institution financière. Elle envisage maintenant utiliser une application de carnet d'adresses dans les nuages pour tenir à jour sa liste de clients et de fournisseurs, et se servir de FreshBooks pour le suivi des dépenses et la facturation.

Bien que ces services dans les nuages intéressent Louise, elle entretient certaines réserves. Elle ne comprend pas tout à fait comment fonctionne la technologie et se sent intimidée par des termes qui ne lui sont pas plus familiers, comme « virtualisation ». Elle se demande aussi comment fonctionne le modèle d'affaires, et comment les fournisseurs de services gèreront son information. Elle craint par exemple ne pas pouvoir accéder à ses données en tout temps. Elle a entendu dire que ses données pourraient se retrouver dans un pays étranger et elle se demande quelles seraient les conséquences juridiques pour ses renseignements personnels et commerciaux. Elle se demande aussi comment ses données seront protégées contre les pirates informatiques et les malicieux.

III. En quoi consiste l'informatique dans les nuages?

L'informatique dans les nuages se définit de différentes façons : en général, il s'agit de la prestation de services sur le Web à partir d'ordinateurs situés à distance, permettant aux personnes et aux entreprises d'utiliser des programmes et des logiciels gérés par des tiers. Parmi les divers types de services offerts, mentionnons le stockage de fichiers en ligne, les sites de réseautage social, les sites de courrier électronique et les applications commerciales en ligne. Le modèle d'informatique dans les nuages permet l'accès à des données et des ressources informatiques partout où est une connexion réseau est offerte. L'informatique dans les nuages donne accès à un bassin commun de ressources, y compris de l'espace de stockage de données, des réseaux, de la puissance de traitement et des applications spécialisées pour les entreprises et les personnes.

En ce qui a trait à l'informatique dans les nuages, Louise joue différents rôles. Comme nous l'avons vu dans la première section du présent rapport, Louise utilise avidement les sites de réseautage social. Louise est également une entrepreneure et elle utilise des services dans les nuages, comme Gmail et Flickr, pour certains aspects de son entreprise. Elle envisage maintenant d'utiliser certains services dans les nuages pour l'aider à gérer les comptes de ses clients. Dans chaque situation, ses attentes et son rôle changent relativement à la protection de

la vie privée. Quand elle utilise un réseau social, elle interagit directement avec le service à titre de personne. Dans la mesure où ce service est véritablement lié de façon considérable au Canada et que, par son entremise, on recueille, utilise ou communique les renseignements personnels de Louise dans le cadre d'une activité commerciale, elle est protégée aux termes de la LPRPDE, et l'organisation est tenue de mettre en œuvre certaines pratiques en conformité avec la loi. Pour ce qui est de sa bijouterie, Louise mène une activité commerciale et traite des renseignements personnels. Elle est donc responsable des renseignements personnels qu'elle confie à un fournisseur de services dans les nuages.

Que ce soit les renseignements personnels de Louise ou ceux de ses clients qui sont détenus par le service dans les nuages, il existe des enjeux liés à leur protection. Voici un aperçu de ce que nous avons appris des observations écrites et des discussions tenues à Calgary, de nos observations, des questions pour lesquelles nous aimerions recevoir des commentaires et de certaines mesures proposées.

III.I Ce que nous avons appris

Bon nombre des 11 observations écrites que nous avons reçues et des discussions tenues dans le cadre d'un événement public à Calgary ont fourni des détails et des explications utiles sur l'informatique dans les nuages et les modèles connexes.

La [définition](#) élaborée par le National Institute of Standards and Technology (NIST) des États-Unis a été mentionnée par un certain nombre de répondants, et il vaut la peine de la fournir dans le présent rapport.

L'informatique dans les nuages est un modèle d'accès au réseau habilitant, pratique et sur demande comprenant un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, entreposage, applications et services) qui peut rapidement être activé et désactivé au moyen d'efforts minimes en matière de gestion ou d'une interaction minimale avec le fournisseur de services. Ce modèle, qui favorise l'accessibilité, est composé de cinq caractéristiques essentielles, de trois modèles de service et de quatre modèles de mise en œuvre^{xlii}. [Traduction]

Parmi ces caractéristiques, on compte le libre-service sur demande, l'accès global au réseau, un bassin de ressources, la souplesse rapide et les services mesurés. Les modèles de service sont les logiciels sous forme de service, la plateforme sous forme de service et l'infrastructure sous forme de service. Les services dans les nuages sont habituellement mis en œuvre par l'entremise d'une infrastructure dans les nuages privée, communautaire, publique ou hybride. Ces caractéristiques et ces modèles de service et de mise en œuvre sont décrits de façon plus détaillée dans la [définition](#) du NIST^{xlii}.

Un répondant a insisté sur les différences entre les infrastructures dans les nuages publique et privée, car elles peuvent avoir différentes répercussions relativement à la protection de la vie privée. Selon la définition du NIST, dans une infrastructure dans les nuages publique, l'infrastructure, qui est offerte au grand public ou à un grand groupe de l'industrie, est détenue par une organisation qui vend des services dans les nuages^{xliii}. Les infrastructures dans les nuages publiques offrent des ressources sur Internet. À titre d'exemples, on compte les services visant les consommateurs, comme les services d'entreposage de photos en ligne, les fournisseurs de comptes de courriel ou les sites de réseautage social, ainsi que les services aux

entreprises. Dans une infrastructure dans les nuages privée, l'infrastructure est destinée uniquement à une organisation. Elle peut être gérée par l'organisation elle-même ou un tiers et elle peut être située à l'interne ou à l'externe^{xliv}. Qu'il s'agisse d'une infrastructure dans les nuages publique ou privée, l'organisation qui prend des dispositions avec le fournisseur de services dans les nuages (et c'est également le cas de Louise quand elle vend des bijoux) doit protéger les renseignements personnels et veiller à ce que le fournisseur qui traite les renseignements personnels offre un degré de protection comparable, comme l'exige la LPRPDE.

Une distinction était également établie dans certaines observations écrites entre les services aux consommateurs et les services aux entreprises. Un répondant a mentionné que, dans les cas où le service dans les nuages est offert directement aux consommateurs, le fournisseur est le gestionnaire des données; cependant, dans les cas où les services sont offerts à des entreprises, le fournisseur est chargé du traitement des données. Dans le cas de Louise, quand elle utilise pour le plaisir un site de réseautage social ou un compte de courriel, le fournisseur du site ou du compte de courriel est le gestionnaire des données. Quand elle souhaite utiliser un service dans les nuages pour l'aider à traiter les données des clients de sa bijouterie, le fournisseur est chargé de traiter les données et Louise, de les contrôler. Cette distinction est importante, car cela signifie que Louise, quand elle contrôle les données, a certaines obligations envers ses clients en ce qui concerne la protection des renseignements personnels.

Avantages et risques

Certains répondants et participants ont mentionné les avantages que présente l'informatique dans les nuages. Voici quelques avantages pour les utilisateurs (entreprises, surtout petites et moyennes, gouvernements et personnes) : variabilité dimensionnelle (capacité illimitée de traitement et d'entreposage), fiabilité (c.-à-d. élimination du risque de perdre des données précieuses sur papier ou en raison de la perte d'ordinateurs portables ou de disques durs, capacité d'accéder à des applications et à des documents partout dans le monde par l'entremise d'Internet), économies, efficacité (c.-à-d. que cela libère des ressources pour se pencher sur l'innovation et la création de produits) et accès à de nouvelles technologies. Certains répondants et participants ont indiqué que puisque les utilisateurs de l'informatique dans les nuages n'ont pas à investir dans une infrastructure des technologies de l'information ni à acheter du matériel informatique ou des licences de logiciels, les avantages sont les suivants : coûts de départ minimes, rendement rapide des investissements, déploiement rapide, personnalisation, usage souple et solutions Internet qui peuvent utiliser de nouvelles innovations Web. D'autres ont mentionné les avantages potentiels pour la société, comme la fourniture plus efficace de soins de santé, la croissance économique et la création d'emplois.

Un avantage potentiel cité par un certain nombre de répondants et de participants est que la protection de la vie privée peut être améliorée. Plus précisément, l'informatique dans les nuages peut améliorer cet aspect grâce à des efforts déployés au cours de la conception et l'utilisation de meilleurs mécanismes de sécurité. On a affirmé que l'informatique dans les nuages facilitera l'acquisition de TI et les améliorations dans ce domaine, ce qui pourrait permettre le rajustement des procédures en fonction du caractère délicat des données. L'utilisation répandue de l'informatique dans les nuages pourrait également favoriser la mise en œuvre de normes transparentes dans ce domaine, ce qui permettra d'établir des fonctions de base communes en matière de sécurité des données dans différents services et chez différents fournisseurs. Les normes techniques pourraient être élaborées au fil du temps (certains ont indiqué qu'elles n'étaient pas bien établies à l'heure actuelle dans le domaine de l'informatique dans les nuages), et l'informatique dans les nuages pourrait donner lieu à des innovations et à une

certaine souplesse. Elle pourrait améliorer la vérification et la fiabilité des données, car les données ne sont plus aussi facilement perdues (en comparaison avec le monde réel).

La plupart des répondants et des participants ont convenu des risques pour la vie privée que posait l'informatique dans les nuages. Ces risques ont généralement trait aux principes figurant à l'annexe 1 de la LPRPDE et concernent les administrations et l'accessibilité des tiers, les mesures de sécurité, les limites de l'utilisation et de la conservation et l'accès et la correction. Une distinction entre les risques posés par le modèle des consommateurs et celui des entreprises, qui ont été abordés dans la section sur le consentement au suivi, au profilage et au ciblage en ligne, est que, souvent, le fournisseur offre au consommateur un accord, qu'il peut accepter ou refuser, tandis que les entreprises ont le loisir de négocier les conditions du service. Les entreprises ont ainsi la capacité d'intégrer certaines mesures de protection de la vie privée, mais les consommateurs sont souvent moins en mesure d'assurer leur propre protection.

III.II LPRPDE — Principes de la protection de la vie privée

Ce que nous avons entendu : LPRPDE — Cadre réglementaire

La plupart des participants reconnaissaient les problèmes posés par le modèle de l'informatique dans les nuages pour la protection de la vie privée et des données, mais ils n'étaient pas tous d'accord pour dire que la LPRPDE est un cadre réglementaire adéquat. La plupart étaient d'avis que la LPRPDE fournit un cadre réglementaire solide et souple par l'entremise duquel on peut aborder les problèmes liés à la protection des renseignements personnels découlant de l'informatique dans les nuages. Selon la plupart des répondants et participants, la force de la LPRPDE tient au fait qu'elle est neutre sur le plan technologique, le Commissariat ayant été en mesure de l'appliquer aux nouvelles technologies et pratiques opérationnelles. Cependant, certains participants ont formulé des suggestions précises en vue de renforcer la LPRPDE. On a également tenu des discussions générales dans le cadre des consultations afin de déterminer si un modèle axé sur les plaintes est adéquat pour protéger les consommateurs qui, pour la plupart, ne connaissent pas l'informatique dans les nuages. On a mentionné que les modifications législatives proposées afin de rendre obligatoire le signalement des atteintes permettront de rendre les pratiques liées à la protection de la vie privée plus transparentes pour les utilisateurs et les autorités chargées de la protection des données, ce qui pourrait favoriser la présentation de plaintes au Commissariat et, ultimement, l'amélioration des pratiques.

Bon nombre de répondants et de participants ont affirmé que l'informatique dans les nuages n'était qu'une forme d'impartition et que les problèmes qui en découlent sont les mêmes que ceux liés à l'impartition. Qui contrôle les données? Qui est responsable? Y a-t-il des mesures de protection adéquates mises en œuvre? Qui a accès aux données? À qui les communique-t-on? De quelle façon les utilise-t-on? Y a-t-il des territoires de compétence où les données ne doivent pas être transmises? Les préoccupations concernant l'acheminement transfrontière des données, sujet de discussion depuis une décennie dans le domaine du droit à la vie privée, sont exacerbées dans le contexte de l'informatique dans les nuages.

Administrations et accès des tiers

En grande partie, l'informatique dans les nuages fait fi des frontières^{xiv}, car les renseignements sont souvent entreposés dans différents territoires. Certains répondants et participants ont expliqué que, lorsqu'une entreprise utilise le modèle de l'informatique dans les nuages, elle ne

peut impartir la responsabilité de la protection des données, cela étant établi clairement dans la section sur la responsabilité de la LPRPDE^{xlvi}. Les lois canadiennes continueront de s'appliquer aux activités, ce qui sera également le cas des lois d'autres administrations.

Un certain nombre de répondants ont affirmé qu'il fallait plus de transparence au sujet de l'endroit où les données pourraient se retrouver pour être traitées. On a également suggéré que les personnes aient la possibilité de refuser certains types de traitement si elles ne voulaient pas que leurs données soient transmises à une certaine administration.

Certains ont indiqué qu'il faut élaborer une solution ici même au Canada. Les activités d'informatique dans les nuages menées uniquement au Canada pourraient atténuer certaines préoccupations soulevées par le fait que les données sont entreposées ou acheminées dans d'autres administrations.

Les questions liées à l'accès aux données par des gouvernements étrangers sont étroitement liées à celles concernant les territoires de compétence. Il y a eu des commentaires selon lesquels l'accès des gouvernements aux renseignements personnels peut être plus complexe dans le modèle de l'informatique dans les nuages que dans d'autres ententes d'impartition dans le domaine des TI.

On était préoccupé par les risques posés par le fait d'impartir le traitement de renseignements personnels dans des pays ayant des lois plus souples (que celles du Canada) en ce qui a trait à leur accès par les gouvernements. Certains considéraient que les risques liés à l'accessibilité ne sont pas plus importants à l'étranger qu'au pays. Les lois canadiennes accordent certains pouvoirs semblables à ceux confiés dans d'autres administrations. De plus, le Canada a conclu bon nombre d'ententes officielles et officieuses d'échange de renseignements avec d'autres administrations.

On a suggéré deux modifications qui pourraient être apportées à la LPRPDE afin de régler le problème de vulnérabilité posé par le fait que les renseignements personnels des Canadiens sont accessibles par des gouvernements étrangers : l'élaboration d'une loi de blocage et l'intégration d'une disposition proactive à la LPRPDE pour renforcer ses exigences en matière de communication. Une loi de blocage permet aux organisations nationales de ne pas respecter une loi étrangère donnée, et une disposition proactive limiterait le traitement des données à l'échelle internationale.

La question de la loi applicable peut être complexe pour certaines organisations. Une organisation a mentionné que les obligations juridiques peuvent parfois être en contradiction et que les restrictions géographiques imposées à l'acheminement des données peuvent complexifier la situation. Ces restrictions peuvent entraver l'expansion et les avantages de l'informatique dans les nuages et entraîner des coûts pour les utilisateurs et les fournisseurs de services. On a plutôt suggéré, avant d'imposer des restrictions à l'acheminement des données, de tout d'abord mener une évaluation au cas par cas des risques liés à la protection de la vie privée qui tient compte du volume de renseignements et de leur nature délicate, de l'utilisation escomptée et de la sécurité offerte par les mesures de protection technologiques, de la mesure dans laquelle il est probable qu'un gouvernement étranger demande l'accès aux renseignements, de la capacité de cibler les renseignements et de la probabilité que des torts soient causés si les renseignements sont divulgués et de la gravité de ces torts. On a suggéré que les gouvernements envisagent l'élaboration d'un cadre multilatéral sur les questions liées à l'acheminement transfrontalier des données sous la forme d'un traité ou d'un instrument international semblable. Une solution moins officielle a été proposée selon laquelle les pays

pourraient, de façon indépendante, mettre en œuvre des procédures pour régler les problèmes liés à l'accès aux données de façon à éviter les conflits de revendication de la compétence.

Observations du Commissariat

Dans le cadre d'enquêtes sur des plaintes antérieures, le Commissariat s'est penché sur des questions concernant d'autres pays et l'accessibilité aux données par des tiers. Par exemple, nous avons examiné le recours à des tiers pour le traitement des renseignements dans d'autres pays et les obligations de l'organisation ayant imparti les données, les tiers qui traitent les données et qui œuvrent dans de multiples nations, y compris le Canada, ainsi que les organisations du Canada qui font appel à eux pour mener divers processus opérationnels. Nous avons été en mesure d'appliquer la LPRPDE dans tous les cas.

À la suite de ces travaux et en réaction à certaines préoccupations à l'égard de la façon dont la LPRPDE s'applique à l'acheminement transfrontalier de données, le Commissariat a diffusé en 2009 un document intitulé [Lignes directrices sur le traitement transfrontalier des données personnelles](#), afin d'expliquer comment la LPRPDE s'applique aux transferts de renseignements personnels à des tierces parties, y compris à des tierces parties exerçant des activités à l'extérieur du Canada, aux fins de traitement. Les lignes directrices décrivent l'approche envisagée aux termes de la LPRPDE pour protéger les renseignements personnels impartis, indiquent les obligations des organisations et fournissent des conseils sur la façon dont les organisations peuvent atténuer les risques potentiels inhérents au traitement transfrontalier des données.

Nous sommes d'avis que les personnes ont des attentes envers les organisations, l'une d'entre elles étant que ces dernières fassent montre de transparence lorsqu'elles acheminent des renseignements personnels dans d'autres pays. Cependant, comme il est mentionné dans les lignes directrices, le Commissariat est conscient que l'univers électronique est complexe et qu'il s'avère parfois impossible pour une organisation de savoir précisément où se trouve l'information en cours de transit. Cela dit, la loi précise clairement où réside la responsabilité, et les organisations doivent, dans leur propre intérêt et dans celui de leur clientèle, faire tout en leur pouvoir pour protéger l'information. Nous sommes d'accord avec les nombreux participants qui ont affirmé qu'une organisation ne peut faire fi des lois d'une administration étrangère dans le cadre d'un marché.

Même si nous comprenons les préoccupations des gens qui proposent de modifier la LPRPDE pour prévenir l'acheminement de données vers certaines administrations, nous ne croyons pas que cela est la solution. Le Canada, qui est un pays membre de l'Organisation de coopération et de développement économiques (OCDE), est en accord avec les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, qui constituent le premier ensemble convenu à l'échelle internationale de principes de protection de la vie privée et qui visent à soutenir la protection de la vie privée des gens tout en éliminant tout obstacle inutile à l'acheminement libre des données imposé au nom de la protection de la vie privée. La LPRPDE est fondée en grande partie sur les principes décrits dans les lignes directrices de l'OCDE et elle vise à établir un équilibre entre le droit des personnes à la vie privée et le besoin des organisations de recueillir, d'utiliser ou de divulguer des renseignements à des fins appropriées. Nous affirmons depuis longtemps que la protection des renseignements personnels ne freine pas l'innovation ni le progrès économique. L'approche adaptée à chaque organisation qui sous-tend la LPRPDE appuie l'acheminement transfrontière et la protection des données en tenant les organisations pour responsables de leurs pratiques de protection des

renseignements personnels. Les autorités peuvent accéder aux renseignements, peu importe où elles se trouvent. Comme il est mentionné dans nos lignes directrices, nous continuons toutefois d'être d'avis qu'il faut mener une évaluation attentive des risques avant de prendre des dispositions visant l'impartition de données personnelles à d'autres organisations qui œuvrent à l'échelle mondiale, et que cette évaluation doit tenir compte des exigences juridiques de l'administration dans laquelle est établi le tiers qui traite les données ainsi que de certaines conditions politiques, économiques et sociales de cette administration et de tout autre facteur de risque qui y existe.

Divers traités et accords ont été conclus entre le Canada et d'autres gouvernements. En ce qui concerne les accords d'échange de renseignements conclus avec d'autres organisations, le Conseil du Trésor a récemment diffusé le [Document d'orientation pour aider à préparer des ententes d'échange de renseignements personnels](#)^{xlvii}. Le Commissariat a été consulté pour l'élaboration de ce document, et nous avons formulé des commentaires pour les domaines où, selon nous, il fallait aborder les préoccupations concernant la protection de la vie privée. Nous croyons que ce document améliorera la gouvernance des renseignements.

Quand une personne comme Louise utilise, par exemple, des applications ou des logiciels dans les nuages, il ne s'agit pas d'impartition; en effet, l'entreprise qui recueille des données auprès de personnes contrôle ces données. La LPRPDE a été appliquée à des entreprises œuvrant dans d'autres pays et entretenant un lien réel et considérable avec le Canada^{xlviii}. Ultimement, le Commissariat croit qu'une approche commune à la protection de la vie privée dans différentes administrations permettrait de garantir que des mesures de protection de la vie privée sont en place et que les entreprises ont un ensemble de règles communes à respecter. Pour ce faire, le Commissariat a travaillé fort avec ses homologues provinciaux et territoriaux pour fournir des approches uniformes à la protection des renseignements personnels pour les citoyens, les consommateurs et les entreprises. À l'échelle internationale, le Commissariat continue de collaborer avec d'autres autorités responsables de la protection des données afin d'en venir à une compréhension mutuelle et à l'élaboration d'approches communes, car nous croyons que les entreprises doivent être uniformes et que les citoyens s'y attendent. Nous avons pris part à l'élaboration de la Résolution de Madrid, et l'avons soutenue, et nous avons participé au Projet responsabilité, dans le cadre duquel s'est réuni un groupe de représentants de gouvernements, d'entreprises et d'universités pour élaborer le concept de responsabilité. Nous participons aux efforts déployés par l'Organisation internationale de normalisation (ISO) en vue d'élaborer et de mettre à jour des normes et des lignes directrices abordant les questions que sont la gestion de l'identité, la biométrie et la protection des renseignements personnels. Parmi les projets clés de l'Organisation internationale de normalisation, on compte l'élaboration de normes-cadres en vue de la gestion de l'identité et de la protection des renseignements personnels et la détermination du besoin d'élaborer à l'avenir des normes et des lignes directrices supplémentaires liées aux technologies qui améliorent précisément la protection de la vie privée.

En ce qui concerne l'application de la loi, nous avons récemment été acceptés à titre de participant à l'initiative de la Coopération économique Asie-Pacifique (APEC) visant l'application transfrontière des lois sur la protection des renseignements personnels. L'entente établit un processus dans le cadre duquel les autorités participantes peuvent demander de l'aide pour la collecte d'éléments de preuve, l'échange de renseignements sur une organisation ou une question faisant l'objet d'une enquête, la prise de mesures et le transfert de plaintes à une autre administration. Le Commissariat est également membre du Global Privacy Enforcement Network (GPEN), qui a été mis sur pied en 2010 pour échanger des renseignements sur les questions, les tendances et les expériences liées à l'application de la loi sur la protection des renseignements personnels. Il participe également à des séances de formation pertinentes,

collabore à des activités de sensibilisation, tient des dialogues avec les organisations pertinentes du secteur privé sur l'application de la loi et les questions liées à la sensibilisation et favorise l'application transfrontière efficace des lois sur la protection des renseignements personnels dans des cas précis en créant une liste de personnes-ressources d'autorités en la matière intéressées par la coopération bilatérale dans les enquêtes transfrontières et les affaires liées à l'application de la loi. Le GPEN a été mis sur pied en réaction à une recommandation formulée par l'OCDE en 2007 selon laquelle les pays membres devaient établir un réseau informel d'autorités chargées de l'application de la loi sur la protection des renseignements personnels.

Dans le projet de loi C-28, la *Loi visant l'élimination des pourriels sur les réseaux Internet et sans fil* proposée aurait pour effet de modifier la LPRPDE pour permettre au Commissariat d'échanger des renseignements avec ses homologues provinciaux et internationaux concernant les pratiques d'organisations en matière de renseignements personnels. Nous croyons qu'il s'agit d'un changement clé de la protection de la vie privée qui découle de la mondialisation des renseignements personnels.

Mesures proposées

- **Le Commissariat encourage les organisations à indiquer clairement aux personnes que leurs renseignements personnels peuvent être traités dans des administrations étrangères et accessibles à des autorités d'application de la loi et de sécurité nationale dans ces administrations. Cela doit être énoncé de façon claire et compréhensible, idéalement au moment où les renseignements sont recueillis.**
- **Le Commissariat continuera d'offrir de l'orientation aux organisations au sujet de l'acheminement transfrontière des données.**
- **Le Commissariat continuera de fournir au Parlement des conseils sur les ententes intergouvernementales visant l'échange de renseignements personnels.**
- **Le Commissariat encourage le Secrétariat du Conseil du Trésor à sensibiliser continuellement les ministères qui accèdent à des données sur les services commerciaux à leurs obligations relatives à la protection de la vie privée à l'appui de ses pratiques exemplaires concernant les ententes d'échange de renseignements.**
- **Le Commissariat presse respectueusement le ministère de la Justice du Canada d'acheminer son document d'orientation sur l'acheminement transfrontière des données et l'accès aux renseignements par des tiers aux conseillers juridiques du gouvernement.**
- **Le Commissariat continuera à travailler à l'élaboration d'approches harmonisées à l'égard de la protection des données et de l'application de la loi.**

Mesures de sécurité

Tous les répondants et les participants ont affirmé que la sécurité des données était l'une des questions les plus importantes relativement à l'informatique dans les nuages. Même si certains étaient d'avis que l'informatique dans les nuages pose certains risques pour la sécurité, d'autres considéraient qu'elle peut renforcer la sécurité si les fournisseurs sont en mesure d'utiliser des technologies et des méthodes de protection qui ne seraient pas habituellement utilisées par des entreprises dans leurs propres centres de données. On a mentionné que la plupart des fournisseurs de ce domaine affectent un volume important de ressources à la protection des renseignements et à l'authentification des utilisateurs et, de façon générale, à la sécurité des données, et une organisation a indiqué que les investissements faits par les fournisseurs de services dans les nuages relativement au personnel et aux pratiques de sécurité bénéficient à tous les utilisateurs de ces services. Elle a expliqué que la technologie s'est répandue plus rapidement qu'il est possible de former des gens pour bien la gérer. Selon un commentaire que nous avons reçu, l'environnement de l'informatique dans les nuages est susceptible d'être plus sécurisé que la plupart des environnements de TI du secteur privé.

Une organisation a affirmé que l'informatique dans les nuages n'accroît pas le risque d'exposition et d'utilisation inadéquate des renseignements (c'est le cas également avec tout fournisseur de services tiers); elle augmente plutôt l'ampleur de l'exposition. Comme il a été mentionné, le regroupement des données peut faire en sorte que les criminels soient intéressés à s'en prendre aux centres de données dans les nuages.

Une autre organisation a expliqué que la sécurité est fonction des contrôles de sécurité du fournisseur de services dans les nuages et de l'utilisation du service dans les nuages par le consommateur. La séparation des données et l'accès limité aux données étaient considérés comme des outils importants. On a discuté de l'encodage, mais un participant a insisté sur le fait qu'il ne s'agit que d'un seul outil d'une stratégie de sécurité. Une organisation soutient les efforts déployés en vue d'élaborer des pratiques de base de protection de la vie privée dans l'industrie de l'informatique dans les nuages qui sont généralement fondées sur les pratiques équitables en matière de renseignements établies dans la LPRPDE. Elle incitait le Commissariat à tenir compte des travaux dans d'autres administrations et des initiatives de l'industrie dans le cadre des directives qu'elle élabore pour assurer une uniformité avec les approches mises en place ailleurs.

L'élaboration de normes très élevées de sécurité des données recevait un soutien général; un groupe de défense des intérêts était d'avis qu'un organe indépendant ou gouvernemental devrait être affecté à la création et à l'application de normes. Cependant, d'autres affirmaient que la culture de l'innovation technologique ne se prête pas bien à la réglementation, ce qui fait que la réglementation accuse du retard sur les progrès technologiques.

Bon nombre de participants ont indiqué que le fait de rendre obligatoire le signalement des atteintes était un moyen utile d'éclairer certaines pratiques afin d'améliorer la protection de la vie privée et la sécurité. Il a été mentionné que les personnes ont de la difficulté à se plaindre de pratiques qu'elles ne connaissent pas du tout. Bon nombre de personnes ne savent même pas que leurs renseignements personnels se trouvent dans une infrastructure dans les nuages, et les atteintes ont souvent pour effet de le leur faire savoir. Un résultat très positif du signalement obligatoire des atteintes est probablement la transparence. Les participants ont laissé entendre que, si cela était rendu obligatoire, les organes de réglementation seraient davantage au courant de la situation et pourraient offrir une orientation afin d'améliorer les pratiques. Un participant a indiqué qu'on pourrait probablement établir une base de données des atteintes pour permettre

aux personnes concernées de découvrir si la sécurité de leurs renseignements personnels a été compromise. On a également mentionné que, pour influencer davantage sur les pratiques, la commissaire devrait avoir le pouvoir de rendre des ordonnances.

Nous avons entendu parler de différents problèmes en matière de sécurité entre les infrastructures dans les nuages publique et privée. Les deux présentent des problèmes qui leur sont propres. Dans l'infrastructure dans les nuages publique, les clients ont probablement moins de contrôle sur la sécurité. On a toutefois mentionné que l'infrastructure dans les nuages privée entraîne également des problèmes malgré le « mur » qui sépare les données et les autres parties d'Internet. Il se peut que des gens ne veuillent pas qu'on accède à certaines données, même à l'intérieur du mur, et l'accès devra être limité à différentes personnes.

On a décrit les différents risques pour la sécurité des modèles des consommateurs et des entreprises. On a indiqué qu'il serait possible d'en faire plus en ce qui a trait à l'entreposage et à l'acheminement des données dans le contexte des services offerts aux consommateurs et souligné que la sécurité fait souvent place à la convivialité et à la facilité d'utilisation. Par contre, dans le modèle des services offerts aux entreprises, la sécurité est un argument de vente, car les attentes des clients sont élevées à cet égard. Les fournisseurs de services dans les nuages aux entreprises le savent et en font une priorité.

Comme il a été expliqué de façon détaillée dans la discussion sur les territoires de compétence et l'accessibilité, les organisations qui font appel à un fournisseur de services dans les nuages sont responsables des données et doivent préciser certaines exigences, y compris en ce qui a trait à l'emplacement des données, à la capacité des fournisseurs de faire de la sous-traitance, à l'accès limité aux données et aux vérifications. Un participant a mentionné que les entreprises peuvent négocier des ententes avec des fournisseurs de services dans les nuages tandis que, bien souvent, les consommateurs se voient offrir un accord qu'ils peuvent accepter ou refuser. Comme un répondant l'a souligné, si les consommateurs étaient aussi conscients des risques à la sécurité que les entreprises le sont, les fournisseurs de services dans les nuages destinés aux consommateurs seraient encouragés à renforcer la sécurité. Cependant, le répondant a expliqué que les consommateurs n'ont pas le luxe de se sensibiliser eux-mêmes, affirmant qu'il pourrait être nécessaire de mettre en œuvre des mesures de protection techniques dans le marché des services dans les nuages offerts aux consommateurs. Certains ont mentionné que, dans l'espace des consommateurs, les services dans les nuages existent depuis un certain temps, et les fournisseurs de services y appliquent un cadre de protection de la vie privée.

Une organisation a reconnu que les fournisseurs de services dans les nuages ont des approches différentes en matière de sécurité, et ces différences découlent de divers facteurs, comme les modèles d'affaires et de revenu, et le fait que les clients sont des consommateurs, des entreprises ou des gouvernements. Elle était d'avis qu'il n'est pas problématique d'avoir différentes approches à la sécurité, mais que le problème tient plutôt au fait que les distinctions entre les pratiques de sécurité des fournisseurs sont presque invisibles.

On a mentionné dans le cadre des discussions tenues pendant les consultations que les consommateurs doivent avoir accès à davantage de renseignements de meilleure qualité sur les problèmes inhérents à l'informatique dans les nuages afin d'être en mesure de bien choisir leur fournisseur de services, et les organisations doivent obtenir de l'orientation sur les exigences qu'elles peuvent imposer au fournisseur et les attentes qu'elles devraient avoir. Pour les très petites entreprises, comme la bijouterie de Louise, les participants ont formulé différents conseils. Le représentant d'une société a discuté de la façon dont la prise de décisions automatisée pourrait être utile pour les petits entrepreneurs comme Louise. D'autres ont

suggéré qu'elle fasse des recherches, non pas sur la technologie, mais plutôt sur ce que des entreprises semblables ont utilisé, les avantages et les risques en découlant et la façon d'atténuer ces risques. Elle devrait demander de l'aide à des amis à qui elle fait confiance. On a suggéré que le Commissariat fournisse des renseignements aux petites et moyennes entreprises sur les questions à examiner quand elles font affaire avec un fournisseur de services dans les nuages.

Observations du Commissariat

Le Commissariat est d'accord pour dire que la sécurité des données personnelles dans une infrastructure dans les nuages est essentielle. De quelle façon Louise peut-elle s'assurer que, quand elle utilise les services dans les nuages pour des motifs personnels, ses renseignements personnels sont protégés? Quand Louise fait appel à un fournisseur de services dans les nuages pour l'aider à gérer son entreprise, quelle est la meilleure façon pour elle de trouver des renseignements pour l'aider à prendre la bonne décision? Peut-elle être plus exigeante? De quelle façon peut-elle savoir quoi chercher ou demander? Après tout, aux termes de la LPRPDE, Louise est obligée de veiller à ce que les renseignements personnels de ses clients soient protégés.

Comme il a été mentionné dans la section sur le suivi, le profilage et le ciblage en ligne, il est essentiel de protéger d'emblée la vie privée, que ce soit dans le cadre des processus technologiques ou opérationnels. Il a été souligné dans les observations écrites et dans le cadre des discussions tenues pendant les consultations que l'informatique dans les nuages peut améliorer la protection de la vie privée et la sécurité, ce qui est encourageant. Nous sommes d'accord avec les commentaires que nous avons entendus sur la nécessité d'élaborer des normes pour l'industrie et encourageons fortement les travaux dans ce domaine. La modification proposée de la LPRPDE qui rendrait obligatoire le signalement des atteintes indique l'importance de la sécurité des renseignements personnels et devrait aider les organisations qui utilisent la technologie et celles qui la créent à mieux intégrer la sécurité à la technologie. Dans le cadre de la discussion, on a mentionné que, une fois que le Commissariat a examiné la façon dont l'atteinte est survenue^{xlix}, nous examinons les normes de l'industrie pour décider s'il aurait été possible d'en faire plus, autre raison importante pour que de telles normes soient élaborées.

En plus de la nécessité d'élaborer des normes, nous sommes d'accord avec les nombreux répondants et participants qui sont d'avis que les utilisateurs et les petites et moyennes entreprises doivent avoir accès à davantage de renseignements. Nous sommes d'accord avec le point de vue selon lequel les consommateurs doivent recevoir une orientation sur les problèmes inhérents à l'informatique dans les nuages et les organisations ont besoin de directives sur ce qu'elles doivent faire dans ce domaine.

Il est également important de fournir une orientation aux nouveaux fournisseurs de services qui tirent profit de l'évolution rapide des produits rendue possible grâce à l'informatique dans les nuages. De plus en plus de concepteurs d'applications, de regroupeurs de données et de fournisseurs de services traitent des renseignements personnels qui sont fournis directement par des consommateurs ou transmis par l'entremise de plateformes hôtes. Certains de ces nouveaux intervenants peuvent ne pas avoir l'expérience et la motivation nécessaires pour protéger adéquatement les renseignements personnels.

Nous avons pris note du commentaire concernant les pouvoirs de la commissaire. Nous sommes à examiner nos propres structure et fonction à titre d'autorité chargée de la protection

des données. À cette fin, nous avons commandé une étude pour examiner le contexte économique, juridique et politique global dans le cadre duquel la LPRPDE a été promulguée pour le comparer à l'environnement actuel. Une partie de cette étude consiste en une comparaison de notre modèle par rapport à celui de provinces et de pays choisis.

Questions à commenter – Mesures de sécurité

- **Nous avons été témoins de discussions sur la nécessité d'élaborer des normes, et nous pressons les organisations d'élaborer des normes de sécurité des renseignements personnels solides. Nous aimerions recevoir d'autres commentaires sur les travaux effectués dans ce domaine au Canada et des suggestions sur les prochaines étapes. Le Commissariat est ouvert aux commentaires de l'industrie à ce sujet.**
- **On a suggéré que le gouvernement élabore de telles normes. Nous aimerions recevoir d'autres commentaires sur cette suggestion.**
- **Nous avons entendu parler des problèmes de sécurité dans les modèles de l'informatique dans les nuages publique et privée, mais pas dans le modèle hybride. Nous aimerions recevoir davantage de commentaires sur les problèmes de sécurité qui pourraient découler du modèle hybride.**

Mesures proposées

- **Le Commissariat travaillera avec Industrie Canada pour déterminer la meilleure façon d'intégrer aux pratiques du secteur privé l'utilisation des EFVP et les principes de protection de la vie privée à l'étape de la conception des produits.**
- **Le Commissariat encourage la GRC à mener des activités de sensibilisation coordonnées auprès du secteur privé au sujet de la sécurité des données et à déterminer des mesures contre le vol d'identité à l'intention des consommateurs.**
- **Le Commissariat incite les organisations à élaborer des normes qui fournissent des mesures de protection de la sécurité solides. Le Commissariat continuera de faire le suivi des travaux effectués par l'Organisation internationale de normalisation sur les normes de l'informatique dans les nuages et d'y contribuer.**
- **Le Commissariat examinera davantage la gestion des renseignements personnels par les concepteurs.**
- **Le Commissariat travaillera à l'élaboration de documents d'orientation pour les organisations sur les questions liées à la protection de la vie privée dans l'informatique dans les nuages.**
- **Le Commissariat travaillera également à l'élaboration d'initiatives de sensibilisation destinées aux personnes qui utilisent les services dans les nuages.**

Nouvelles utilisations et conservation

Nous avons été témoins de discussions sur le détournement d'usage. Compte tenu du potentiel de tirer profit du volume imposant de données qu'ils détiennent, certains fournisseurs de services dans les nuages pourraient être tentés d'utiliser ces renseignements à d'autres fins. La publicité comportementale, qui a également fait l'objet de discussions dans le cadre des consultations, est un exemple de la façon dont les renseignements pourraient être utilisés à d'autres fins; cela toucherait les consommateurs comme Louise qui interagissent directement avec les services dans les nuages offerts aux consommateurs. On a également discuté de l'utilisation des renseignements des clients de Louise. On a mentionné les données transactionnelles (les données créées pour décrire une transaction) ou les flux de données et la façon dont ils pourraient être utilisés. Un participant a indiqué qu'il était nécessaire de compter sur un meilleur nettoyage des bases de données. Comme il est peu dispendieux de conserver des données, les organisations ne sont pas enclines à s'en débarrasser, mais plutôt encouragées à les utiliser à d'autres fins. Dans le modèle des entreprises, l'organisation qui conclut un marché (p. ex. Louise, à titre d'entrepreneure) peut imposer des restrictions et veiller à ce que, avant que les données soient utilisées de nouvelles façons, le consentement soit obtenu. Voici deux suggestions formulées pour régler ce problème : les organisations pourraient intégrer à leurs systèmes des restrictions sur les types d'utilisation des données recueillies et elles pourraient uniquement recueillir des données qui sont absolument nécessaires à la fourniture des services. Par ailleurs, l'établissement de calendriers de conservation des données sera utile pour améliorer le nettoyage des bases de données.

Observations du Commissariat

Le Commissariat partage les préoccupations exprimées par bon nombre de participants sur la façon dont les données peuvent être utilisées. La LPRPDE indique clairement que les utilisateurs doivent consentir aux nouvelles fins de la collecte, de l'utilisation ou de la communication de renseignements, et que la collecte de renseignements personnels doit être limitée à ce qui est nécessaire. Aux termes de la LPRPDE, les données ne peuvent être conservées indéfiniment. Compte tenu du modèle de responsabilité décrit dans la *Loi*, les organisations qui passent un marché avec un fournisseur de services dans les nuages ont la capacité d'imposer certaines restrictions et de mener des vérifications. Les préoccupations les plus importantes semblent viser le modèle des consommateurs, dans lequel les personnes ont probablement moins de contrôle et où la transparence et le consentement pourraient être à risque. Cela peut également être problématique pour les très petites entreprises qui peuvent ne pas avoir la capacité d'exercer la diligence raisonnable nécessaire avant de conclure un marché avec un fournisseur de services dans les nuages. Nos demandes de commentaires supplémentaires et nos mesures proposées figurent dans les sections antérieures du présent rapport.

Accès à ses renseignements personnels

Dans les observations écrites et pendant les consultations, on avait tendance à indiquer que la façon dont les personnes peuvent accéder à leurs renseignements personnels est liée à la propriété et à la portabilité. En effet, il s'agit d'une question sur laquelle doit se pencher Louise, car elle est obligée de fournir à ses clients un accès à leurs renseignements personnels et la possibilité de les corriger. Qui est le propriétaire des renseignements? Peuvent-ils être déplacés? Certains se demandaient ce qu'il adviendrait de ses renseignements si, par exemple, Louise souhaitait mettre fin au marché conclu avec le fournisseur de données. Peut-elle les

reprendre et s'assurer qu'ils ne seront pas utilisés à l'avenir? De quelle façon peut-elle les reprendre dans un format utile? On a indiqué que la suppression des données ou le fait de les redonner en format utile n'étaient pas garantis. Un répondant, mentionnant que bon nombre de fournisseurs de services dans les nuages ne permettent pas aux utilisateurs de récupérer ou de retirer facilement leurs renseignements quand ils décident de changer de fournisseur ou d'annuler les services, était d'avis que cela entravait davantage les utilisateurs qui souhaitaient partir et laissait place à des abus potentiels du pouvoir sur le marché et à l'utilisation abusive des renseignements des utilisateurs. Il a suggéré que l'élimination des obstacles pourrait atténuer bon nombre de problèmes potentiels liés à la protection de la vie privée.

Observations du Commissariat

Le consentement et la capacité d'accéder à ses renseignements personnels et de les corriger sont des pratiques équitables en matière de renseignements figurant dans la LPRPDE qui permettent aux personnes de contrôler leurs renseignements personnels. Les autres pratiques protègent essentiellement ces renseignements et soutiennent la capacité de la personne de les contrôler. Une préoccupation du Commissariat est que l'accès aux données et leur correction ne sont pas facilités dans Internet, mais nous reconnaissons que cela peut être complexe. Les technologies, les modèles opérationnels et le nombre important d'intervenants font qu'il est très difficile pour les personnes de découvrir les renseignements que les organisations détiennent sur elles et de corriger les erreurs factuelles. Cela est une préoccupation pour nous et a trait à la gestion de son identité et de sa réputation en ligne ainsi qu'à la sécurité des renseignements personnels. En ayant accès à davantage de renseignements, les utilisateurs sont susceptibles de soulever plus de préoccupations, mais le Commissariat est d'avis que l'industrie doit en faire plus pour aborder les problèmes liés à l'accès et à la correction en ligne.

Mesure proposée

- **Le Commissariat encourage l'industrie à trouver des façons novatrices de respecter les dispositions concernant l'accès et la correction de la LPRPDE et souhaite que davantage de discussions soient tenues sur cette question.**

Sommaire des questions à commenter

Suivi, profilage et ciblage en ligne

Distinctions entre les domaines public et privé, et réputation

- Le Commissariat aimerait tenir d'autres discussions avec les intervenants sur la gestion de l'identité en ligne.
- Le Commissariat met l'industrie au défi de trouver des façons et des moyens de favoriser l'expiration des données et souhaite tenir d'autres discussions à cet égard. La LPRPDE indique clairement que les renseignements personnels ne doivent pas être conservés pour toujours.

Il faut prêter une attention particulière aux enfants

- Le Commissariat aimerait recevoir des commentaires sur ce que pourraient être les normes de base concernant la protection des renseignements personnels des enfants et la façon dont ces normes pourraient être élaborées. Le Commissariat aimerait également obtenir des points de vue sur le type de cadre qu'il faudrait mettre en œuvre.

Consentement, consentement valable et transparence

- Le Commissariat continuera de collaborer avec l'industrie pour élaborer la meilleure approche possible pour veiller à ce que les personnes fournissent un consentement valable à des pratiques opérationnelles légitimes. Il s'agit d'un domaine dans lequel la technologie peut être utile pour régler ce problème. Par conséquent, nous aimerions recevoir des commentaires sur la meilleure façon de réaliser cet objectif.
- Le Commissariat continuera d'axer ses activités de sensibilisation sur les personnes afin de les aider à mieux se protéger en ligne. Pour ce faire, on examinera la meilleure façon d'aider les personnes à prêter attention aux explications sur la protection de la vie privée qui leur sont fournies. Le Commissariat aimerait recevoir des commentaires sur la meilleure façon de réaliser cet objectif.

Autres utilisations et modes de communication

- Le Commissariat aimerait obtenir des points de vue et des commentaires supplémentaires sur les pratiques actuelles et futures de suivi et de profilage en ligne (à l'exception de la publicité comportementale) au Canada.

Informatique dans les nuages

Mesures de sécurité

- Nous avons été témoins de discussions sur la nécessité d'élaborer des normes, et nous pressons les organisations d'élaborer des normes de sécurité des renseignements personnels solides. Nous aimerions recevoir d'autres commentaires sur les travaux effectués dans ce domaine au Canada et des suggestions sur les prochaines étapes. Le Commissariat est ouvert aux commentaires de l'industrie à ce sujet.
- On a suggéré que le gouvernement élabore de telles normes. Nous aimerions recevoir d'autres commentaires sur cette suggestion.
- Nous avons entendu parler des problèmes de sécurité dans les modèles de l'informatique dans les nuages publique et privée, mais pas dans le modèle hybride. Nous aimerions recevoir davantage de commentaires sur les problèmes de sécurité qui pourraient découler du modèle hybride.

Le Commissariat aimerait recevoir des commentaires au plus tard le **10 décembre 2010**. Nous espérons diffuser le rapport final sur les consultations au début de 2011.

Conclusion

(À élaborer après la période de commentaires
sur le rapport de consultation)

Notes en fin de texte

- i Aux termes de l'alinéa 26(2)b) de la LPRPDE, le gouverneur en conseil peut exclure l'organisation, l'activité ou la catégorie de l'application de la LPRPDE à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels qui s'effectue à l'intérieur d'une province qui a promulgué une loi semblable à la LPRPDE. L'Alberta, la Colombie-Britannique et le Québec ont des lois sur la protection des renseignements personnels dans le secteur privé qui sont considérées comme semblables à la LPRPDE. La *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario vise les dépositaires de renseignements sur la santé.
- ii Voir le document intitulé *Tracer le chemin : principaux développements au cours des sept premières années d'application de la Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) (Commissariat, 2008)
http://www.priv.gc.ca/information/pub/lbe_080523_f.cfm
- iii Voir le document intitulé *Tracer le chemin : principaux développements au cours des sept premières années d'application de la Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) (Commissariat, 2008)
http://www.priv.gc.ca/information/pub/lbe_080523_f.cfm
- iv Nous examinons également la protection des renseignements génétiques. La technologie intelligente est un autre domaine d'intérêt pour nous.
- v La surveillance des données est définie comme l'utilisation systématique de systèmes de données personnelles pour faire enquête ou surveiller les gestes ou les communications de personnes; Roger Clarke, *IT and Dataveillance*, novembre 1987
- vi <http://www.kidscreen.com/articles/news/20100616/ipsos.html> L'étude semble laisser entendre que de très jeunes enfants vont en ligne et interagissent avec des sites Web et d'autres diffuseurs de médias. <http://www.nngroup.com/reports/kids/>. Cette étude laisse entendre que les enfants ont une grande expérience de l'utilisation des ordinateurs et d'Internet et qu'ils sont exposés à la technologie à un âge relativement jeune.
- vii En date du 31 août 2010, la webémission sur l'événement de Toronto a été regardée 969 fois. Au cours de la journée de l'événement, le nombre total de microbillets portant le nom #priv2010 était de 231 et le nombre total de pages affichées au sujet des consultations sur le site Web du Commissariat était de 639. Pour l'événement de Montréal, en date du 31 août 2010, la webémission a été regardée 493 fois. Au cours de la journée de l'événement, le nombre total de microbillets portant le nom #priv2010 était de 193, et le nombre de pages affichées au sujet des consultations sur le site Web du Commissariat était de 256. Pour l'événement de Calgary, la webémission a été regardée 482 fois en date du 31 août 2010. La journée de l'événement, on a compté 161 microbillets et 212 pages consultées.
- viii Concept de vente au détail inspiré d'un récit paru en mars 2010 dans RFID Journal : <http://www.rfidjournal.com/article/print/7333>
- ix *Ibid.*
- x Tiré de http://www.networkadvertising.org/networks/Web_Beacons_rev_11-1-04.pdf
- xi *Ibid.*
- xii Voir la p. iii à l'adresse suivante : <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>
- xiii http://www.piac.ca/privacy/piac_comments_to_privacy_commissioner_of_canada_on_behavioural_targeting
- xiv http://www.priv.gc.ca/parl/2009/parl_bg_20091208_f.cfm

-
- xv http://www.piac.ca/privacy/tracking_consumers_online_behavioural_targeted_advertising_and_a_do_not_track_list_in_canada/
- xvi <http://www.the-cma.org/downloads/regulatory/SubmissionAdvertisingMar10.pdf> and http://www.the-cma.org/PublicUploads/224933BehaviouralAdvertising_09.pdf
- xvii *Recherche sur la confidentialité et l'utilisation des données géospatiales*, sommaire, novembre 2009, préparée pour Ressources naturelles Canada; http://epe.lac-bac.gc.ca/100/200/301/pwgsc-tpsgc/por-ef/natural_resources/2009/091-08-f/sommaire.pdf; le rapport figure à l'adresse suivante : http://epe.lac-bac.gc.ca/100/200/301/pwgsc-tpsgc/por-ef/natural_resources/2009/091-08-f/rapport.pdf
- xviii Tiré du mot d'ouverture de J. Stoddart à Montréal, 19 mai 2010
- xix Discussion dans le cadre des consultations tenues à Toronto sur le suivi géodépendant, 29 avril 2010
- xx Consultations sur la publicité tenues à Toronto, 29 avril 2010
- xxi Voir, <http://www.danah.org/papers/WhyYouthHeart.pdf>
- xxii Voir, <http://pewinternet.org/Reports/2010/Reputation-Management/Summary-of-Findings.aspx?r=1>
- xxiii Voir, <http://www.danah.org/papers/talks/2009/SupernovaLeWeb.html>
- xxiv Voici les priorités stratégiques du Commissariat : technologies de l'information, gestion de l'identité, sécurité nationale et protection des renseignements génétiques.
- xxv Voir le blogue Web sur l'identité de Kim Cameron à l'adresse suivante : <http://www.identityblog.com>
- xxvi Le Commissariat finance un ensemble de groupes de discussion avec des parents, des enseignants, des enfants et des jeunes dans quatre régions du Canada dans le cadre de la troisième phase du projet Les jeunes Canadiens dans un monde branché, vaste étude complète menée par MNet sur l'utilisation d'Internet par les enfants au Canada.
- xxvii Voir le Résumé de conclusions d'enquête en vertu de la LPRPDE n° 2003 – 162 à l'adresse suivante : http://www.priv.gc.ca/cf-dc/2003/cf-dc_030416_7_f.cfm
- xxviii http://www.priv.gc.ca/cf-dc/2005/319_20051103_f.cfm et http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_f.cfm
- xxix http://www.priv.gc.ca/cf-dc/2006/351_20061109_f.cfm
- xxx http://www.priv.gc.ca/information/pub/rfid_f.pdf
- xxxi Voir les pages 20 à 25 du document intitulé *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, février 2009. <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>
- xxxii Voir : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf
- xxxiii Voir : <http://www.futureofprivacy.org/2010/01/>
- xxxiv À l'article 7 de la LPRPDE, on énumère les situations dans lesquelles on peut recueillir, utiliser ou communiquer des renseignements à l'insu de l'utilisateur ou sans son consentement. Voir : <http://laws-lois.justice.gc.ca/fra/P-8.6/index.html>.
- xxxv Pour obtenir de plus amples renseignements, voir : http://www.priv.gc.ca/fs-fi/02_05_d_24_f.cfm.
- xxxvi Voir : http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_f.cfm. Il importe de mentionner que les fonctions de publicité sociale ont changé sur le site depuis.

- xxxvii Paragraphe 5(3)
- xxxviii *How Companies are using your Social Media Data*, Mashable, 2 mars 2010
<http://mashable.com/2010/03/02/data-mining-social-media/>
- xxxix <http://www.fastcompany.com/blog/lucas-conley/advertising-branding-and-marketing/company-we-keep>
- xl Pour obtenir des renseignements sur les nombreux intervenants dans l'environnement de la publicité en ligne, voir l'adresse suivante : <http://news.ghostery.com/post/948639073/the-many-data-hats-a-company-can-wear>
- xli Définition de l'informatique dans les nuages du NIST, version 15
<http://csrc.nist.gov/groups/SNS/cloud-computing/>
- xliv <http://csrc.nist.gov/groups/SNS/cloud-computing/>
- xlvi *Ibid.*
- xlvi *Ibid.*
- xlvi Certains fournisseurs de services dans les nuages œuvrent uniquement au Canada.
- xlvi Le principe 4.1.3 indique ce qui suit : « Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie. » Voir : <http://laws-lois.justice.gc.ca/fra/P-8.6/index.html>
- xlvi Voir : <http://www.tbs-sct.gc.ca/atip-aiprp/isa-eer/isa-eer01-fra.asp>
- xlvi Voir : http://www.priv.gc.ca/cf-dc/2009/2009_009_rep_0731_f.cfm et http://www.priv.gc.ca/cf-dc/2008/389_rep_080529_f.cfm pour consulter deux exemples récents.
- xlvi Pour de plus amples renseignements sur la façon dont le Commissariat réagit en cas d'atteintes à la vie privée, veuillez consulter l'adresse suivante : http://www.priv.gc.ca/resource/pb-avp/pb-avp_intro_f.cfm.