

**LA PROTECTION INTÉGRÉE DES
RENSEIGNEMENTS –
PERMETTRE AU CONSOMMATEUR DE FAIRE DES
CHOIX ET DE DONNER UN CONSENTEMENT
SIGNIFICATIFS EN MATIÈRE DE
CONFIDENTIALITÉ**



Rédigé par :

Alysia Lau
Le Centre pour la défense de l'intérêt public
1 rue Nicholas, bureau 1204
Ottawa, Ontario K1N 7B7
Canada

Juin 2017

CDIP © Tous droits réservés 2017

Il est interdit de reproduire ce document à des fins commerciales,
mais sa reproduction à d'autres fins est encouragée, à condition que la source soit citée.

Le Centre pour la défense de l'intérêt public
(CDIP)

Bureau 1204

1, rue Nicholas

Ottawa (Ontario)

K1N 7B7

Tél. : (613) 562-4002 Télécopieur : (613) 562-0007

Courriel : piac@piac.ca Site Web : www.piac.ca

Données de catalogage avant publication (Canada)

La protection intégrée des renseignements –
Permettre au consommateur de faire des choix et de donner un consentement significatifs
en matière de confidentialité

Remerciements

Le Centre pour la défense de l'intérêt public a reçu du financement en vertu du Programme de contributions pour les organisations sans but lucratif de consommateurs et de bénévoles d'Innovation, Sciences et Développement économique Canada.

Les opinions exprimées dans ce rapport ne sont pas nécessairement celles d'Innovation, Sciences et Développement économique Canada ou du gouvernement du Canada.

L'auteur tient à remercier Philippa Lawson pour ses conseils et sa rétroaction spécialisés dans le cadre de ce rapport. Merci à tous les intervenants et participants qui ont participé à l'élaboration d'un rapport sur des enjeux d'actualités importants durant une période d'innovation bourgeonnante et d'expansion des réseaux à large bande.

Résumé

Le présent rapport examine l'élaboration notionnelle d'une protection universelle intégrée de la sécurité des paramètres de protection de la vie privée et des renseignements des utilisateurs de services et d'applications en ligne. L'objectif principal du rapport consiste à contribuer au débat sur la conception de la protection de la vie privée et à l'examiner du point de vue du consommateur. Les recherches se sont penchées sur l'intérêt du consommateur relativement à un ensemble normalisé de paramètres de sécurité ou de renseignements applicable à différentes plateformes, y compris les navigateurs internet, les tablettes et les téléphones intelligents. Ce rapport propose également les commentaires du consommateur sur les fonctionnalités de la case relative à la protection des renseignements personnels, notamment son aspect et son caractère obligatoire éventuel dans le cas de tous les utilisateurs et organisations.

La grande part des recherches de base qui constituent le fondement du présent rapport repose sur quatre groupes de réflexion mené auprès d'internautes canadiens tenus à Ottawa et à Toronto en octobre 2016. Le rapport propose également un examen des travaux de recherche publiés sur la vie privée en ligne et le comportement des internautes, de même que l'évolution de la protection des renseignements personnels sur mesure; et des entretiens et des consultations avec des intervenants, notamment des chercheurs universitaires, des représentants du secteur et Commissariat à la protection de la vie privée au Canada.

De nombreux Canadiens valorisent la protection de la vie privée pour des raisons qui vont de soi. Ils ne sont pas toujours d'accord avec la collecte et l'utilisation des renseignements à leur sujet par les entreprises, en particulier puisque la portée des activités de suivi n'est pas claire. Les participants aux groupes de discussion s'inquiétaient particulièrement de la collecte de certains types de renseignements de nature délicate, notamment en matière d'emplacement, d'emploi et d'orientation sexuelle.

Cependant, la plupart des canadiens estiment qu'ils n'ont pas de mot à dire sur le suivi de leurs activités en ligne. Un sondage d'opinion publique réalisé en 2016 commandé par le commissaire à la vie privée du Canada a conclu que 74 % des répondants estiment que la protection de leurs renseignements personnels dans leur vie quotidienne est inférieure à la situation d'il y a dix ans. Un Canadien sur deux était également en désaccord avec l'énoncé selon lequel ils pouvaient contrôler comment leurs renseignements personnels sont recueillis et utilisés par les organisations. Un participant au groupe de discussion a décrit la situation comme étant semblable à essayer d'arrêter au compte-gouttes un océan d'eau torrentielle se dirigeant vers lui. La plupart des participants aux groupes de

réflexion pensaient également que les services et les applications en ligne recueillaient et partageaient leurs renseignements à leur insu et sans leur consentement.

Si les experts en matière de protection de la vie privée et de services en ligne font valoir que de nombreux outils de confidentialité existent, de nombreux consommateurs semblent estimer qu'ils n'ont aucun choix ou contrôle quant au suivi et au partage de leurs renseignements personnels ou que les outils de protection de la vie privée existants ne sont pas utiles. La plupart des participants aux groupes de réflexion trouvent les outils relatifs à la confidentialité difficiles à comprendre ou à utiliser. Très peu de participant comprennent ou tentent même de lire les politiques de confidentialité et nombre d'entre eux ont conclu que les déclarations et les paramètres de confidentialité étaient modifiés à leur insu par les entreprises. Certains participants ont également constaté que le volume important des sites Web et applications utilisées rendait pratiquement impossible de gérer les paramètres de protection des renseignements personnels de chacun des sites Web.

Lorsque l'initiative du concept de protection intégrée des renseignements personnels, les participants aux groupes de réflexion étaient généralement ouverts à l'idée d'un guichet unique pour les paramètres et l'information de confidentialité par défaut. En particulier, les participants ont insisté sur l'importance du droit de choisir quand ils partagent leurs renseignements et comment ceux-ci sont utilisés et divulgués à d'autres parties.

De nombreux participants aux groupes de discussion ont convenu que les consommateurs aiment les services gratuits et qu'ils seraient peu disposés à payer un service en ligne ou à s'en passer afin de protéger leurs renseignements personnels. Toutefois, nombre des participants ont reconnu que des limites devraient s'imposer au suivi des activités en ligne. Ils ont fait valoir que les entreprises ne devraient pas suivre sans discrimination toutes les activités en ligne et que les utilisateurs devraient avoir la liberté d'interdire le suivi de certaines consultations considérées comme privées. Les participants aux groupes de réflexion ont également établi une distinction entre l'affichage sur internet en soi – accepté comme modèle courant de génération de revenus – et la collecte et la divulgation de masse à des fins multiples, y compris les publicités axées sur le comportement. Les groupes de discussion se souciaient tout particulièrement de la limite de la communication de leurs données personnelles aux entreprises et aux parties non liées au service initialement utilisé.

Les participants aux groupes de discussion préféraient généralement une case relative à la protection des renseignements personnels évidente, simple et facile à comprendre dotée d'un nombre limité d'options. Alors que certains participants souhaitaient un contrôle accru de la collecte de leurs renseignements en soi, la plupart s'inquiétaient du partage de leurs données avec des organismes tiers. Ils étaient également préoccupés par la collecte de renseignements jugés de nature délicate ou privée. De nombreux participants

souhaitaient également consulter des données particulières récemment recueillies auprès d'eux par des organisations.

Les recherches du CDIP appuient l'élaboration et la mise en œuvre d'une case relative à la protection des renseignements personnels qui :

- ❖ permet aux consommateurs d'interdire le suivi de leur emplacement. Cette protection intégrée pourrait également donner aux consommateurs la possibilité de sélectionner le type de renseignement qui peut ou non être recueilli ou suivi;
- ❖ permet aux consommateurs d'interdire le partage de données avec des tierces parties;
- ❖ propose des sommaires énonçant clairement : *a*) les tierces parties avec lesquelles les données de l'utilisateur sont partagées et l'emplacement des tiers, et *b*) le mode spécifique d'utilisation des données utilisateur;
- ❖ fournit aux utilisateurs des moyens d'accéder aux données récemment recueillies à leur sujet, par ordre d'organisation.

La protection intégrée des renseignements personnels sur mesure est et deviendra de plus en plus importante en vue de protéger la vie privée des Canadiens et d'assurer qu'ils disposent de choix et de contrôles réels, notamment en matière de consentement significatif visant la collecte, l'utilisation et la divulgation de leurs renseignements. À mesure que l'innovation continue de figurer au cœur du programme politique du gouvernement fédéral canadien, les décideurs doivent apporter un soutien financier et autre à la confidentialité adaptée.

Recommandations du CDIP

Recommandation n° 1

La « Protection intégrée des renseignements » développée dans le présent rapport doit être prise en compte par toutes les entreprises et les organismes privés dotés d'une présence en ligne et idéalement coordonnées par une association du secteur (telle que les Normes canadiennes de publicité ou la Network Advertising Initiative).

Recommandation n° 2

Le commissariat à la vie privée du Canada doit publier des lignes directrices sur l'adoption et la mise en œuvre de mesures de protection de la vie privée par les

services et application en ligne, l'accent étant particulièrement mis sur les organisations privées. Il doit également, de manière générale, mettre en relief la protection intégrée des renseignements personnels sur mesure, notamment : a) la publication de rapports et de documents de recherche; b) l'instauration de lignes directrices claires et d'exemples ou la création d'une norme de protection intégrée des renseignements sur mesure.

Recommandation n° 3

Les exigences de protection des renseignements sur mesures doivent être inscrits dans la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) fédérale.

Recommandation n° 4

Le gouvernement de Canada doit consacrer un financement public aux initiatives et à la recherche sur la protection intégrée des renseignements personnels sur mesure, en particulier celles entreprises par des organismes sans but lucratif et des chercheurs universitaires.

Recommandation n° 5

Les législateurs et les décideurs fédéraux doivent envisager de retirer la permission d'obtenir un consentement implicite de la collecte, de l'utilisation et de la divulgation des renseignements personnels aux termes de la LPRPDE. Il y a également lieu d'envisager l'interdiction du regroupement des modalités de confidentialité que l'utilisateur doit accepter en vue d'accéder un service en ligne ou de s'en servir.

Recommandation n° 6

Le commissariat à la vie privée du Canada doit réexaminer l'efficacité et la pertinence des politiques de protection de la vie privée à titre de mode de communication des principales informations en la matière aux particuliers.

Table des matières

Remerciements	iii
Résumé	iv
I. Introduction	1
II. Les consommateurs accordent-ils de la valeur à la protection de la vie privée?	3
2.1 Les Canadiens accordent de la valeur à la protection de la vie privée	4
2.2 Les Canadiens n'ont pas toujours l'impression d'avoir le choix ou d'exercer un contrôle en ce qui a trait à leurs renseignements personnels.....	12
III. Les consommateurs et les outils de protection de la vie privée.....	18
3.1 Outils de protection de la vie privée existants et lois applicables	18
3.2 Utilisation des outils de protection de la vie privée par les consommateurs.	23
IV. Vers la création d'une « case relative à la vie privée ».....	31
4.1 Principes de protection intégrée de la vie privée.....	31
4.2 Attitudes des consommateurs à l'égard d'une case relative à la vie privée ...	35
4.3 Adhésion des intervenants et des services.....	38
4.4 Caractéristiques de la case relative à la vie privée	44
4.4.1 Qu'est-ce que la case relative à la vie privée devrait inclure?.....	44
4.4.2 À quoi devrait ressembler la case relative à la protection des renseignements personnels?	48
4.5 Existe-t-il un compromis en matière de protection des renseignements personnels?	54
V. Sommaire et recommandations.....	58
5.1 Il y a place à de nouvelles initiatives de vie privée sur mesure, ce qui comprend la protection intégrée des renseignements personnels.....	58
5.2 Recommandations finales.....	61
Bibliographie	67

I. Introduction

Qu'est-ce que la « protection intégrée de la vie privée »? D'après Ann Cavoukian, ancienne commissaire à l'information et à la protection de la vie privée de l'Ontario, la protection intégrée de la vie privée « s'inscrit dans l'optique que l'avenir de la vie privée ne peut pas être certifiée qu'en conformité aux cadres législatifs et réglementaires; au contraire, la certification de la vie privée doit devenir le mode l'opération par défaut d'une organisation¹. »

La protection intégrée de la vie privée ne concerne pas que la conception de la sécurité, qui vise à protéger l'information recueillie². En effet, la protection intégrée de la vie privée reconnaît que la collecte, l'utilisation et la divulgation de l'information dépendent des lois et règlements, de la technologie, des normes culturelles, de l'économie et, ce sur quoi met l'accent le présent rapport, des utilisateurs³.

Bien que les organismes de réglementation, les décideurs et les intervenants de l'industrie aient déjà discuté longuement de la protection intégrée de la vie privée, peu d'études ont abordé la question du point de vue du consommateur. Pensons notamment à des sujets tels que le droit de regard et le choix quant à la collecte de renseignements personnels, ou bien la facilité de l'accès et de l'utilisation des outils de protection de la vie privée.

Le présent rapport du Centre pour la défense de l'intérêt public (CDIP) se penche sur la possible création d'une « trousse de protection de la vie privée » universelle qui contiendrait des paramètres de protection et de l'information à l'intention du consommateur. Cette étude vise à sonder l'intérêt des consommateurs pour un ensemble normalisé de paramètres ou d'information qu'un utilisateur n'appliquerait qu'une fois et qui seraient valides d'une plate-forme à l'autre, comme les fureteurs Internet, les tablettes et les téléphones intelligents. Le rapport contient aussi les commentaires d'utilisateurs au sujet des fonctions de la trousse de protection de la vie privée, comme son apparence et la possibilité de la rendre obligatoire pour les utilisateurs et les organisations. Bien qu'une trousse de protection de la vie privée soit applicable à la fois aux organisations publiques et privées, dans cette étude, le CDIP s'est particulièrement intéressé aux organisations commerciales privées.

¹ Ann Cavoukian, *Privacy by Design* (2013), en ligne : CIPVP <<https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf>>, p. 1.

² Ann Cavoukian, Stuart Shapiro et R. Jason Cronk, *Privacy Engineering: Proactively Embedding Privacy, by Design* (janvier 2014), en ligne : CIPVP <<https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-priv-engineering.pdf>>, p. 5.

³ *Idem*.

Dans la première section du rapport, nous examinerons l'opinion des Canadiens sur la vie privée et la valeur qu'ils lui accordent, et nous verrons de quelle façon cette opinion change en fonction du contexte, des relations et du type d'information. Les consommateurs croient-ils en la vie privée seulement par principe? Comment les attentes à l'endroit de la vie privée ont-elles changé, particulièrement en ce qui concerne Internet? La deuxième section aborde les lois et les outils actuels liés à la protection de la vie privée des personnes. Ces outils sont-ils efficaces? Sont-ils largement utilisés par les consommateurs? Dans la troisième section, nous détaillons les conclusions du CDIP concernant la trousse de protection de la vie privée, notamment l'accueil de la trousse par les consommateurs, les outils et l'information à inclure absolument, ainsi que les fonctions et l'apparence de la trousse. Dans la dernière section, nous résumons la discussion et les faits saillants que la recherche réalisée en vue du rapport a mis au jour. Nous y présentons aussi les recommandations finales du CDIP.

La majeure partie de la recherche originale réalisée pour le rapport découle de quatre groupes de discussion avec des utilisateurs d'Internet canadiens à Ottawa et Toronto par l'agence d'étude de marché Environics Research Group en octobre 2016. Quatre groupes ont été créés : un en français et trois en anglais. Pour être sélectionnés, les participants n'avaient qu'à être des utilisateurs réguliers d'Internet sans autre exigence précise quant aux caractéristiques démographiques. Deux groupes ont été répartis en fonction de l'âge; un des groupes était composé des participants de 40 à 70 ans, et l'autre des 18 à 39 ans. Le rapport comporte aussi une analyse documentaire de la recherche sur la vie privée en ligne, le comportement des utilisateurs et les réalisations liées à la protection intégrée de la vie privée. Des entrevues et consultations avec des intervenants tels que des chercheurs en milieu universitaire, des représentants de l'industrie et le Commissariat à la protection de la vie privée du Canada enrichissent le rapport. Nous remercions chaleureusement tous les intervenants qui ont participé à l'étude.

II. Les consommateurs accordent-ils de la valeur à la protection de la vie privée?

Les recherches effectuées par le CDIP montrent que les consommateurs canadiens accordent de la valeur à la protection de la vie privée en ligne, mais croient que la capacité de vraiment protéger leurs renseignements personnels diminue rapidement.

Un rapport de 2014 sur les mégadonnées et sur la protection de la vie privée rédigé par le conseil présidentiel d'experts en science et technologie, aux États-Unis, a révélé ce qui suit :

[Traduction]

Les mégadonnées sont « méga » dans deux sens distincts. Elles le sont du point de vue de la quantité et de la diversité des données qui sont accessibles à des fins de traitement. Par ailleurs, elles sont « méga » du point de vue de l'échelle d'analyse (appelée « analytique ») qui peut leur être appliquée à la limite pour tirer des déductions et des conclusions. Grâce à l'exploration de données et à d'autres types d'analytique, des renseignements non évidents et parfois personnels peuvent être obtenus à partir de données qui, au moment de leur collecte, ne semblaient poser aucun problème du point de vue de la vie privée ou n'en poser que des gérables. [...] Même en principe, toutefois, on ne peut jamais savoir quels renseignements pourraient, plus tard, être extraits de tout groupe de mégadonnées particulier, puisque ces renseignements pourraient simplement découler de la combinaison d'ensembles de données apparemment sans lien et que l'algorithme servant à révéler les nouveaux renseignements n'avait peut-être même pas encore été inventé au moment de la collecte des renseignements.

Les données et l'analytique qui offrent des avantages aux personnes et à la société peuvent, même lorsqu'elles sont utilisées de façon appropriée, causer des préjudices potentiels ou poser des menaces pour les renseignements communiqués à grande échelle et personnels, selon les normes relatives à la protection de la vie privée⁴.

L'International Data Corporation estime que, dans le monde entier, les recettes liées aux mégadonnées et à l'analyse des activités augmenteront pour passer de 122 milliards de

⁴ Bureau administratif du président, conseil présidentiel d'experts en science et technologie, *Report to the President on Big Data and Privacy: A Technological Perspective*, 2014, en ligne : HSDL, <<https://www.hsdl.org/?view&did=755569>>, p. ix-x.

dollars en 2015, à plus de 187 milliards de dollars d'ici 2019⁵. Au Canada, le Conseil des technologies de l'information et des communications estime que le marché des services de mégadonnées a généré environ 1,1 milliard de dollars de recette en 2015 et qu'il devrait presque doubler d'ici 2020⁶.

Cela signifie que les données personnelles des Canadiens ont de la valeur, et que cette valeur augmente probablement. Comme les Canadiens pourraient passer des années, voire des décennies et, dans le cas des enfants, peut-être même leur vie entière sur un service en ligne comme un site Web de réseautage social, la quantité de renseignements personnels recueillis auprès d'un utilisateur pourrait être effarante.

2.1 Les Canadiens accordent de la valeur à la protection de la vie privée

Bennett et Bayley affirment que les gens comprennent la protection de la vie privée et qu'ils y accordent de la valeur, même si les attentes et les normes en matière de protection des renseignements personnels changent. Dans l'ouvrage intitulé *Exploring the Boundaries of Big Data* publié par le Conseil scientifique pour les politiques gouvernementales des Pays-Bas, les auteurs écrivent ce qui suit :

[Traduction]

Les sondages d'opinion sur la vie privée ont une longue histoire controversée. Les méthodes qui s'y rattachent et leur utilité varient considérablement. Cependant, un thème commun les relie. Le grand public peut généralement faire la distinction entre les demandes légitimes et illégitimes de données personnelles. La plupart des gens savent comment appliquer le critère du « ce ne sont pas vos affaires ». La limite varie au fil du temps et en fonction d'une foule de variables démographiques et culturelles⁷.

La protection de leurs propres renseignements personnels a de l'importance pour la plupart des Canadiens. Le sondage d'opinion publique mené auprès des Canadiens en 2016 par le Commissariat à la protection de la vie privée (CPVP) du Canada a révélé

⁵ International Data Corporation, « Worldwide Big Data and Business Analytics Revenues Forecast to Reach \$187 Billion in 2019, According to IDC », 23 mai 2016, en ligne : IDC, <<https://www.idc.com/getdoc.jsp?containerId=prUS41306516>>.

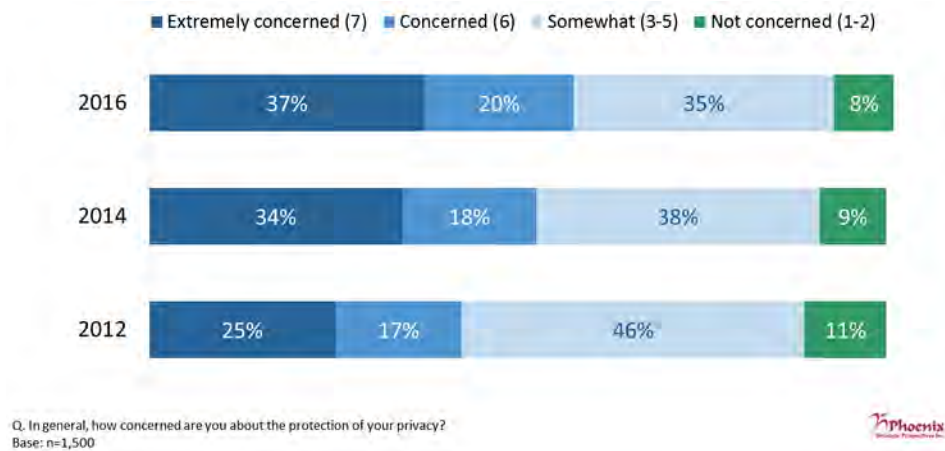
⁶ Conseil des technologies de l'information et des communications, *Big Data and the Intelligence Economy: Canada's Hyper Connected Landscape*, 2015, en ligne : ICTC <<http://www.ictc-ctic.ca/wp-content/uploads/2015/12/BIG-DATA-2015.pdf>>, p. 4.

⁷ Bennett, Colin J. et Robin M. Bayley, « Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments », dans van der Sloot, Bart, Dennis Broeders et Erik Schrijvers, eds., *Exploring the Boundaries of Big Data* (Amsterdam: Amsterdam University Press, 2016), p. 209.

que **92 % des Canadiens** sont préoccupés au sujet de la protection de leurs renseignements personnels⁸.

⁸ Commissariat à la protection de la vie privée du Canada, *Sondage auprès des Canadiens sur la protection de la vie privée de 2016 : Rapport final*, 2016, en ligne : Priv.gc.ca < https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/por_2016_12/>, figure 2.

Figure 2-1. Préoccupation au sujet de la protection des renseignements personnels



Source : Commissariat à la protection de la vie privée du Canada, 2016

Des groupes de discussion organisés par Option consommateurs dans le but d’analyser la publicité comportementale en ligne ont également montré que les participants étaient surpris et préoccupés une fois informés de la mesure dans laquelle leurs renseignements personnels étaient recueillis et suivis et du fait que c’était même le cas des renseignements provenant de comptes de courriel personnels⁹. Certains participants ont évoqué des scénarios d’un futur orwellien ou dystopique.

Ces résultats se reflètent de la même manière dans des sondages américains menés en 2015 par le centre de recherche Pew, lesquels ont montré ce qui suit :

- Des Américains interrogés, 93 % ont affirmé qu’il était important de pouvoir décider qui pouvait obtenir des renseignements à leur sujet;

⁹ Option consommateurs, *Le prix de la gratuité : Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne?*, 2015, en ligne : Option consommateurs <https://www.option-consommateurs.org/documents/principal/en/File/option_consommateurs_2015_gratuite_english.pdf>, p. 31.

« En fait, la protection de la vie privée a de la valeur dans son propre intérêt. Si j'avais voulu rendre mes renseignements publics, j'aurais choisi de les publier. Même quand nous allons dans les magasins, on nous demande si nous voyons un inconvénient à donner notre code postal. Oui, j'y vois un inconvénient. Vous n'avez pas besoin de l'obtenir. Peut-être que les commerçants veulent l'obtenir afin de déterminer la démographie de leurs clients et de savoir d'où ils viennent, mais ils n'ont pas besoin de savoir. Le fait de disposer de notre code postal leur permet de savoir exactement où nous vivons. »

« On reçoit les choses gratuitement, mais ce n'est pas vraiment gratuit parce qu'en fait, c'est un cadeau empoisonné, ce n'est pas vrai. Ça devrait être totalement transparent. »

« Pour le consommateur, l'avantage est allé au commerçant, puis c'est que, moi, si je veux bien avoir une expectative de quiétude... mais ce n'est pas vrai que je donne carte blanche à tout le monde pour faire connaître mes tendances et plein de choses pour lesquelles je ne donne pas mon consentement. »

– Participants au groupe de discussion du CDIP

- Il était important pour 90 % d'entre eux de pouvoir décider lesquels de leurs renseignements étaient recueillis;

- Il était important pour 88 % d'entre eux que personne ne les regarde ou ne les écoute sans leur permission¹⁰.

La disposition des consommateurs à communiquer leurs renseignements personnels variait en fonction de la situation. Option consommateurs a conclu que les consommateurs étaient plus disposés à communiquer certains types de renseignements, comme l'alimentation, le divertissement et les passe-temps, et qu'ils répugnaient à en communiquer d'autres, comme les renseignements médicaux et sur les relations amoureuses¹¹.

Un sondage national commandé par le CDIP aux fins de son rapport de 2015 intitulé *Off the Grid* a révélé que 77 % des Canadiens étaient [traduction] « un peu mal à l'aise » ou « très mal à l'aise » avec l'idée qu'un détaillant, une application en ligne ou un fournisseur de services de télécommunication puisse les localiser d'après l'utilisation de leur téléphone intelligent ou de leur tablette¹². Quand les participants ont été appelés à indiquer leurs principales préoccupations à l'égard de la localisation, la réponse la plus fréquente (32 %

¹⁰ Madden, Mary et Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, 2015, centre de recherche Pew, <<http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>>, p. 17.

¹¹ Option consommateurs, *Le prix de la gratuité : Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne?*, 2015, en ligne : Option consommateurs <https://www.option-consommateurs.org/documents/principal/en/File/option_consommateurs_2015_gratuite_english.pdf>, p. 34.

¹² White, Geoff, *Off the Grid: Pinpointing Location-based Technologies and the Law* (Ottawa: Centre pour la défense de l'intérêt public, 2015, en ligne : CDIP <<http://www.CDIP.ca/wp-content/uploads/2016/03/Off-the-Grid-Pinpointing-Location-based-Technologies-and-the-Law-September-8-2015.pdf>>, annexe A, figure 6.

des répondants) était qu'il s'agissait en définitive d'une [traduction] « atteinte à la vie privée¹³ ». La deuxième réponse la plus fréquente (14 %) était que ce n'étaient « les affaires de personne », et 11 % des répondants craignaient que leurs renseignements soient « mal utilisés, vendus ou communiqués ».

Le centre de recherche Pew a également découvert que le contexte de la collecte et de l'utilisation des renseignements personnels a de l'importance, puisque 52 % des Américains estimaient qu'il était acceptable de divulguer des renseignements sur la santé à une base de données sécurisée en ligne à laquelle leurs médecins ont accès, alors que 51 % ont affirmé qu'il n'était pas acceptable qu'une plateforme de médias sociaux gratuite leur présente des publicités fondées sur leurs renseignements, et 55 % ont déclaré qu'il n'était pas acceptable d'installer un thermostat intelligent qui pouvait surveiller les déplacements dans la maison et peut-être réduire leur facture d'électricité¹⁴.

« Je travaille dans le domaine du marketing et de l'administration des affaires, et je sais que les renseignements sont utiles et qu'ils contribuent à l'élaboration de nouveaux produits et à ce genre de choses. Toutefois, en même temps, je veux pouvoir décider à quels renseignements je donne accès et lesquels sont utilisés. »

– Participant au groupe de discussion du CDIP

Enfin, les Américains croyaient également que la période pendant laquelle une entreprise conservait les renseignements personnels devrait être limitée. Par exemple, la moitié d'entre eux pensaient que les annonceurs en ligne ne devraient enregistrer aucun renseignement sur leurs activités, alors que seulement 5 % croyaient que ces derniers devraient conserver les renseignements pour aussi longtemps qu'ils en avaient besoin¹⁵. Les réponses variaient en fonction du type d'organisation qui recueillait les renseignements, c'est-à-dire que 22 % des Américains affirmaient que les sociétés émettrices de carte de crédit devraient conserver les renseignements sur leurs activités pour aussi longtemps qu'elles en avaient besoin.

¹³ *Ibid.*, figure 8.

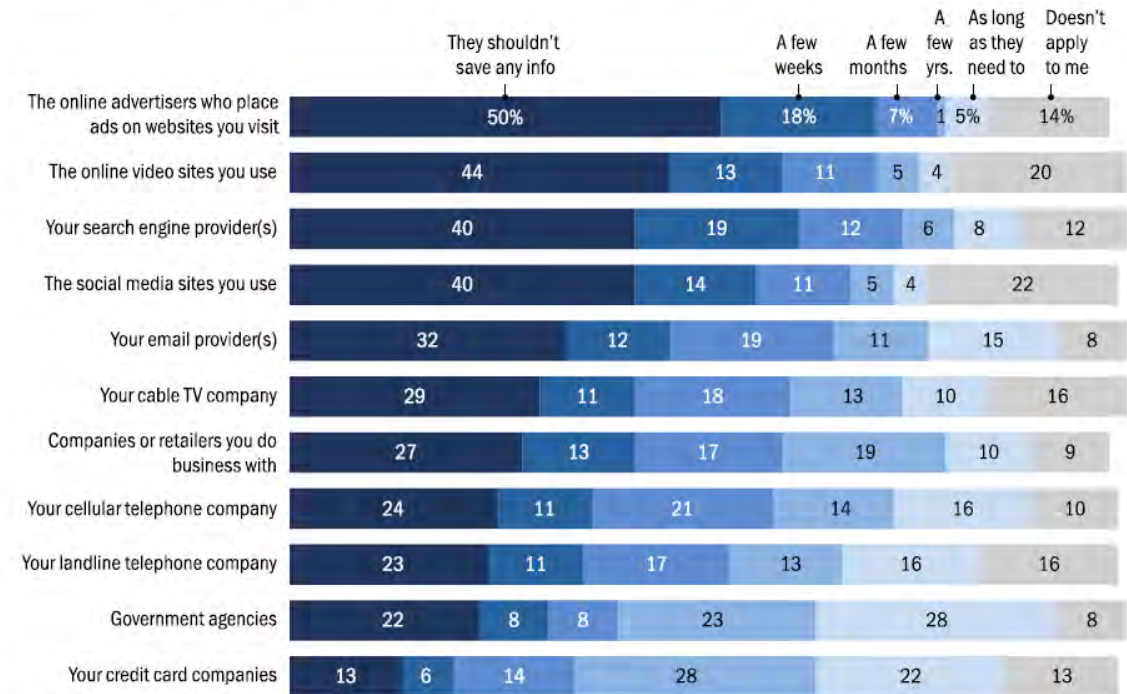
¹⁴ Rainie, Lee et Maeve Duggan, *Privacy and Information Sharing*, 2016, en ligne : Pew Research Center <http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf>, p. 4.

¹⁵ Madden, Mary et Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, 2015, centre de recherche Pew <<http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>>, p. 25.

Figure 2-2. Attentes quant à la durée de la période pendant laquelle les organisations devraient tenir des registres des activités

Most Expect Limits on How Long the Records of Their Activity Are Stored

% of adults who think the following length of time is "reasonable" for different companies or organizations to retain records or archives of their activity



Source: Pew Research Center's Privacy Panel Survey #2, Aug. 5, 2014-Sept. 2, 2014 (N=498). Refused responses not shown.

PEW RESEARCH CENTER

Source : centre de recherche Pew, 2015

D'autres études indiquent également que les consommateurs changent leur comportement et leurs activités en ligne en réaction à des menaces réelles ou perçues pour leur vie privée. Par exemple, la National Telecommunications and Information Administration des États-Unis a découvert que 45 % des ménages en ligne avaient déclaré qu'au cours de la dernière année, des préoccupations relatives à la protection de leurs renseignements personnels ou à leur sécurité les avaient arrêtés au moment de faire ce qui suit : [traduction] « effectuer des transactions financières, acheter des biens ou des services, afficher des renseignements sur des réseaux sociaux ou exprimer des opinions sur des enjeux controversés ou politiques sur Internet », ce qui a eu des

« conséquences néfastes » sur l'activité économique en ligne et sur le libre-échange d'idées¹⁶.

L'inverse est également vrai. Les consommateurs tendent à être plus disposés à interagir avec des organisations qui mettent en œuvre et favorisent des pratiques rigoureuses en matière de protection des renseignements personnels et à faire leurs achats auprès de ces organisations. Dans une étude expérimentale, Tsai et coll. ont conclu ce qui suit :

[Traduction]

[...] les participants à qui des renseignements essentiels sur la vie privée avaient été fournis ont pris ces renseignements en considération en effectuant des achats auprès de sites Web offrant des niveaux de protection des renseignements personnels moyens ou élevés. Nos résultats indiquent que, contrairement au point de vue courant selon lequel les consommateurs sont peu susceptibles de payer pour protéger leurs renseignements personnels, ces derniers pourraient être disposés à payer un supplément afin de protéger leur vie privée¹⁷.

Une recherche expérimentale effectuée par Acquisti, Brandimarte et Loewenstein a également montré que [traduction] « même si les personnes abandonnent parfois leurs données personnelles pour de petits avantages ou rabais, à d'autres moments, elles engagent volontairement des coûts importants afin de protéger leur vie privée¹⁸ ». Par exemple, dans le cadre d'une expérience où la moitié des participants se sont vu remettre une carte cadeau « anonyme » de 10 \$ (les transactions effectuées au moyen de la carte n'allaient pas permettre de retracer le sujet) et l'autre moitié, une carte de 12 \$ retraçable (les transactions effectuées au moyen de cette carte allaient être liées au nom du sujet), tous les participants se sont ensuite vu offrir l'option d'échanger leur carte pour l'autre carte. Acquisti et coll. ont constaté que [traduction] « cinq fois plus de participants (52,1 %) ont choisi [la carte anonyme de 10 \$] et l'ont conservée au lieu de l'échanger pour l'autre carte que de participants qui, au départ, détenaient la carte ayant la plus grande valeur (9,7 %) ¹⁹ ». Par conséquent, de nombreux consommateurs reconnaissent la protection de la vie privée et y accordent de la valeur lorsqu'ils y ont accès.

¹⁶ Goldberg, Rafi, « Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities », 13 mai 2016, en ligne : NTIA <<https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>>.

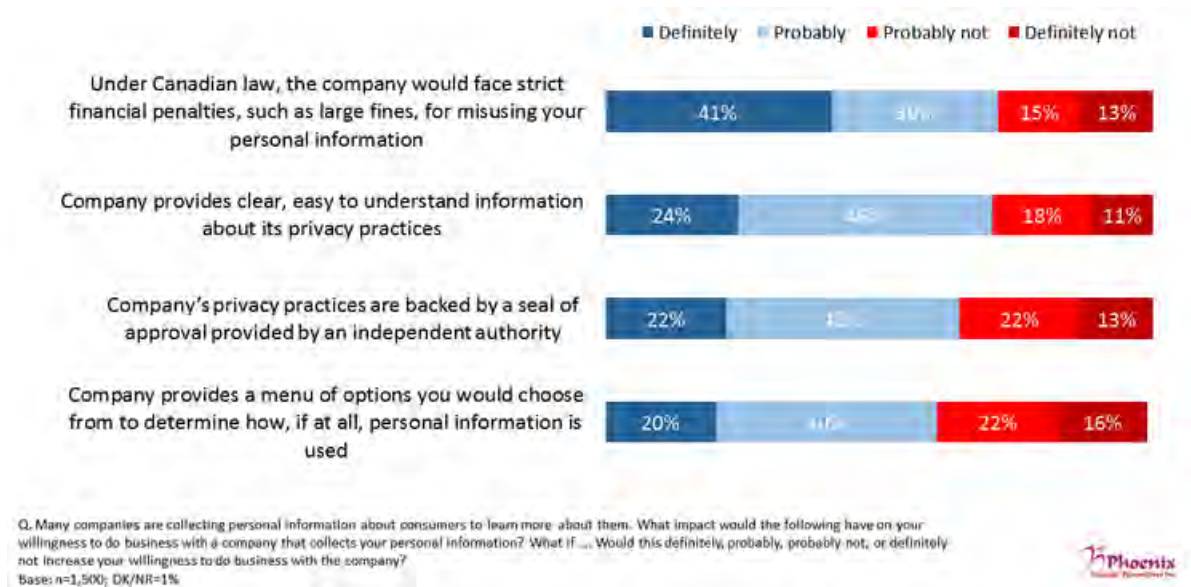
¹⁷ Tsai, Janice Y., Serge Egelman, Lorrie Cranor et Alessandro Acquisti, « The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study », 2011, 22 :2, *Information Systems Research*, 25, p. 266.

¹⁸ Acquisti, Alessandro, Laura Brandimarte et George Loewenstein, « Privacy and Human Behavior in the Age of Information », 2015, 347:6221, *Science* 509, p. 510.

¹⁹ *Ibid.*

Le sondage d'opinion publique mené par le CPVP a également indiqué que les pratiques des entreprises en matière de protection des renseignements personnels ont une incidence sur la disposition de la majorité des Canadiens à faire affaire avec ces entreprises.

Figure 2-3. Mesure dans laquelle les lois et les pratiques relatives à la protection de la vie privée influent sur la disposition des consommateurs à faire affaire avec une entreprise



Source : Commissariat à la protection de la vie privée du Canada, 2016

Par conséquent, une grande partie des consommateurs canadiens accordent de la valeur à la protection de leurs renseignements personnels et sont préoccupés à ce sujet. Les menaces d'atteinte à la vie privée et le fait d'avoir subi de telles atteintes influent sur la disposition des consommateurs à mener une activité en ligne.

2.2 Les Canadiens n'ont pas toujours l'impression d'avoir le choix ou d'exercer un contrôle en ce qui a trait à leurs renseignements personnels

Pourtant, une grande partie des Canadiens semblent avoir l'impression d'exercer aujourd'hui moins de contrôle que jamais sur la façon dont leurs renseignements personnels sont recueillis et utilisés. Le sondage d'opinion publique réalisé par le CPVP a révélé que 74 % des répondants — le pourcentage le plus élevé des huit derniers sondages du CPVP — avaient l'impression que leurs renseignements personnels étaient moins protégés dans le cadre de leur vie quotidienne qu'ils l'étaient il y a 10 ans²⁰. Un Canadien sur deux était également en désaccord avec l'énoncé selon lequel ils estimaient qu'ils pouvaient décider comment leurs renseignements personnels sont recueillis et utilisés par les organisations²¹. En outre, seulement environ la moitié des Canadiens étaient convaincus qu'ils disposaient de suffisamment d'information pour savoir comment les nouvelles technologies pourraient influencer sur leurs renseignements personnels²².

Figure 2-4. Contrôle sur les renseignements personnels recueillis et utilisés



Source : Commissariat à la protection de la vie privée du Canada, 2016

²⁰ Commissariat à la protection de la vie privée du Canada, *Sondage auprès des Canadiens sur la protection de la vie privée de 2016 : Rapport final*, 2016, en ligne : Priv.gc.ca <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/por_2016_12/>, figure 4.

²¹ *Ibid.*, figure 5.

²² *Ibid.*, figure 3.

Un sondage de 2015 mené auprès de résidents de l'Union européenne a également révélé que seulement 15 % des répondants avaient l'impression d'exercer un contrôle complet sur les renseignements qu'ils fournissaient en ligne et que 31 % croyaient qu'ils n'avaient absolument aucun contrôle²³. Parallèlement, 71 % des répondants ont affirmé que la fourniture de renseignements personnels faisait [traduction] « de plus en plus partie de la vie moderne », et 58 % étaient d'accord pour dire qu'on n'a « pas d'autre choix que de fournir des renseignements personnels si l'on veut obtenir des produits ou des services²⁴ ».

Le centre de recherche Pew a également découvert que peu d'Américains croient que leurs dossiers seront tenus confidentiels et en lieu sûr par les organisations. De façon générale, ils affirment faire le plus confiance aux sociétés émettrices de cartes de crédit, aux

organismes gouvernementaux et aux compagnies de téléphone, et ils font le moins confiance aux moteurs de recherche, aux médias sociaux, aux sites de vidéos en ligne et aux annonceurs en ligne²⁵.

« Ainsi, en réalité, d'une certaine manière, oui, il s'agit d'une atteinte [à la vie privée]; toutefois, il faut tout simplement l'accepter parce que, dans un certain sens, que pouvons-nous y faire? »

« Eh bien, le problème que posent les accords sur Internet, c'est qu'il s'agit du genre d'entente où l'on obtient tout ou rien. Si on accepte les conditions, on peut utiliser Internet, mais, si on ne les accepte pas, on ne peut pas utiliser Internet. »

– Participants au groupe de discussion du CDIP

²³ Direction générale de la justice et des consommateurs de la Commission européenne, *Special Eurobarometer 431: Data Protection Report*, 2015, en ligne : Europa.eu, <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf>, p. 6.

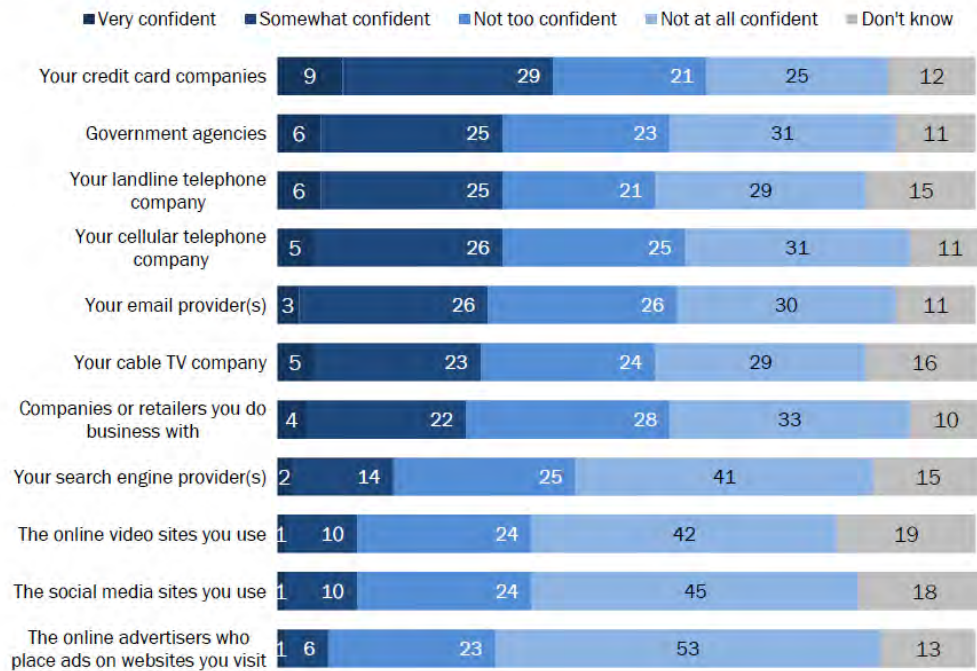
²⁴ *Ibid.*, p. 28-29.

²⁵ Madden, Mary et Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, 2015, centre de recherche Pew <<http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>>, p. 29.

Figure 2-5. Confiance à l'égard du fait que leurs dossiers resteront confidentiels et en lieu sûr

Few Express Confidence That Their Records Will Remain Private and Secure

% of adults who say they are ... that the records of their activity maintained by various companies and organizations will remain private and secure



Source: Pew Research Center's Privacy Panel Survey #2, Aug. 5, 2014-Sept. 2, 2014 (N=498). Refused responses not shown.

PEW RESEARCH CENTER

Source : centre de recherche Pew, 2015

Natasha Tusikov, professeure adjointe à l'Université York, a affirmé lors d'une entrevue que les gens comprennent généralement le fait que le contexte a de l'importance et qu'ils pourraient, par exemple, changer ce qu'ils communiquent à un réseau social par rapport à ce qu'ils communiquent à une institution financière. Toutefois, elle croyait que les consommateurs ne sont peut-être pas conscients des vastes conséquences de la façon dont leurs données sont stockées, traitées et communiquées, même sur des plates-forme comme Spotify. Par ailleurs, M^{me} Tusikov était d'avis que, même si les consommateurs sont généralement au courant des énormes atteintes à la protection des données, comme dans le cas de Target ou d'Ashley Madison, ils pourraient croire à tort que, pourvu qu'ils ne s'adonnent pas à des activités illégales ou déplorables comme tromper leur conjoint, ils ne subiront pas de préjudices liés à la collecte, à l'utilisation et à la communication de leurs données. M^{me} Tusikov se

doute que ces impressions ou croyances pourraient changer dans l'avenir, compte tenu de l'Internet des objets et des appareils portables, et que les consommateurs pourraient prendre de plus en plus conscience des répercussions du suivi et de la collecte des données.

En général, les participants aux groupes de discussion accordaient de la valeur à la protection de leur vie privée et à la capacité d'exercer un contrôle sur les renseignements personnels qui étaient recueillis auprès d'eux et utilisés. L'opinion des participants variait en fonction du type de renseignements recueillis. Certains s'opposaient à la collecte de tout renseignement qu'ils ne divulguaient pas volontairement. De nombreux participants ne s'opposaient pas à la collecte de renseignements comme les passe-temps, le divertissement ou les intérêts. Cependant, tous les participants s'opposaient généralement à la collecte de types de renseignements de nature plus « délicate », comme les renseignements sur la santé, les renseignements financiers et même leurs adresses IP. Les participants étaient particulièrement préoccupés au sujet de la géolocalisation ou du suivi fondé sur l'emplacement et préféraient fortement ne pas être suivis lorsqu'ils se déplacent. Ils étaient également très préoccupés au sujet de l'utilisation des renseignements recueillis auprès d'eux dans le but de prendre des décisions qui pourraient les toucher, comme les décisions relatives à l'emploi, à l'assurance ou à la santé.

Sans égard à ce qu'ils pensaient du suivi et de la protection de la vie privée en ligne, la plupart des participants étaient conscients du fait que leurs activités en ligne faisaient probablement l'objet d'un suivi et avaient l'impression de ne pas pouvoir faire grand-

« En réalité, il n'y a aucune protection de la vie privée, même si on est discret. Il y a certaines choses qu'on ne communique pas. On communique tout de même des bribes d'information. Alors, nous n'avons pas vraiment de vie privée. »

« Nous parlions de l'idée des marques permanentes. On met quelque chose sur Internet, et ça y reste pour toujours. »

« Comme l'information qu'on demande, qu'on veut obtenir, sur Wikipédia ou sur Google, c'est super accessible, mais aussi, de l'autre côté, comme on l'a déjà dit, le problème, sur Internet, même si c'est sur un compte privé confidentiel sécuritaire, c'est qu'une fois que c'est sur Internet, c'est sur Internet pour toujours. »

« Je suppose que c'est ce que c'est. J'aime les médias sociaux. Alors, au bout du compte, toutes ces choses n'ont pas vraiment d'importance. Je vais tout de même être sur Internet. Peut-être que... j'ai comme envie d'aller chez moi pour faire une recherche sur Google afin de savoir ce qui arrive avec mes données, puis regarder une vidéo sur YouTube. Je veux savoir. »

– Participants au groupe de discussion du CDIP

chose pour que cesse ce suivi. Toutefois, nombre d'entre eux étaient encore surpris par l'ampleur du suivi en ligne et de la communication des renseignements recueillis auprès des utilisateurs. Un extrait d'une étude portant sur les sites Web populaires menée en 2015 par des chercheurs de l'Université de la Pennsylvanie a été cité aux participants. Cette étude avait révélé ce qui suit :

[Traduction]

[P]rès de 9 sites Web sur 10 divulguent des données d'utilisateurs à des parties, probablement sans que l'utilisateur le sache; plus de 6 sites Web sur 10 génèrent des témoins de tierces parties; et plus de 8 sites Web sur 10 téléversent le code JavaScript de parties externes vers l'ordinateur des utilisateurs. Les sites qui divulguent des données d'utilisateurs communiquent avec en moyenne neuf domaines externes, ce qui indique que les utilisateurs pourraient être suivis par une multitude d'entités en parallèle²⁶.

Même si certains participants n'étaient pas complètement surpris par ces révélations, ils ne s'attendaient pas nécessairement à l'ampleur du suivi qui avait lieu en ligne, surtout sans leur consentement apparent ou à leur insu. Les participants étaient particulièrement préoccupés au sujet des renseignements qui sont communiqués à des sites Web et à des applications externes. Même s'ils s'attendaient à ce que les sites Web qu'ils visitaient recueillent des renseignements à leur sujet, ils ne s'attendaient pas à ce que ces renseignements soient mis en commun et communiqués à des tiers.

Quoi qu'il en soit, en général, les participants avaient l'impression qu'il n'y avait rien à faire pour arrêter ou limiter le suivi en ligne et le traitement des données ou pour mieux protéger les renseignements personnels. Un participant a décrit la situation comme le fait de tenter d'empêcher un océan de se déverser sur lui « au moyen d'un compte-goutte ». Certains participants ont manifesté une forte méfiance à l'égard des entreprises privées en ligne; ils ont affirmé se demander, même dans une situation hypothétique, où une politique de confidentialité prétendrait que l'entreprise n'allait pas utiliser ou divulguer de renseignements personnels, s'ils croiraient cette déclaration. Certains participants trouvaient du réconfort dans le fait qu'Internet compte des millions d'utilisateurs et que les ensembles de données abondent, ce qui réduit la probabilité qu'ils soient personnellement ciblés ou touchés par des activités de suivi.

²⁶ Libert, Timothy, « Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites », 2015, 9, *International Journal of Communication*, 3544.

Par conséquent, de nombreux Canadiens semblent accorder de la valeur à la protection de la vie privée pour ce qu'elle est. Ils ne sont pas toujours d'accord pour que les

« Il est clair que c'est pas juste ton information; tu fais partie des millions et des billions de gens. Tu es tellement petit dans le, comment dit-on, "the amount of information" [la quantité d'information], vous savez, "the pool" [le bassin]; tu es tellement petit que, si tu te fais prendre, c'est comme si tu te faisais frapper par un éclair. »

« Toutefois, si vous n'êtes qu'une personne ordinaire, normale et ennuyante, comme ce genre de personnes sont très nombreuses sur Internet, vous vous en tirez assez bien. Les probabilités que vous soyez victime de piratage et de choses de ce genre ne sont pas très élevées. »

– Participants aux groupes de discussion du CDIP

entreprises recueillent et utilisent les renseignements à leur sujet, surtout puisque l'étendue de ces activités de suivi n'est pas claire. Toutefois, ils ont l'impression de n'exercer pratiquement aucun contrôle sur les pratiques et les activités de suivi en ligne. Ils sont conscients du fait que leurs données sont maintenant une source de revenus pour les entreprises en ligne et que ces dernières sont peu susceptibles d'« abandonner » leurs données volontairement. Les participants aux groupes de discussion ont également déclaré que l'accès à Internet et son utilisation sont maintenant presque une nécessité; la plupart avaient l'impression qu'il était presque impossible d'arrêter d'y recourir ou de l'utiliser dans le but de protéger leurs renseignements personnels.

III. Les consommateurs et les outils de protection de la vie privée

Les experts en matière de protection de la vie privée et les responsables des services en ligne affirment qu'il existe des outils de protection de la vie privée qui sont facilement accessibles; pourtant, les consommateurs semblent avoir l'impression de n'avoir ni le choix ni le contrôle en ce qui a trait au suivi et à la communication de leurs renseignements personnels, ou bien que les outils de protection de la vie privée actuels ne sont pas nécessairement utiles. Pourquoi est-ce le cas?

3.1 Outils de protection de la vie privée existants et lois applicables

Selon les entreprises en ligne et les chercheurs universitaires consultés aux fins du présent rapport, les consommateurs ont déjà accès à un grand nombre d'outils et de pratiques de protection de la vie privée.

Ces outils et pratiques de protection de la vie privée sont en grande partie fondés sur ce qu'on appelait au départ les « principes relatifs aux pratiques équitables de traitement de l'information » (FIPP). Ces principes ont d'abord été proposés dans un rapport publié en 1973 par le comité consultatif sur les systèmes de données personnelles automatisés du secrétaire du département de la Santé de l'Éducation et des Affaires sociales des États-Unis, qui examinait l'incidence de l'informatisation de l'information sur la confidentialité des renseignements personnels des citoyens²⁷. Les principes proposés par le comité étaient les suivants :

- ∂ Il ne doit y avoir aucun système de conservation des dossiers contenant des données personnelles dont l'existence même est secrète.
- ∂ Il doit exister un moyen pour les gens de découvrir quels renseignements à leur sujet se trouvent dans un dossier et comment ils sont utilisés.
- ∂ Les gens doivent avoir le moyen d'empêcher que les renseignements à leur sujet qui ont été obtenus à une fin soient utilisés ou rendus accessibles à d'autres fins sans leur consentement.
- ∂ Il doit y avoir un moyen pour les gens de corriger ou de modifier un dossier contenant des renseignements nominatifs à leur sujet.
- ∂ Toute organisation qui crée, conserve, utilise ou diffuse des dossiers de données personnelles nominatives doit veiller à la fiabilité des données pour leur

²⁷ Département de la Santé, de l'Éducation et des Affaires sociales des États-Unis, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, Washington D.C. : Department of Health, Education, and Welfare, 1973.

utilisation prévue et doit prendre des précautions afin de prévenir le mésusage des données²⁸.

Par la suite, les FIPP ont été enchâssés dans la *Privacy Act of 1974*²⁹ des États-Unis et modifiés de manière à inclure un grand nombre des principes aujourd'hui bien reconnus, comme les suivants : la notification de chaque utilisateur et la transparence; l'accès des personnes à leurs dossiers et la modification par ces personnes de leur dossier; la réduction minimum de la quantité de données et la limitation de leur utilisation; la responsabilité et l'application de la loi; et la sécurité³⁰.

Les FIPP sont devenus le fondement de lois sur la protection des renseignements personnels (ou « protection des données ») de partout dans le monde.

Les organisations offrant des produits ou des services aux résidents de l'Union européenne (UE) sont visées par la *directive sur la protection des données*³¹ de l'UE et seront régies par le nouveau *règlement général concernant la protection des données*³², dès le mois de mai 2018.

Au Canada, la collecte, l'utilisation et la divulgation de renseignements personnels par des organisations privées sont régies à l'échelon fédéral par la *Loi sur la protection des renseignements personnels et les documents électroniques*³³ (LPRPDE). Les provinces de l'Alberta, de la Colombie-Britannique et du Québec ont également adopté des lois provinciales relativement à la protection de la vie privée, lesquelles ont été jugées très semblables à la LPRPDE³⁴. Dans le secteur des services de santé, la protection des renseignements personnels est également régie par certaines lois provinciales. Les principes de protection de la vie privée enchâssés dans ces lois sont généralement semblables aux FIPP établis aux États-Unis. Autrement dit, la LPRPDE prévoit qu'une

²⁸ *Ibid.*, p. 41.

²⁹ *The Privacy Act of 1974*, 5 U.S.C. § 552a.

³⁰ *Ibid.* Voir aussi : Electronic Privacy Information Center, « The Privacy Act of 1974 », en ligne : EPIC, <<https://epic.org/privacy/1974act/>>, consulté le 22 février 2017; Rubinstein, Ira S. et Nathaniel Good, « Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents », 2013, 28:2 Berkeley Tech. L.J. 1333, p. 1343.

³¹ Directive 95/46/CE du Parlement européen et du conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

³² Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

³³ *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, chap. 5. [LPRPDE].

³⁴ Voir : *Personal Information Protection Act*, S.A. 2003, chap. P-6.5;

Personal Information Protection Act, S.B.C. 2003, chap. 63; et

Loi sur la protection des renseignements personnels dans le secteur privé, C.Q.L.R. chap. P-39.1.

personne doit savoir et donner son consentement — le terme « consentement » signifie que la personne comprend la nature, le but et les conséquences de l'activité — pour que ses renseignements personnels puissent être recueillis, utilisés ou divulgués, et que la collecte de renseignements personnels doit être limitée aux renseignements qui sont nécessaires aux fins établies par l'organisation³⁵. La LPRPDE établit également des principes concernant les éléments suivants :

- l'établissement des fins pour lesquelles les renseignements personnels sont recueillis;
- les situations où un consentement explicite ou implicite est requis;
- la conservation et la suppression des données;
- l'accès par une personne à ses renseignements personnels;
- la transparence au sujet des politiques et des pratiques relatives à la collecte et au traitement des données;
- les mesures de sécurité.

Certaines organisations intègrent maintenant les FIPP dans la conception et le fonctionnement de leurs services plates-formes, au moyen de ce qu'on appelle maintenant les « technologies d'amélioration de la confidentialité » (TAC), qui constituent la base d'un aspect de la protection de la vie privée dès la conception. Les TAC et la protection de la vie privée dès la conception ne sont toutefois pas identiques, comme l'a signalé Rubinstein. Cet auteur a écrit ce qui suit :

[Traduction]

Même si les TAC et la protection de la vie privée dès la conception ne font pas toujours l'objet d'une définition précise et que ces deux idées se chevauchent même du point de vue de leur utilisation, elles ne sont pas identiques. Ce qui les distingue pourrait être résumé ainsi : les TAC sont des applications ou des outils aux buts distincts qui touchent une seule dimension de la protection de la vie privée, comme l'anonymat, la confidentialité ou le contrôle sur les renseignements personnels. Souvent, les TAC sont ajoutées aux systèmes existants; il s'agit parfois d'une réflexion après coup des concepteurs et parfois d'utilisateurs finaux sensibles à la protection de la vie privée. Au contraire, la protection de la vie privée dès la conception est non pas une technologie ou un produit particulier, mais une approche systématique pour la conception de toute technologie qui intègre la protection de la vie privée dans les spécifications ou l'architecture sous-jacentes³⁶.

³⁵ LPRPDE, art. 6.1 et annexe 1, art. 4.3 et 4.4.

³⁶ Rubinstein, Ira S., « Regulating Privacy by Design », 2011, 26, *Berkeley Tech. L.J.*, 1409, p. 1411-1412.

Par conséquent, aujourd’hui, les consommateurs ont accès à un certain nombre d’outils de protection de la vie privée. Le type d’outil de protection de la vie privée le plus courant est la « politique de confidentialité » (ou « politique de protection des données »), qui explique aux utilisateurs du site d’une entreprise ses pratiques de l’entreprise en matière de protection des renseignements personnels – y compris pourquoi l’organisation recueille des renseignements personnels, comment elle utilisera les données et pendant combien de temps elle les stockera. La plupart des grands sites Web commerciaux et des applications ont une politique de confidentialité. Même si le Commissariat à la protection de la vie privée du Canada (CPVP) fournit des lignes directrices sur la façon de créer des politiques de protection de la vie privée plus transparentes et efficaces³⁷, ces politiques tendent à varier considérablement du point de vue de la longueur, de la complexité, du libellé, de l’intelligibilité et d’autres facteurs. Le CDIP examinera les points de vue et les réactions des consommateurs à l’égard des politiques de protection de la vie privée plus tard dans la présente section.

Cependant, un éventail d’autres outils de protection de la vie privée sont également accessibles au public. De nombreux navigateurs Internet, comme Firefox, offrent maintenant des modes de navigation privée ou « incognito »; il existe des moteurs de recherche privée, comme DuckDuckGo, Hulbee et StartPage, qui ne suivent pas les utilisateurs, et le nombre d’applications comme les bloqueurs de publicité s’accroît également.

Ann Cavoukian, directrice générale du Privacy and Big Data Institute de l’Université Ryerson, a affirmé lors d’une entrevue que le nombre d’outils de protection de la vie privée accessibles a augmenté de façon importante, surtout à l’ère « post Edward Snowden ». Elle croyait que les gens étaient peut-être en train de perdre espoir au sujet de la possibilité de protéger leurs renseignements personnels, mais que [traduction] « des mesures de contrôle extrêmement élevées sur les renseignements personnels » sont à la disposition des consommateurs, notamment le cryptage et les paramètres de confidentialité. Natasha Tusikov était aussi d’avis qu’il existe maintenant de nombreux outils de protection de la vie privée « post Snowden », y compris certains qui sont faciles à utiliser (p. ex. les réseaux virtuels privés) et d’autres qui sont plus difficiles (p. ex. le cryptage).

Des organisations — plus particulièrement des multinationales à grand volume de données — ont également élaboré leurs propres outils de protection de la vie privée à

³⁷ Voir : Commissariat à la protection de la vie privée du Canada, *Dix conseils pour améliorer votre politique de confidentialité en ligne et la transparence de vos pratiques en matière de protection de la vie privée*, 2013, en ligne : CPVPC, <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/politiques-de-confidentialite/02_05_d_56_tips2/>.

l'intention des utilisateurs. Aux fins du présent rapport, des représentants de Google Canada et de Facebook Canada ont communiqué leur point de vue sur les options de confidentialité qu'ils offrent à leurs utilisateurs. Facebook a renvoyé le CDIP à ses commentaires sur la consultation du CPVP concernant le consentement au titre de la LPRPDE³⁸, dans lesquels les auteurs ont écrit ce qui suit :

[Traduction]

Nous avons investi abondamment dans le but d'offrir de nouvelles formes de transparence et de contrôle qui sont conçues pour habiliter les gens qui utilisent Facebook, tout en leur procurant l'expérience rapide et fluide qu'ils attendent de notre service. Notre approche par rapport à la protection de la vie privée allie : 1) des produits précisément conçus pour informer les gens au sujet des pratiques relatives aux données; 2) des fonctions intégrées dans les produits qui permettent aux gens de comprendre et de déterminer la façon dont leurs renseignements sont utilisés et communiqués; et 3) une expérience contextuelle dans le produit, qui sensibilise continuellement les gens et leur rappelle les façons dont nous utilisons leurs renseignements afin d'alimenter nos services.

Voici certains des outils que Facebook met à la disposition de ses utilisateurs :

- *Principes de base liés à la confidentialité* : Guide interactif qui répond à la plupart des questions fréquemment posées au sujet des mesures de contrôle de la confidentialité de Facebook.
- *Assistance confidentialité* : Outil qui donne aux utilisateurs un aperçu général des personnes qui peuvent voir leurs publications et leurs activités.
- *Préférences publicitaires* : Outil qui informe les utilisateurs au sujet des annonces qu'ils voient et qui leur permet de retirer des « centres d'intérêt » ou les annonces publicitaires d'un annonceur particulier.

Colin McKay, chef des politiques publiques et des relations avec le gouvernement à Google Canada, a affirmé qu'il croyait que les utilisateurs du Web ont maintenant l'impression de ne pas avoir de contrôle, car Internet n'offre plus l'« obscurité pratique » qu'il accordait autrefois aux actes publics. À son avis, les personnes ont encore le choix d'effectuer ou non un acte public, mais cet acte a maintenant une durée de vie plus longue. Par conséquent, Google se concentre sur le fait de fournir à ses

³⁸ Facebook, *Consentement et protection de la vie privée : Commentaires de Facebook sur le document de discussion du Commissariat à la protection de la vie privée du Canada*, 2016, en ligne : CPVP, <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultation-sur-le-consentement-en-vertu-de-la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques/memoires-recus-dans-le-cadre-de-la-consultation-sur-le-consentement-en-vertu-de-la-lprpde/sub_consent_32/>.

utilisateurs des outils de contrôle par l'utilisateur et de protection des renseignements personnels. Ces types d'outils comprennent les suivants :

- *Paramètres de l'historique du compte* : outil qui permet aux utilisateurs de gérer les types de renseignements qu'ils communiquent à Google, y compris leur emplacement, les renseignements sur leur appareil, les recherches effectuées sur Google et leur activité de visionnement sur YouTube.
- *Google Takeout* : outil de portabilité des données qui permet aux utilisateurs d'exporter leurs renseignements de produits ou services de base de Google lorsqu'ils décident de cesser d'utiliser le produit ou le service en question.
- *Gestionnaire de compte inactif* : outil qui permet aux utilisateurs de gérer les données une fois que leur compte devient inactif. Parmi les options, mentionnons le fait d'amener Google à supprimer leurs données après une période d'inactivité de 3 à 12 mois ou de permettre à des « contacts de confiance » de recevoir des données provenant de services particuliers, comme Google Drive ou Gmail.

Google et Facebook permettent tous deux aux utilisateurs de modifier les paramètres de confidentialité de chaque jeu et application.

Le CPVP publie également des conseils et des lignes directrices visant à aider les Canadiens à protéger leurs renseignements personnels. En consultation avec le CDIP aux fins du présent rapport, le CPVP a affirmé que son site Web comportait maintenant une page « Pour les individus » contenant de l'information sur les lois relatives à la protection de la vie privée au Canada, les droits de la protection des renseignements personnels des consommateurs et la protection de renseignements personnels clés, comme les numéros de permis de conduire ou d'assurance sociale. Le site Web du CPVP comprend également diverses pages d'information telles que « Protection de la vie privée en ligne », « Vol d'identité » et « Appareils numériques », et le Commissariat a récemment publié une série d'articles de blogues sur la confidentialité en ligne.

Par conséquent, un certain nombre d'outils et de lignes directrices pour la protection de la vie privée sont accessibles pour les utilisateurs d'Internet.

3.2 Utilisation des outils de protection de la vie privée par les consommateurs

Pourtant, malgré la vaste accessibilité de divers outils de protection de la vie privée, les consommateurs sont tout de même préoccupés au sujet de leur confidentialité et

semblent ne pas être disposés à tirer pleinement profit de ces outils et options ou être incapables de le faire. Pourquoi est-ce le cas?

Solove fait valoir que les responsables des politiques relatives à la protection de la vie privée et les organismes de réglementation ne peuvent pas compter uniquement sur l'« autogestion de la confidentialité », c'est-à-dire la création d'un ensemble de droits, qui, au bout du compte, donne à la personne de prendre toutes les décisions au sujet de la façon de gérer ses données. Pour décrire la façon dont l'autogestion de la confidentialité a évolué et s'est transformée en lois et en pratiques relatives à la protection de la vie privée, Solove écrit ce qui suit :

[Traduction]

L'autogestion de la confidentialité trouve refuge dans le consentement. Elle tente d'être neutre quant à la substance — quant au fait que certaines formes de collecte, d'utilisation ou de divulgation de données personnelles sont bonnes ou mauvaises — et se concentre plutôt sur le fait que les gens consentent ou non aux diverses pratiques relatives à la protection de la vie privée. Le consentement rend légitimes presque toutes les formes de collecte, d'utilisation ou de divulgation de données personnelles³⁹.

Solove fait valoir que l'autogestion de la confidentialité est encore un élément crucial de la réglementation de la protection des renseignements personnels, mais qu'elle ne permet pas aux gens d'exercer un [traduction] « contrôle important sur leurs données », et ce, pour plusieurs raisons⁴⁰.

Le premier problème est d'ordre cognitif : la recherche en sciences sociales montre que les personnes ont de la difficulté à faire des [traduction] « choix éclairés et rationnels au sujet des coûts et des avantages liés au fait de consentir à la collecte, à l'utilisation et à la divulgation de leurs données personnelles⁴¹ ». Dans le cas de celles qui se donnent la peine de lire les énoncés de confidentialité, elles sont nombreuses à avoir des présomptions fausses ou inexactes au sujet de la façon dont leurs données sont utilisées, ou ont de la difficulté à appliquer ce qu'elles savent à des situations complexes concernant la confidentialité. Par exemple, les gens tendent à considérer les dangers qu'ils connaissent bien comme étant plus risqués que ceux qu'ils ne connaissent pas

³⁹ Solove, Daniel J., « Introduction: Privacy Self-Management and the Consent Dilemma », 2013, 126, *Harvard L. Rev.*, 1880, p. 1880.

⁴⁰ *Ibid.*

⁴¹ *Ibid.*, p. 1880-1881.

bien⁴². De plus, les personnes ont tendance à établir leurs préférences en matière de confidentialité dans un contexte plutôt que dans l'abstrait⁴³.

Le deuxième problème est d'ordre structurel : même lorsque les gens sont pleinement informés et qu'ils agissent rationnellement, des problèmes structurels se posent, comme l'échelle. Même si un utilisateur était en mesure de personnaliser tous ses paramètres de confidentialité pour un service, les services, produits et applications qu'une personne doit gérer par elle-même sont bien trop nombreux⁴⁴. Comme les sites Web communiquent également des renseignements à des tierces parties, l'agrégation constitue un autre problème structurel : les utilisateurs ne peuvent pas toujours contrôler ou gérer la façon dont chaque élément de donnée qu'ils ont fourni séparément à diverses entreprises pourrait être combiné et analysé⁴⁵.

Le troisième problème présenté par Solove est celui de l'évaluation des préjudices. Même s'il est possible pour un utilisateur d'évaluer les coûts et les avantages liés au fait de consentir à la collecte, à l'utilisation et à la divulgation de données à un certain moment, il serait extrêmement difficile pour cet utilisateur de prévoir les préjudices qui pourraient en découler cumulativement au fil du temps⁴⁶. Dans le même ordre d'idées, même si l'autogestion de la confidentialité est axée sur les choix faits et le contrôle exercé par une personne, elle ne tient pas compte des vastes conséquences sociales et culturelles de chacune des décisions relatives à la protection de la vie privée⁴⁷. Par conséquent, le fait de compter uniquement sur l'autogestion de la confidentialité, plus particulièrement par la notion de consentement éclairé, constitue probablement une solution inadéquate pour s'assurer que les renseignements personnels des utilisateurs sont protégés et que les consommateurs le savent et le ressentent.

Sauf dans le cas de grands sites Web de réseautage social sophistiqués, qui offrent habituellement aux utilisateurs des paramètres de confidentialité plus détaillés, et de certains appareils, comme les téléphones intelligents qui permettent aux utilisateurs de personnaliser certains paramètres de confidentialité pour chaque application, la majeure partie des sites Web commerciaux et des applications comptent sur des pratiques informatives en ce qui concerne la protection de la vie privée, notamment des énoncés ou des politiques de confidentialité.

⁴² *Ibid.*, p. 1886-1887.

⁴³ *Ibid.*

⁴⁴ *Ibid.*, p. 1888.

⁴⁵ *Ibid.*, p. 1889.

⁴⁶ *Ibid.*, p. 1891 et 1893.

⁴⁷ *Ibid.*, p. 1892.

« C'est facile d'avoir accès à l'information, mais est-ce que c'est un langage qui se prête à tout le monde? Non, j'ai une formation en droit... Je ne sais pas, même avec une formation en droit... Je ne sais pas, ce n'est pas évident tout le temps non plus. »

« Les énoncés apparaissent, et je passe tout simplement à autre chose. Je n'ai pas le temps. Si vous allez chez Tim Hortons et que vous recevez une tasse de... allez-vous rester là...? Qui lit ces énoncés? Mon café est rendu froid; j'ai terminé, exactement. Maintenant, que vais-je faire? »

« [La politique de confidentialité de] Facebook. Tout d'abord, elle est extrêmement difficile à trouver sur la nouvelle mise en page, et elle change toujours. Alors, c'est une chose. Ensuite, elle est très longue. C'est presque comme si on ne vous donnait pas l'information que vous recherchez. On vous donne les renseignements de base, qu'il est évident que vous connaissez déjà, et vous voulez savoir, mais j'ai l'impression qu'il y en a toujours plus... »

– Participants aux groupes de discussion du CDIP

Toutefois, des recherches de plus en plus nombreuses montrent que les politiques de confidentialité sont en grande partie inefficaces, incompréhensibles et inaccessibles pour les utilisateurs. Par exemple, Bruening et Culnan concluent que, lorsque des avis de confidentialité (comme des énoncés ou des politiques de confidentialité) sont présentés, leur [traduction] « utilité [est] limitée » – autrement dit, ils ne sont pas rédigés d'une manière qui les rend utiles pour les personnes⁴⁸. Cette utilité limitée est créée par un certain nombre de facteurs, y compris la difficulté à trouver l'avis de confidentialité; d'importants problèmes de lisibilité; et l'interminable longueur du texte et le volume de renseignements qui n'appuient pas nécessairement la capacité limitée d'une personne de traiter l'information⁴⁹. Bruening et Culnan concluent également que les gens obtiennent moins de choix, ou des choix moins importants, relativement au traitement des données, sans égard à l'accessibilité d'avis de confidentialité⁵⁰. Par exemple, les utilisateurs pourraient n'avoir la permission de renoncer qu'à certaines pratiques seulement, ou bien devoir consentir à *toutes* les activités de traitement des données menées par une organisation.

Une comparaison et évaluation par Reidenberg et coll. de la capacité de trois groupes d'utilisateurs — des experts en matière de protection de la vie privée, des diplômés en droit et en politique publique et des utilisateurs

d'Internet typiques — de comprendre et d'interpréter les politiques d'entreprises a

⁴⁸ Bruening, Paula J. et Mary J. Culnan, « Through a Glass Darkly: From Privacy Notices to Effective Transparency », 17:4 *North Carolina J.L. & Tech.*, 515, p. 542.

⁴⁹ *Ibid.*, p. 543-545.

⁵⁰ *Ibid.*, p. 546-547.

révélé certaines caractéristiques communes, mais aussi des lacunes importantes au chapitre de l'interprétation des énoncés de confidentialité, plus particulièrement en ce qui a trait à la communication des données⁵¹. Ces lacunes sont ressorties à l'intérieur des groupes (surtout chez les experts en matière de protection de la vie privée) et entre les experts et les deux autres groupes. Voici la conclusion de Reidenberg et coll. :

[Traduction]

[L]es désaccords entre les experts et le désaccord entre les experts et les autres groupes reflètent le fait que le libellé ambigu des politiques de confidentialité typique mine la capacité de ces politiques de communiquer efficacement au grand public un avis concernant les pratiques relatives aux données. Par conséquent, les résultats de cette recherche auront d'importantes conséquences sur les politiques du point de vue de la construction de l'avis et du cadre choisi et sur le recours à cette approche par les États-Unis⁵².

Borgesius écrit ce qui suit :

[Traduction]

En somme, l'économie comportementale montre que la protection de la vie privée au moyen de l'instrument du consentement éclairé pose de nombreux problèmes. Il ne s'agit que d'une légère exagération que d'affirmer que les gens ne lisent pas les politiques de confidentialité; s'ils les lisaient, ils ne les comprendraient pas; s'ils les comprenaient, ils n'agiraient pas. De plus, si tous leurs concurrents exploitent la symétrie de l'information et les partis pris des gens, les entreprises doivent faire la même chose pour rester en affaires⁵³.

Selon un sondage mené en 2015 auprès de résidents de l'UE, seulement 2 répondants sur 10 étaient [traduction] « toujours informés au sujet de la collecte des données et de la façon dont elles sont utilisées », et seulement 18 % avaient pleinement lu les énoncés de confidentialité⁵⁴. Appelés à expliquer pourquoi ils n'avaient pas lu les énoncés de confidentialité, 67 % ont affirmé que ces énoncés étaient trop longs à lire; 38 % ont dit qu'ils n'étaient pas clairs ou qu'ils étaient trop difficiles à comprendre; et 15 % ont

⁵¹ Joel R. Reidenberg et coll., « Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding », 2015, 30:1, *Berkeley Tech. L.J.*, 39, p. 40.

⁵² *Ibid.*

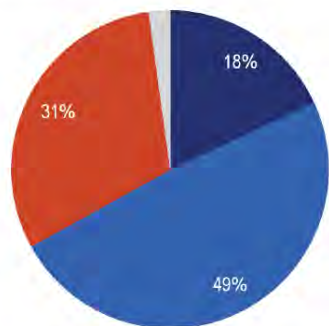
⁵³ Borgesius, Frederik Zuiderveen, « Informed Consent: We Can Do Better to Defend Privacy », 2015, en ligne : IVIR.nl <<http://www.ivir.nl/publicaties/download/1795>>, p. 7-8.

⁵⁴ Direction générale de la justice et des consommateurs de la Commission européenne, *Special Eurobarometer 431: Data Protection Report*, 2015, en ligne : Europa.eu, <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf>, p. 81 et 84.

affirmé qu'ils pensaient que les sites Web ne respecteraient pas l'énoncé de confidentialité de toute manière⁵⁵.

Figure 3-1. Attitudes des consommateurs de l'UE à l'égard des énoncés de confidentialité

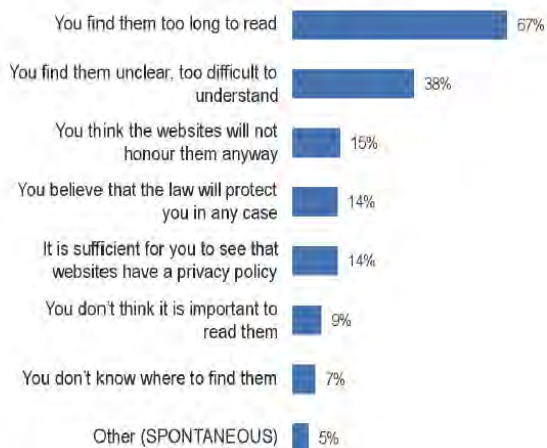
QB14. Thinking about privacy statements on the Internet, which of the following sentences best describes what you usually do?



- You read them fully
- You read them partially
- You do not read them at all
- Don't know

EU28

QB15. What are the reasons why you usually do not read or read only partially the privacy statements? (MULTIPLE ANSWERS POSSIBLE)



Don't know | 1%

EU28

Source : Commission européenne, 2015

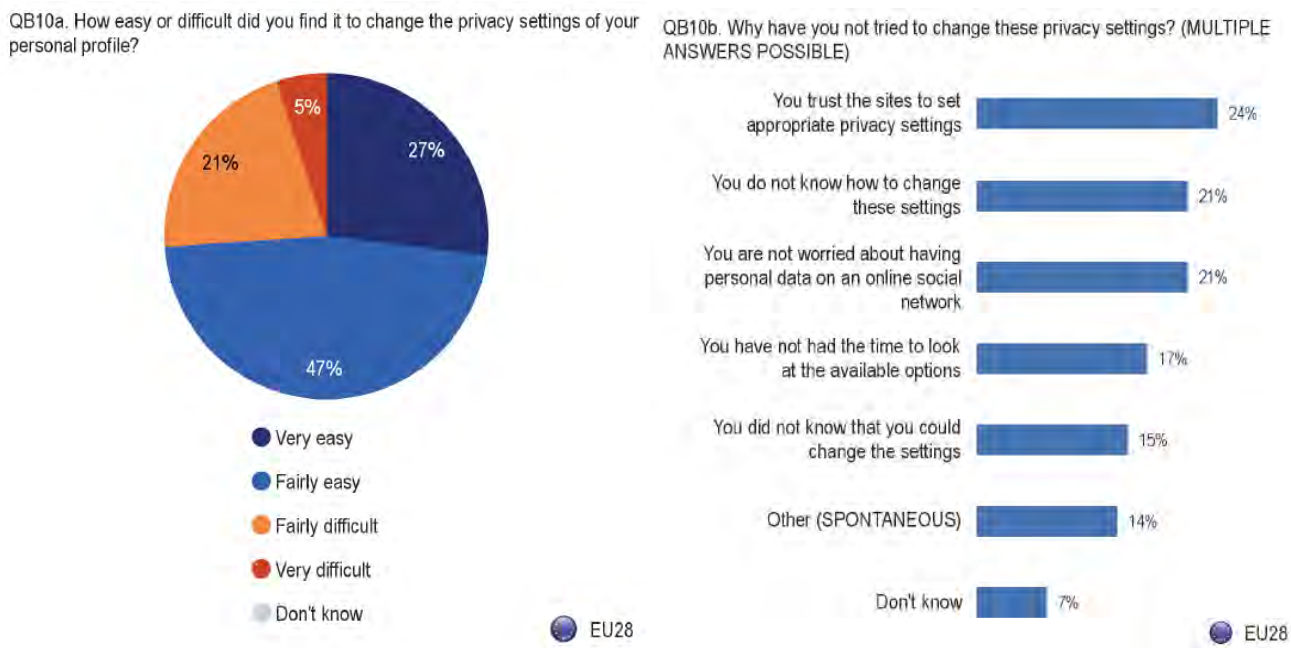
Ann Cavoukian était d'avis que, même si le nombre d'outils de protection de la vie privée s'accroît, le problème tient au fait qu'actuellement, [traduction] « l'option par défaut n'est pas la confidentialité ». Il y a beaucoup de [traduction] « jargon juridique lié à la protection des renseignements personnels », et les paramètres de confidentialité pourraient ne pas être faciles à trouver; les consommateurs veulent que les outils de protection de la vie privée soient faciles à trouver et à comprendre. Michelle D'Souza et Dana Ayotte, chercheuses à l'Inclusive Design Research Centre de l'Université de l'ÉADO, ont formulé des commentaires semblables. Elles avaient généralement l'impression que les gens ne se donnaient pas la peine de lire les politiques de confidentialité, qui étaient souvent prolixes et mêlantes, et qu'ils n'avaient peut-être pas le temps de chercher les outils de protection de la vie privée existants. Par exemple, même si D'Souza et Ayotte pensaient que les options offertes par *Mon activité* de Google étaient sophistiquées et impressionnantes, il n'était pas nécessairement facile de trouver l'outil, c'est-à-dire que les utilisateurs étaient peu susceptibles de tomber dessus. Les chercheuses ont également constaté que les outils de protection de la vie

⁵⁵ *Ibid.*, p. 87.

privée n'étaient pas tous conviviaux ou explicites — certains possédaient des paramètres par défaut ouverts —, ce qui rendait difficile pour les utilisateurs de déterminer dans quelle mesure leurs données allaient être exposées.

Selon le sondage de l'UE, même si 57 % des répondants ont affirmé qu'ils avaient tenté de modifier leurs paramètres de confidentialité sur un réseau social en ligne, 42 % ont également affirmé ne pas l'avoir fait⁵⁶. De ceux qui avaient tenté de modifier leurs paramètres, 47 % ont trouvé que c'était [traduction] « assez facile », et 27 %, que c'était « très facile », alors qu'environ 1 répondant sur 4 a trouvé que c'était « assez difficile » ou « très difficile »⁵⁷. Ceux qui n'ont pas tenté de modifier les paramètres de confidentialité par défaut ont donné un certain nombre de raisons pour ne pas l'avoir fait, notamment qu'ils se fiaient aux sites Web pour régler les paramètres par défaut appropriés; de ne pas savoir comment modifier les paramètres; ou de ne pas avoir le temps d'étudier les options offertes⁵⁸.

Figure 3-2. Les consommateurs de l'UE et les paramètres de confidentialité des réseaux sociaux



Source : Commission européenne, 2015

⁵⁶ Direction générale de la justice et des consommateurs de la Commission européenne, *Special Eurobarometer 431: Data Protection Report*, 2015, en ligne : Europa.eu, <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf>, p. 91.

⁵⁷ *Ibid.*, p. 94.

⁵⁸ *Ibid.*, p. 96.

Un grand nombre des participants aux groupes de discussion du CDIP connaissaient les paramètres de confidentialité de services particuliers, comme Facebook, et les avaient personnalisés afin de changer les publics qui pouvaient ou ne pouvaient pas voir leur activité sur les médias sociaux. Certains participants connaissaient également d'autres outils de protection de la vie privée, comme les modes de navigation privée. Toutefois, la plupart des participants trouvaient que les outils de protection de la vie privée étaient difficiles à comprendre ou à utiliser. Très peu comprenaient les politiques de confidentialité des sites Web ou avaient même tenté de les lire, et certains se sont dits frustrés par le rythme auquel les politiques changeaient. Ils trouvaient que les politiques et paramètres de confidentialité étaient souvent modifiés par les entreprises sans qu'ils le sachent et que les paramètres étaient différents de ceux qu'ils avaient réglés auparavant. Certains participants ont également souligné le volume des sites Web et des applications qu'ils visitaient, affirmant qu'il était pratiquement impossible de gérer les paramètres de confidentialité de chaque site Web ou de se tenir à jour par rapport à ceux-ci. De plus, certains participants, qui avaient tenté d'utiliser la navigation privée ou des bloqueurs de publicité se sont plaints du fait que ces outils désactivaient certaines fonctions des applications ou des sites Web ou nuisaient à ces fonctions et que certains sites Web ne fonctionnaient pas du tout.

« Les entreprises devraient raccourcir leurs énoncés de confidentialité. » « Plus courts et plus faciles à lire. » « Une version simplifiée des politiques. » « Oui, des termes courants dont toute personne pourrait vraiment comprendre la signification de ce à l'égard de quoi on donne son consentement. »

« Personnellement, mon expérience de Facebook et de la modification des paramètres de confidentialité est... en plus du fait qu'il y a constamment des problèmes techniques, que Facebook change constamment les paramètres de ce qu'on peut et ne peut pas faire sur son réseau. Il m'est tout à fait impossible de suivre le rythme. À ce jour, en ce moment, je ne sais pas quel est l'état de mon compte Facebook, du point de vue de qui peut voir quoi et de ce qui va où. J'ai tenu des conversations que je pensais se dérouler entre une personne et une autre, puis d'autres personnes se sont mises à commenter les propos que j'avais tenus. Il s'agissait d'une conversation privée, ou, du moins, je le pensais. »

« Vous pouvez télécharger sur votre ordinateur un logiciel qui élimine tout le suivi, les témoins et les choses... Toutefois, j'estime qu'ils ruinent tout simplement toute l'expérience d'utilisation d'Internet. Bien des sites Web cessent de fonctionner adéquatement. »

– Participants aux groupes de discussion du CDIP

IV. Vers la création d'une « case relative à la vie privée »

Le principal objectif de cette étude était d'examiner les points de vue des consommateurs sur la création d'une « case relative à la vie privée » notionnelle qui pourrait s'appliquer sur toutes les plateformes, dans tous les navigateurs et toutes les applications. Cette case relative à la vie privée présenterait un ensemble normalisé de paramètres personnalisés de protection de la vie privée et permettrait aux utilisateurs d'avoir accès à des renseignements normalisés concernant la vie privée, ce qui s'appliquerait à tous les sites Web consultés et à toutes les applications utilisées. Cette idée d'une case relative à la vie privée universelle a été examinée avec les groupes de réflexion créés en vue de la production de ce rapport de même qu'avec les universitaires et les intervenants du secteur de la réglementation et de l'industrie.

4.1 Principes de protection intégrée de la vie privée

La protection intégrée de la vie privée découle du point de vue voulant que l'ingénierie de la sécurité des données seule ne permet pas de relever entièrement le défi que pose la protection de la vie privée des personnes. En 2002, dans le cadre d'une étude sur les répercussions sur la vie privée des systèmes de gestion des droits numériques, Feigenbaum *et coll.* ont écrit ce qui suit :

La distribution par internet de contenus de marketing de masse fournit d'excellentes occasions aux producteurs, aux distributeurs et aux consommateurs, mais elle peut constituer une menace importante pour la vie privée des utilisateurs. Certaines des voies menant à la perte de la vie privée sont très familières (p. ex. l'extraction des données de cartes de crédit), mais d'autres sont nouvelles ou beaucoup plus graves qu'elles ne l'étaient dans les régimes de distribution antérieurs [...] les technologies de protection de la vie privée (p. ex. cryptage, anonymat et utilisation de pseudonymes) qui captent la majeure partie de l'attention de la communauté de recherche et développement en sécurité ne peuvent pas à elles seules régler les problèmes liés à la protection de la vie privée soulevés par la gestion des droits numériques, même si elles peuvent jouer un rôle dans diverses solutions⁵⁹.

⁵⁹ Joan Feigenbaum et coll., « Privacy Engineering for Digital Rights Management Systems », dans Tomas Sander, éd., *Revised Papers from the ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management* 79 (2002), en ligne : Université Yale <<http://www.cs.yale.edu/homes/jf/FFSS.pdf>> à p. 1.

Feigenbaum *et coll.* ont soutenu que certaines solutions de protection de la vie privée axées sur la sécurité, comme la cryptographie, sont insuffisantes pour diverses raisons, notamment :

- La cryptographie n'est pas nécessairement appropriée pour la distribution commerciale, où ce ne sont pas toutes les parties qui sont clairement bonnes ou mauvaises, et il peut y avoir des fins légitimes et des sources de confiance.
- La cryptographie n'est pas nécessairement facile à utiliser ou conviviale et pourrait ralentir des dispositifs plus petits.
- Il y avait aussi une difficulté liée à l'intégration des solutions de protection de la vie privée aux anciens systèmes, qui ne tenaient pas compte de la protection de la vie privée des utilisateurs au moment de la conception⁶⁰.

La protection intégrée de la vie privée est difficile, car les valeurs en matière de protection de la vie privée peuvent changer et sont souvent influencées par le contexte. Irwin Altman, par exemple, a soutenu que les personnes exprimaient leurs valeurs en matière de protection de la vie privée en étant plus ou moins accessibles (ou ouverts) au moyen d'un éventail de mécanismes comportementaux comme le ton, la création d'un espace personnel et la posture⁶¹. D'après lui, les outils de protection de la vie privée devraient permettre aux personnes de réguler les limites dans différentes interactions. Helen Nissenbaum percevait les flux d'information comme étant déjà influencés par le contexte au quotidien. Autrement dit, ce que les personnes partageaient avec leur médecin était différent de ce qu'elles partageaient avec leur époux ou un représentant du service à la clientèle dans un magasin – les personnes comprennent et appliquent naturellement les normes sociales appropriées à chaque contexte⁶². Elle a laissé entendre que les solutions de protection de la vie privée devraient permettre aux utilisateurs de divulguer différents types de renseignements selon le contexte.

D'autres chercheurs ont élaboré et précisé des principes de protection intégrée de la vie privée et des lignes directrices d'ingénierie. Ann Cavoukian, par exemple, établit sept « principes de base » de protection intégrée de la vie privée qui sont maintenant intégrés au cadre de certification de la protection intégrée de la vie privée de l'Université Deloitte-Ryerson⁶³. Il s'agit des principes suivants :

⁶⁰ *Ibid.* à p. 7-9.

⁶¹ Ira S. Rubinstein et Nathaniel Good. « Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents » (2013) 28:2 Berkeley Tech. L.J. 1333 à p. 1369-70.

⁶² *Ibid.* à p. 1372.

⁶³ Voir : Deloitte, *Protection intégrée de la vie privée : Nouvelle norme de certification de protection de la vie privée* (2015), en ligne : Deloitte

1. Prendre des mesures proactives et non réactives, des mesures préventives et non correctives.
2. Assurer la protection implicite de la vie privée. La personne n'a aucune mesure à prendre pour protéger sa vie privée – la protection est intégrée au système, par défaut.
3. Intégrer la protection de la vie privée dans la conception.
4. Assurer une fonctionnalité intégrale (selon un paradigme à somme positive et non à somme nulle). Chercher à tenir compte de tous les objectifs et intérêts légitimes de façon positive et gagnante pour toutes les parties. La protection intégrée de la vie privée évite les prétentions concernant de fausses dichotomies, comme la protection de la vie privée par rapport à la sécurité.
5. Assurer la sécurité de bout en bout.
6. Assurer la visibilité et la transparence.
7. Respecter la vie privée des utilisateurs. Il faut que les architectes et les opérateurs protègent les intérêts de la personne en offrant des mesures comme de solides paramètres par défaut de protection de la vie privée, des avis appropriés et l'habilitation de solutions conviviales⁶⁴.

D'autres principes et approches de protection intégrée de la vie privée ont aussi été examinés. Tant Spiekermann et Cranor que Rubinstein et Good ont séparé la protection intégrée de la vie privée en différentes approches selon le type de solution de protection de la vie privée.

Rubinstein et Good analysent la protection intégrée de la vie privée de deux points de vue : (1) l'ingénierie de protection de la vie privée, « la conception et la mise en œuvre d'un logiciel qui favorise la protection de la vie privée »; et (2) une protection intégrée de la vie privée facile à utiliser, ce qui permet de garantir que « les utilisateurs comprennent les contrôles bien conçus de protection de la vie privée et en bénéficient »⁶⁵.

Spiekermann et Cranor présentent deux approches d'ingénierie tenant compte de la vie privée :

<<https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-fr-ers-privacy-by-design-brochure.PDF>>.

⁶⁴ Ann Cavoukian, *Privacy by Design* (2013), en ligne : Commissaire à l'information et à la protection de la vie privée de l'Ontario <<https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf>> à p. 2-3.

⁶⁵ Ira S. Rubinstein et Nathaniel Good. « Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents » (2013) 28:2 Berkeley Tech. L.J. 1333 à p. 1342.

- la « protection de la vie privée au moyen de politiques » met l'accent sur les principes « de notification et de choix » relatifs aux pratiques équitables concernant l'information;
- la « protection de la vie privée intégrée à l'architecture » vise principalement à « réduire au minimum la collecte de renseignements personnels permettant d'identifier la personne et préconise le maintien de l'anonymat de même que le stockage et le traitement des données du côté du client »⁶⁶.

Spiekermann et Cranor favorisent les approches de protection de la vie privée intégrée à l'architecture, qui fournissent généralement « aux utilisateurs des niveaux plus élevés de protection de la vie privée de façon plus fiable et sans qu'il soit nécessaire pour eux d'analyser ou de négocier des politiques relatives à la vie privée »⁶⁷ et mettent l'accent en particulier sur la « possibilité de réunir des renseignements personnels pour créer un profil complet et identifiable, ce qui est la clé pour déterminer le degré de vie privée dont une personne bénéficie »⁶⁸. Par conséquent, Spiekermann et Cranor pressent les concepteurs de systèmes de protection de la vie privée de se concentrer sur la prévention de l'établissement de liens (ou identifiabilité) entre un pseudonyme et une personne.

Lederer *et coll.* ont aussi publié « cinq pièges »⁶⁹ pour les concepteurs de systèmes tenant compte de la vie privée, notamment :

- Cacher le flux d'information potentiel : Les organisations devraient indiquer clairement la nature et l'étendue des possibilités de divulgation.
- Cacher le flux d'information réel : Les organisations devraient indiquer clairement la divulgation réelle de renseignements par le système, notamment quels renseignements sont communiqués à qui. Lederer *et coll.* citent l'utilisation des témoins comme exemple.
- Mettre l'accent sur la configuration plutôt que sur les mesures prises : Les systèmes ne devraient pas avoir besoin d'une « configuration excessive » pour protéger la vie privée et devraient plutôt permettre aux utilisateurs de gérer leur vie privée de façon semi-intuitive. Par exemple, la configuration des préférences liées à la vie privée constitue souvent une difficulté pour les utilisateurs, qui doivent prévoir leurs besoins et qui définissent parfois, au bout du compte, des préférences qui ne s'appliquent pas à des situations précises.

⁶⁶ Sarah Spiekermann et Lorrie Faith Cranor, « Engineering Privacy » (2009) 35:1 *IEEE Transactions on Software Engineering* 67.

⁶⁷ *Ibid.* à p. 79.

⁶⁸ *Ibid.* à p. 75. (Italique ajouté.)

⁶⁹ Scott Lederer et coll., *Personal Privacy through Understanding and Action: Five Pitfalls for Designers* (2004), en ligne : Berkeley <<https://www2.eecs.berkeley.edu/bears/2004/STARS/lederer-personal.pdf>>.

- Ne pas inclure de contrôles très généraux :

Les conceptions devraient offrir un mécanisme évident d'échelon élevé pour interrompre et reprendre la divulgation de renseignements personnels. Souvent, un bouton de mise en marche ou de sortie fera l'affaire. Les utilisateurs sont habitués à arrêter quelque chose quand ils veulent mettre fin à son fonctionnement. L'interruption du flux d'information est un comportement instinctif qui a une incidence sur la vie privée des personnes⁷⁰.

- Bloquer les pratiques établies : Par exemple, les personnes peuvent faire intentionnellement des divulgations ambiguës de renseignements fondées sur des pratiques sociales. Les conceptions ne devraient pas empêcher les divulgations ambiguës. Par exemple, actuellement, le suivi de l'emplacement permet seulement aux utilisateurs de divulguer un endroit précis ou rien du tout.

Même s'il existe divers principes et approches de protection intégrée de la vie privée, peu d'études ont examiné le point de vue des consommateurs sur une initiative ou un concept particulier de protection intégrée de la vie privée. Les sections suivantes exposeront les réactions des consommateurs et des intervenants face au concept d'une case relative à la vie privée.

4.2 Attitudes des consommateurs à l'égard d'une case relative à la vie privée

On a présenté aux participants au groupe de réflexion l'idée d'une « case relative à la vie privée » qui s'appliquerait à tous les sites Web ou à toutes les applications et qui permettrait aux utilisateurs en ligne de personnaliser leurs paramètres de protection de la vie privée ou de consulter des types précis d'information liés à leur vie privée. On a demandé à des groupes de réflexion s'ils seraient intéressés par la case relative à la vie privée et s'ils pouvaient donner plus de

« C'est un peu comme si vous aviez déjà laissé le cheval sortir de l'écurie ou quelque chose du genre. Mais je pense qu'il devrait y avoir quelque chose à cet égard pour qu'il y ait une solution possible pour les gens. Vous devriez avoir la possibilité de choisir si vous voulez [partager de l'information] ou pas. Je sais que c'est comme un couteau à double tranchant en ce qui concerne les raisons pour lesquelles on obtient [un service] gratuitement, mais je pense qu'on devrait avoir cette possibilité. C'est peut-être une loi, mais je pense aussi qu'il devrait y avoir une certaine responsabilité, parce qu'on ne sait pas qui obtient ces choses. »

– Participant au groupe de réflexion du Centre pour la défense de l'intérêt public (CDIP)

⁷⁰ Ibid. à p. 7.

détails sur les caractéristiques précises de la case, sur les plans fonctionnel et esthétique.

« Je l'adopterais. Je serais heureux. Vous savez, c'est un peu comme quand on fait attention à sa santé, mais que le vaccin nous aide à combattre la grippe. C'est peut-être comme un vaccin, comme un petit extra. »

« Personnellement, je me porte bien. C'est tout ce que je peux vous dire. Mais je comprends qu'il y a peut-être quelque chose. Peut-être pas aujourd'hui, mais dans l'avenir, il y a peut-être quelque chose que je voudrai garder privé, et je devrais avoir le choix. »

« Moi je pense que ça devrait être légiféré surtout si on a la possibilité de choisir ou de ne pas choisir de partager l'information parce qu'à ce moment-là il va y avoir un avantage, et ceux qui veulent vraiment être "in the public eye" et puis publique, ils partageront leur information. Tu sais c'est un choix que chacun fait, mais tu sais à ce moment-là ça devient notre choix. »

« Je pense que ce serait un désavantage de mettre ça, de donner l'option au client, de donner une "false hope"... Absolument, si je clique ça, je crois que c'est sécuritaire ça sera pas partagé — "yeah right". Ça va jamais arriver, c'est impossible. »

– Participants au groupe de réflexion du CDIP

En général, les participants au groupe de réflexion étaient réceptifs à l'idée d'un guichet unique pour les renseignements et les paramètres par défaut de protection de la vie privée. Selon eux, la case relative à la vie privée serait un outil utile et informatif. Plus particulièrement, les participants ont insisté sur l'importance du besoin et sur le droit de choisir le moment pour partager leur information et déterminer la façon dont cette information est utilisée ou communiquée à d'autres parties.

Certains participants étaient sceptiques quant à l'efficacité d'une case relative à la vie privée. Même s'ils pensaient que cela pourrait être utile, ils étaient convaincus que les organisations privées trouveraient une autre façon de la contourner pour recueillir les renseignements personnels des utilisateurs et en tirer profit. Ils croyaient qu'il y avait trop d'argent en jeu. Certains ont aussi indiqué qu'il pourrait y avoir une difficulté liée à la conformité; comme l'internet est mondial, ils n'étaient pas convaincus qu'une loi canadienne pourrait obliger tous les sites Web et toutes les applications à respecter une case relative à la vie privée.

Les participants comprenaient généralement qu'ils ont actuellement accès à des services gratuits en échange de la publicité (ciblée ou non) et que le fait d'empêcher un site Web ou une application de les suivre pourrait avoir une incidence sur le prix de ce service. Bien que nombre de participants croyaient que les consommateurs préfèrent, au bout du compte, que les services demeurent gratuits, ils croyaient aussi que les utilisateurs devraient avoir le choix.

À la question de savoir si les entreprises devraient offrir la possibilité d'un abonnement à un service en échange d'une entente de ne pas recueillir les renseignements de l'utilisateur ni en faire le suivi, nombre de participants étaient sceptiques face à cette idée. Ils croyaient que peu de consommateurs choisiraient cette solution et renonceraient à un service gratuit. Certains participants avaient aussi des doutes quant au fait de savoir si les entreprises respecteraient cette entente. Toutefois, d'autres participants pensaient qu'un abonnement serait une solution plus honnête et transparente.

Tous les participants ont dit que la case relative à la vie privée devrait s'appliquer par défaut à tous les sites Web et, idéalement, sur les diverses plateformes (téléphone portable, tablette, navigateurs internet) aussi. Ils estimaient aussi, toutefois, que les utilisateurs recherchent l'efficacité et le côté pratique et qu'ils devraient avoir la possibilité de renoncer à la case relative à la vie privée s'ils le souhaitent. Nombre de participants ont aussi laissé entendre que la case devrait être accompagnée de campagnes d'éducation publique qui permettraient de s'assurer que les consommateurs comprennent la portée de la case.

« Je trouve qu'il doit y avoir une transparence, des restrictions et puis c'est comme n'importe quoi, je vais donner comme exemple l'alcool, ça existe depuis des années... je veux dire c'est légiféré d'une certaine façon, jusqu'à un certain point. Quelque chose comme ça devrait être légiférée. Puis c'est facile de dire, ah ça on va jamais pouvoir contrôler la situation, mais c'est certain qu'on sera pas capable si on essaie pas. »

« L'idée, comme disait cet homme, est que parfois on souffre de quelque chose, que c'est privé et qu'on essaie d'obtenir de l'information. Nous allons tous sur l'internet, nous tenons cela pour acquis chaque jour, mais je crois qu'on y pensera un peu plus quand cette fenêtre contextuelle apparaîtra. »

« Ce qui se passe avec la vie privée, c'est que nous devrions aussi avoir le choix de ce que nous devrions... comme vous l'avez dit, de savoir où nos renseignements vont, surtout s'ils vont servir à faire de l'argent sur notre dos ou je ne sais pas quoi. Nous devrions aussi surveiller ce que nous voulons, les renseignements que nous voulons leur donner. »

« Je pense que ça serait bien. Je ne sais pas s'il y aurait des règles différentes pour des personnes différentes, comme les associations mutuelles sans but lucratif par rapport aux entreprises qui recueillent des renseignements. Il faudra peut-être les définir un peu différemment, mais définitivement de façon plus directe. »

« Je pense que c'est une bonne chose. Cela donne le choix aux gens, en présumant que le bouton fonctionne. Ce n'est pas comme si... c'est là, mais ça ne fonctionne pas vraiment. »

« Cette case relative à la vie privée devrait avoir une bonne réputation. Elle doit avoir existé... il faudrait qu'elle existe depuis un bon moment. » « Il faudrait que les gens y croient, non? » « Oui, il faudrait y croire. » « Si vous n'y croyez pas, vous allez simplement sauter cette case. »

« C'est peut-être une mesure qui est dans le bon sens des choses, je veux dire l'autre option c'est statu quo et puis clairement ça marche pas. Bon, je veux dire, peut-être que ça viendrait rassurer la population qui voudrait un peu plus de contrôle sur, ou un peu plus d'information. Mais un peu au point de vue de [un autre participant] je dirais qu'il y a simplement trop d'argent impliqué. »

– Participants au groupe de réflexion du CDIP

4.3 Adhésion des intervenants et des services

L'une des préoccupations entourant l'idée d'une case relative à la vie privée est la mesure dans laquelle les consommateurs et les décideurs peuvent s'attendre à une adhésion suffisante des fournisseurs et des intervenants de l'industrie. Cette

préoccupation a déjà été soulevée par des chercheurs qui s'intéressent à la protection intégrée de la vie privée.

Spiekermann et Cranor ont écrit ce qui suit :

Aujourd'hui, l'approche de politique de protection de la vie privée a été adoptée par de nombreuses entreprises parce qu'elle n'interfère pas avec les modèles d'affaires actuels qui s'appuient sur une utilisation importante des renseignements personnels. En l'absence de restrictions imposées par une loi sur l'utilisation des données personnelles, l'approche de politique de protection de la vie privée se fie aux entreprises pour fournir des renseignements accessibles et des choix significatifs en matière de protection de la vie privée pour que les utilisateurs puissent faire affaire avec les entreprises qui répondent à leurs attentes concernant la vie privée. Cependant, comme Kang le fait remarquer : « Pour de nombreuses raisons, comme les coûts des transactions, les personnes et les responsables de la collecte de renseignements ne négocient et ne concluent généralement pas des contrats exprès avant d'entreprendre chaque transaction réalisée dans le cyberspace. Toute proposition de solution fondée sur le marché qui ne tient pas compte de cette réalité économique est déficiente. »⁷¹

Rubinstein et Good ont écrit ce qui suit :

[N]ous croyons que la principale difficulté liée à la protection intégrée efficace de la vie privée n'est pas l'absence de lignes directrices sur la conception. C'est plutôt le fait que les préoccupations des entreprises sont souvent en compétition avec les préoccupations liées à la vie privée et leur font de l'ombre [...] Alors, qu'est-ce qui se passe ici? Nous croyons que Google (comme nombre de ses pairs) a une compréhension flexible des exigences liées à la protection de la vie privée qui s'adapte bien à ses propres intérêts commerciaux. Nous croyons que les cinq incidents liés à la vie privée que nous avons examinés dans la section III.A démontrent que la politique organisationnelle de Google lui permet de trouver un équilibre entre les exigences liées à la vie privée et ses objectifs commerciaux essentiels [*sic*] comme l'augmentation de ses revenus provenant de la publicité. De plus, ce processus d'équilibre est presque complètement caché aux observateurs externes. [...] Comme les exigences des entreprises et de protection de la vie privée sont souvent contradictoires, une réglementation claire serait profitable pour les entreprises. Sans des lignes directrices bien définies sur ce que cela signifie que de mettre en œuvre une protection intégrée de la vie privée, les considérations commerciales l'emporteront toujours sur la protection de la vie privée : les champions internes de la protection de la vie

⁷¹ Sarah Spiekermann et Lorrie Faith Cranor, « Engineering Privacy » (2009) 35:1 *IEEE Transactions on Software Engineering* 67, à p. 79.

privée ne pèseront jamais assez lourd pour gagner les luttes serrées. Au contraire, si les organismes de réglementation élaboraient une norme concernant le caractère raisonnable de protection de la vie privée intégrée aux produits et services, les entreprises sauraient ce qu'on attend d'elles et prendraient plus au sérieux les exigences liées à la conception au moment de trouver un équilibre approprié⁷².

Pendant la préparation du présent rapport, le CDIP a consulté divers intervenants sur la case relative à la vie privée et la réception par l'industrie d'une telle initiative. Même si certains, comme le Commissariat à la protection de la vie privée du Canada (CPVP), n'étaient pas en mesure de commenter l'initiative à ce moment-là, la case relative à la vie privée a fait l'objet de discussions importantes entre d'autres intervenants.

En général, les chercheurs qui s'intéressent à la protection de la vie privée ont soutenu l'idée d'une case relative à la vie privée, mais étaient moins certains par rapport à son adoption éventuelle par les fournisseurs et services en ligne.

Ann Cavoukian, directrice administrative du Privacy and Big Data Institute de l'Université Ryerson, croyait que la case relative à la vie privée serait une excellente idée, mais qu'il faudrait aussi éduquer le public pour que les utilisateurs sachent où la trouver et comment l'utiliser. En ce qui concerne les caractéristiques de la case, Cavoukian a dit qu'elle devrait être simple et directe, et que des limites et spécifications des objectifs d'utilisation des données seraient essentielles. Même si Cavoukian ne s'opposait pas à une intervention réglementaire pour promouvoir ou exiger la case relative à la vie privée, elle a proposé que l'on commence par utiliser la case relative à la vie privée au niveau des entreprises comme façon de gagner la confiance des consommateurs et de s'assurer leur loyauté. Le problème potentiel avec une exigence réglementaire est que les entreprises ont tendance à la considérer comme une obligation négative et voudront peut-être mettre en œuvre le minimum seulement, au lieu de la voir comme quelque chose de positif pour elles et qui pourrait leur donner un avantage concurrentiel.

Natasha Tusikov, professeure adjointe à l'Université York, a également soutenu l'idée d'une case relative à la vie privée et a fait remarquer que toute initiative résumant des documents légaux complexes sur la protection de la vie privée serait un pas en avant. Madame Tusikov a aussi convenu que la case devrait inclure un langage simple et direct, et elle était particulièrement préoccupée par la communication de données à des tiers. Elle croyait que dans de nombreux cas, les consommateurs ne savaient pas qui étaient ces tiers et comment les renseignements des utilisateurs étaient communiqués ou

⁷² Ira S. Rubinstein et Nathaniel Good, « Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents » (2013) 28:2 Berkeley Tech. L.J. 1333 à p. 1333, 1409 et 1411.

utilisés. Madame Tusikov était préoccupée par la mesure dans laquelle l'industrie était prête à adopter la case relative à la vie privée. Elle croyait que les entreprises ont tendance à aimer la flexibilité et que même si les entreprises du secteur technique défendent certains éléments de protection intégrée de la vie privée, elles sont aussi extrêmement préoccupées par les revenus de publicité, surtout quand elles ne chargent aucun frais pour un service. Elle préconise un rôle important du gouvernement et des organismes de réglementation dans la protection intégrée de la vie privée, et se disait préoccupée par l'idée de donner trop de contrôle à l'industrie dans ce domaine. Elle a mentionné que les gouvernements assurent déjà une importante surveillance réglementaire d'autres problèmes jugés importants, comme les enfants et l'alcool. Par conséquent, s'ils soutiennent, par exemple, que les enfants ne devraient pas être exposés à certains niveaux de publicité, ils pourraient imposer des exigences réglementaires plus importantes.

L'Inclusive Design Research Centre de l'École d'art et de design de l'Ontario entreprend aussi un projet sur la faisabilité de la protection intégrée de la vie privée qui cherche à concevoir une interface qui permettrait aux utilisateurs individuels de définir leurs propres préférences et accords en matière de vie privée et de les appliquer aux produits et services en ligne⁷³. Le projet met surtout l'accent sur la protection des utilisateurs vulnérables, comme les « personnes handicapées, les personnes vieillissantes et d'autres personnes victimes de discrimination, de stéréotypes, de marginalisation ou d'exclusion ». Michelle D'Souza et Dana Ayotte ont laissé entendre que le produit ou l'interface pourrait être repris par de plus petits joueurs de l'industrie d'abord, mais devrait finir par être applicable de façon universelle. Elles ont senti qu'il serait difficile d'obtenir l'adhésion initiale du fournisseur, mais elles espéraient que plus on pourrait mettre de connaissances dans les mains des utilisateurs, plus les utilisateurs pourraient mettre de pression sur les fournisseurs. Au bout du compte, l'adoption de la case relative à la vie privée ou d'autres outils de protection de la vie privée serait probablement le résultat d'une approche de politique à plusieurs volets, y compris des lois et des règlements, une validation de principe et l'éducation.

Rubinstein écrit ce qui suit :

L'acceptation par les fonctionnaires responsables de la protection de la vie privée des technologies d'amélioration de la confidentialité et de la protection

⁷³ École d'art et de design de l'Ontario, *Comprendre, connaître et affirmer les préférences personnelles en matière de protection de la vie privée : Étude de faisabilité*, en ligne : CPVP <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/financement-pour-les-projets-de-recherche-et-d-application-des-connaissances/cp_bg/>. Pour de plus amples renseignements, voir aussi : <[https://wiki.fluidproject.org/display/fluid/\(Floe\)+Privacy+Needs+and+Preferences](https://wiki.fluidproject.org/display/fluid/(Floe)+Privacy+Needs+and+Preferences)>.

intégrée de la vie privée offre des possibilités excitantes et des difficultés importantes. Même si les entreprises pourraient améliorer leurs pratiques de gestion des données en adoptant des technologies d'amélioration de la confidentialité appropriées ou en intégrant la protection de la vie privée à la conception de nouveaux produits ou services, elles sont peu susceptibles de profiter de l'initiative tant que les incitatifs économiques demeurent inadéquats et que le sens de la protection intégrée de la vie privée ou des technologies d'amélioration de la confidentialité demeure inexact. Face à une faible demande des consommateurs, le manque de données pertinentes pour entreprendre des analyses coûts-avantages, les coûts de renonciation élevés de toute restriction volontaire de la collecte et de l'analyse de données personnelles de valeur et la perte de réputation ne sont souvent pas assez convaincants pour susciter de nouveaux investissements dans la protection de la vie privée, ce qui fait que des incitatifs réglementaires sont requis⁷⁴.

Certains des intervenants de l'industrie interrogés pendant la préparation du présent rapport insistaient sur le besoin de flexibilité plutôt que d'une approche unique pour tous. Ils ont aussi mentionné que la taille, la sophistication et les modèles d'affaire des entreprises en ligne varient considérablement.

Colin McKay, chef de la politique d'intérêt public et des relations gouvernementales à Google Canada, a dit qu'un cadre fondé sur des principes crée un environnement où une entreprise peut innover avec des produits et services, alors qu'un modèle plus prescriptif – comme des paramètres présélectionnés de protection de la vie privée – rendrait l'innovation plus difficile parce que les utilisateurs ont tendance à être plus prudents. Il croyait qu'il serait aussi plus difficile pour les jeunes entreprises de surmonter les « paramètres créés par les institutions ». Monsieur McKay estimait qu'il pourrait être utile d'élaborer des directives ou un code de conduite sur les types de permissions auxquels les utilisateurs s'attendent, mais que des paramètres préétablis pourraient avoir une incidence négative sur les avantages à long terme d'une nouvelle technologie ou plateforme. Il a aussi insisté sur le fait que la majeure partie des services en ligne dépendent des revenus de la publicité et que la publicité ciblée est devenue efficace et extrêmement utile pour les annonceurs. Monsieur McKay a fait remarquer qu'en fin de compte, Google veut être transparent auprès de ses utilisateurs sur la façon dont leurs renseignements sont recueillis et utilisés et veut leur offrir des solutions possibles concernant cette collecte et cette utilisation. Il a signalé que Google a travaillé très dur pendant la dernière année pour faire en sorte que ses paramètres de protection de la vie privée soient accessibles pour ses utilisateurs.

⁷⁴ Ira S. Rubinstein, « Regulating Privacy by Design » (2011) 26 Berkeley Tech. L.J. 1409 à p. 1453.

Facebook a renvoyé le CDIP à ses commentaires dans la consultation du CPVP de 2016 concernant le consentement prévu par la LPRPDE, où il a écrit ce qui suit :

Nombre des questions et préoccupations peuvent être gérées grâce à l'utilisation d'approches de consentement amélioré qui se concentrent sur des façons novatrices et conviviales de présenter les pratiques de gestion de l'information d'une organisation et de fournir aux utilisateurs des renseignements clairs concernant leurs choix en matière de collecte et d'utilisation de leurs données de même que les façons de faire ces choix. [...] Nous croyons qu'un modèle de protection de la vie privée qui est flexible et qui reconnaît un éventail d'approches de consentement qui sont appropriées dans le contexte dans lequel les données sont utilisées est encore la meilleure approche pour habilitier les gens à faire des choix à propos de leurs renseignements et constitue une base appropriée pour un cadre législatif⁷⁵.

Jason McLinton, vice-président, Division alimentaire et Affaires réglementaires du Conseil canadien du commerce de détail (CCCD), a signalé que le CCCD représente 45 000 comptoirs de services dont le thème commun est le commerce de détail et que chaque membre aurait probablement une capacité et une approche différentes concernant la protection de la vie privée en ligne. Il croyait que pendant que nombre de commerces de détail ont adopté des politiques de protection de la vie privée, d'autres peuvent suivre des protocoles pour protéger les renseignements au lieu d'avoir des politiques officielles – ce qui représente un éventail d'approches sous l'égide du CCCD. En ce qui concerne l'idée d'une case relative à la vie privée ou d'une approche normalisée de protection de la vie privée, Monsieur McLinton trouve l'idée intéressante et croit que le niveau d'intérêt varierait probablement d'un membre à l'autre. La plupart des membres du CCCD ont pu, par exemple, s'adapter à la *Loi canadienne anti-pourriel*, surtout avec les lignes directrices et l'aide du CCCD et du Conseil de la radiodiffusion et des télécommunications canadiennes.

⁷⁵ Facebook, *Consentement et protection de la vie privée : Commentaires de Facebook sur le document de discussion du Commissariat à la protection de la vie privée du Canada* (2016), en ligne : CPVP <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-the-personal-information-protection-and-electronic-documents-act/submissions-received-for-the-consultation-on-consent/sub_consent_32/>.

Différents intervenants de l'industrie semblent avoir des approches différentes de protection de la vie privée des utilisateurs en ligne. Certains semblent soutenir la flexibilité d'élaborer leurs propres initiatives de protection intégrée de la vie privée tandis que d'autres pourraient apprécier des directives plus précises et une approche plus

« À propos de la case, peut-être que vous pourriez indiquer "J'ai des enfants", ce qui signifie que vous êtes encore plus responsable de vous assurer que tout ce que vous envoyez à ce ménage est vraiment... » « Oui, une option d'ordinateur partagé peut-être. »

« Qu'en est-il de la question de savoir si vous leur donnez la permission de recueillir vos données et de les communiquer à des tiers? » « Oui. Je pense que c'est la question la plus importante, parce qu'à ce moment-là, vous ne savez pas qui sont ces tiers [...] si ce sont les sites Web eux-mêmes, vous vous dites qu'il n'y a pas de problème. »

« Comme je disais avant, vous voulez voir ce qu'ils ne vous disent pas. Donc, évidemment, un grand nombre de sites Web prennent vos renseignements et les communiquent à on ne sait qui. Mais qui sont-ils et que font-ils avec ces renseignements? Je pense que cela est plus informatif. »

– Participants au groupe de réflexion du CDIP

normalisée. En général, il semble que les entreprises en ligne plus grandes et sophistiquées préfèrent se concentrer sur l'élaboration de leurs propres approches de notification et de contrôle en matière de vie privée, tandis que les plus petites entreprises pourraient bénéficier d'une norme approuvée ou établie pour l'information et les paramètres de protection de la vie privée.

4.4 Caractéristiques de la case relative à la vie privée

Cette section examine les caractéristiques d'une case relative à la vie privée qui seraient les plus importantes pour les consommateurs et les intervenants interrogés dans le cadre du présent rapport.

4.4.1 Qu'est-ce que la case relative à la vie privée devrait inclure?

Les participants au groupe de réflexion et les chercheurs universitaires croyaient que la case relative à la vie privée pourrait jouer un rôle essentiel quand vient le temps de fournir aux utilisateurs certains paramètres de protection de la vie privée et des éléments clés d'information sur la protection de la vie privée. Plus particulièrement, les groupes de réflexion et les chercheurs semblaient préoccupés principalement par :

1. l'interdiction de recueillir des données de localisation;
2. l'interdiction de la communication de données à des tiers et de la combinaison de données par des tiers;

3. l'accès à l'information concernant la façon dont les données recueillies sont utilisées, notamment l'identification des tiers;
4. l'accès à l'information sur les éléments de données récemment recueillis auprès d'une personne (organisée par l'entreprise qui l'a recueillie).

Certains participants ont aussi proposé de fournir une option d'ordinateur partagé ou un autre outil qui pourrait indiquer la présence d'enfants utilisateurs sur un ordinateur ou un appareil.

Paramètres de protection de la vie privée : Collecte de renseignements à caractère délicat et communication des renseignements à des tiers

Un certain nombre de participants au groupe de réflexion s'attendaient à ce que les sites Web ou applications qu'ils utilisent fassent un suivi des données ou les recueillent, y compris leur activité de navigation, auprès d'eux. Cependant, il y avait deux domaines notables où les consommateurs ont exprimé le désir d'un meilleur contrôle.

Les participants au groupe de réflexion étaient presque tous d'accord pour dire que certains renseignements personnels, comme les renseignements sur la santé, l'emploi, l'orientation sexuelle et la religion, sont plus délicats et ne devraient faire l'objet d'aucun suivi ni collecte. Les participants étaient aussi extrêmement préoccupés par la **localisation** et ne voulaient pas que personne soit au courant de leurs déplacements ou voyages.

Un sondage commandé par le CDIP dans son rapport de 2015, *Déconnecté du réseau?*, a révélé que 82 % des Canadiens pensaient qu'il était *très important* qu'on demande leur permission avant qu'une application, un commerce de détail ou un fournisseur de services de télécommunications en ligne puisse commencer à les localiser⁷⁶. De plus, 93 % des Canadiens pensaient que les entreprises qui commencent à suivre les déplacements d'une personne avant d'obtenir sa permission devraient être pénalisées ou sanctionnées d'une façon ou d'une autre⁷⁷.

Par conséquent, le CDIP recommande que la case relative à la vie privée permette aux consommateurs d'interdire la collecte de leurs données de localisation. Même si les paramètres de la case relative à la vie privée pourraient se concentrer sur les données de localisation en particulier, ils pourraient aussi établir un lien avec des options plus détaillées qui permettraient aux utilisateurs d'autoriser ou d'interdire plus spécialement

⁷⁶ Geoff White, *Déconnecté du réseau? Repérage des technologies basées sur la localisation et la Loi* (Ottawa : CDIP, 2015), en ligne : CDIP <http://www.CDIP.ca/wp-content/uploads/2015/09/OCA-2014-15-Off-the-Grid-Location-based-technologies-and-the-law-Final-Report_FR.pdf>, Annexe A, Figure 10.

⁷⁷ *Ibid.*, Figure 11.

le suivi d'autres catégories de données. Le paramètre par défaut devrait toutefois être de ne recueillir aucun renseignement à caractère délicat comme l'emplacement.

❖ La case relative à la vie privée devrait permettre aux consommateurs d'interdire le suivi de leur emplacement. Elle pourrait aussi donner aux consommateurs l'occasion de préciser davantage les types de renseignements dont ils n'autorisent pas la collecte ni le suivi.

Le deuxième domaine de préoccupation des consommateurs était la communication des données recueillies à des tiers. Les participants au groupe de réflexion soupçonnaient que leurs activités faisaient l'objet d'un suivi, mais avaient très peu de connaissances sur la façon dont ces données étaient utilisées ou à qui elles étaient communiquées. Nombre de participants se sont dits surpris et étaient clairement mal à l'aise quand ils ont appris que 90 % des sites Web populaires communiquaient les données des utilisateurs à des parties externes – parties qui étaient essentiellement inconnues des consommateurs. En outre, la grande majorité de ces données sont reçues par une poignée d'entreprises américaines. Les participants au groupe de réflexion étaient donc d'avis que la case relative à la vie privée devait se concentrer surtout sur l'idée de permettre aux consommateurs d'interdire la communication des données recueillies auprès d'eux à des tiers (autrement dit, les parties à l'extérieur du site Web ou de l'application original consulté ou utilisée).

❖ La case relative à la vie privée devrait permettre aux consommateurs d'interdire la communication à des tiers des données recueillies.

Information sur la vie privée : Communication à des tiers et profils individuels

La case relative à la vie privée offre aussi une occasion de communiquer aux consommateurs des éléments clés d'information sur la vie privée au moyen de liens vers des renseignements supplémentaires.

Les chercheurs universitaires en particulier ont laissé entendre que la case relative à la vie privée pourrait être utilisée pour communiquer plus efficacement la façon dont les données sont utilisées et à qui elles ont été communiquées. Natasha Tusikov a signalé qu'on en sait encore très peu sur les tiers qui reçoivent les données des utilisateurs de même que sur l'endroit où les données sont traitées ou transférées. Elle était aussi d'avis que parfois, les entreprises semblaient intentionnellement vagues à ce sujet, même si cette information est très importante pour les consommateurs.

« Je pense que ce serait vraiment incroyable si l'on pouvait, d'une façon ou d'une autre, mettre un genre de [...] être cérébral ou je ne sais quoi et juste être en mesure de voir la quantité de nos renseignements qui sont vraiment en circulation. Si on avait vraiment une idée de cela, du volume d'information qui est réellement en circulation.... »

« Je pense que c'est bon à savoir, surtout si les entreprises font de l'argent grâce à nos renseignements à tous. Nous devrions avoir le choix de voir l'information et d'être avertis de ce qui est recueilli et des sites Web qui recueillent ou non nos renseignements. »

– Participants au groupe de réflexion du CDIP

La case relative à la vie privée pourrait dissiper ces préoccupations en fournissant un résumé clair des noms et des types de tiers qui pourraient recevoir des renseignements (p. ex. annonceurs, organismes du gouvernement, enquêteurs en ligne, compagnies d'assurance, etc.) et l'endroit où ils se trouvent, de même que la façon dont les données recueillies pourraient être utilisées (p. ex. publicité ciblée, développement de logiciels pour l'internet, etc.) La case pourrait aussi inclure des liens vers des pages Web qui pourraient fournir de plus amples renseignements. Ces pages Web pourraient contenir des renseignements supplémentaires sur une entreprise, un site Web ou un tiers en particulier (p. ex. nommer des tiers précis auxquels une entreprise comme Facebook communique des renseignements).

❖ La case relative à la

vie privée devrait fournir des résumés définissant clairement : (a) les tiers auxquels les données des utilisateurs sont communiquées et l'endroit où ils se trouvent; et (b) la façon précise dont les données sont utilisées.

Certains participants au groupe de réflexion, en particulier les plus jeunes, ont aussi dit qu'ils souhaiteraient connaître les données exactes qui sont recueillies auprès d'eux. Cela pourrait inclure des renseignements recueillis récemment auprès d'eux, toutes les données dont une entreprise dispose sur eux ou ce à quoi ressemble leur profil de données. D'autres participants préféraient ne pas savoir ou pensaient qu'il pourrait être dangereux de consulter les renseignements recueillis auprès d'eux. Actuellement, la LPRPDE permet aux utilisateurs individuels de demander l'accès aux renseignements qu'une organisation a recueillis auprès d'eux et entreposés⁷⁸. Cependant, ce processus

⁷⁸ Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, chap. 5, Annexe 1, article 4.9.

est onéreux et limité aux organisations individuelles; tout rapport qui en découle pourrait ne pas donner à l'utilisateur une vision complète de la façon dont les divers ensembles de données peuvent être analysés ou combinés pour créer un profil.

La capacité d'être informé des renseignements recueillis récemment auprès d'un utilisateur pourrait être utile et informative. La case relative à la vie privée devrait fournir une façon pour les utilisateurs de consulter les données recueillies récemment auprès d'eux par une organisation. Afin de protéger la confidentialité d'un utilisateur, une option pourrait être fournie pour effacer ce registre, un peu comme on efface les témoins au moment de la fermeture d'une session de navigation. Cela exigerait de nouveaux changements administratifs et techniques pour les organisations; toutefois, l'accès des utilisateurs à ces données pourrait aussi améliorer grandement la transparence et la confiance envers les organisations en ligne.

❖ La case relative à la vie privée devrait permettre aux utilisateurs d'avoir accès aux données recueillies récemment auprès d'eux par l'organisation.

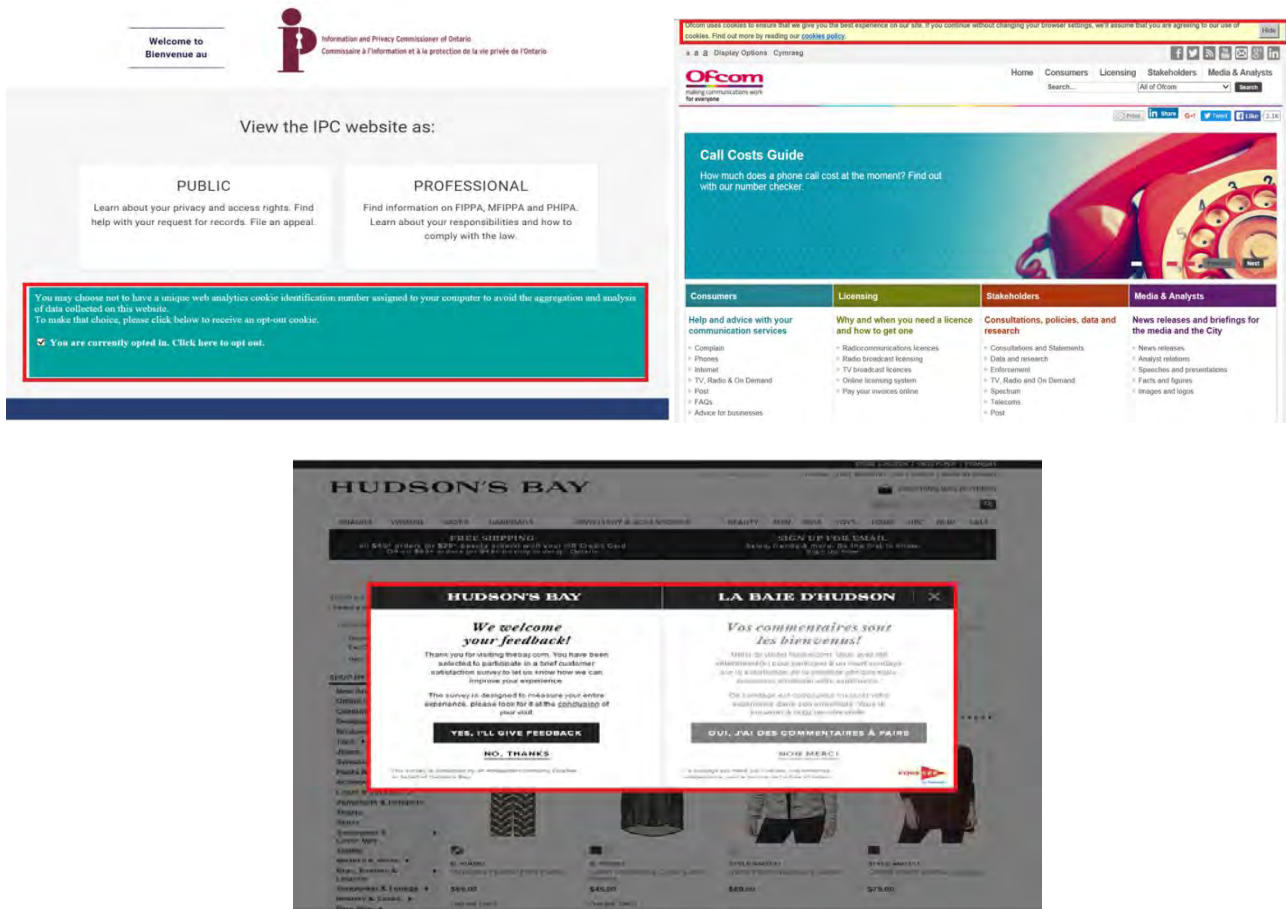
4.4.2 À quoi devrait ressembler la case relative à la protection des renseignements personnels?

Les participants au groupe de réflexion du CDIP ont également eu l'occasion de décrire comment devrait s'afficher de manière à être le plus utile possible pour les internautes. Cela comprend demander aux participants de décrire la case et de dessiner son agencement idéal et d'offrir une rétroaction sur des exemples existants de fenêtres de dialogue ou d'autres outils de notification.

La fenêtre de protection de la vie privée doit être évidente et facile d'accès, et non dissimulée

Les participants aux groupes de réflexion étaient presque unanimement d'accord que toute protection intégrée des renseignements personnels devrait être évidente et facile à accéder, non cachée ou dissimulée dans le coin d'une page Web. Il a été demandé aux participants de commenter trois exemples de fenêtres de notification (illustrées ci-après).

Figure 4-1. Échantillons de fenêtres de notification



Tous les participants qui se sont prononcés ont préféré l'exemple de dialogue de la Baie d'Hudson, comparativement à une barre de défilement intégrée au contenu de la page Web. Certains participants se sont plaints de la petite taille de la police des deux autres exemples d'Ofcom et du commissaire à la protection des renseignements personnels de l'Ontario. Ils estimaient important que la fenêtre relative à la protection de la vie privée figure dans un espace évident et exige une intervention avant d'autoriser l'utilisateur à accéder à une page Web ou à une application.

Il est intéressant de constater que nombre de participants ont comparé les fenêtres de dialogue de protection intégrée des renseignements aux notifications d'avertissement sur les virus incitant les consommateurs à mettre à niveau leur logiciel antivirus. Ils semblent alors accorder beaucoup d'importance à la protection intégrée de la vie privée.

« *It shouldn't be a free-for-all because they'll do anything and design it. The box will be to the right or to the left.* »

« *I think it has to be a pop-up, otherwise it's just going to be some box down at the bottom, already pre-clicked 'yes' unless you change it, and you will never know.* »

« *Moi ce serait plutôt un 'basic', ce serait deux boîtes, mais il faudrait activer, il faudrait cliquer sur une des deux boîtes avant de pouvoir procéder sur le site, alors ce serait un peu le panneau de stop puis... Avec un bonhomme si tu es pas d'accord si tu veux pas le partage ou oui partage l'information et le go... »*

« *J'avais au beau milieu de l'écran, une boîte carrée — peu importe la forme — qui soit rouge et qui clignote.* »

« *The other thing that you have to look at is it has to be a responsive design, for sure, that people can use it on mobile. The thing is, people don't want to take the extra step. This is a very instantaneous society. That's what I find, especially the younger generation. It's like, oh, my god. So, if they have to actually take time every single time they click on a website to complete a privacy box... »*

– *Participants au groupe de discussion du CDIP*

Lorsqu'il a été demandé aux participants de dessiner l'idéale case relative à la protection des renseignements personnels, les caractéristiques des croquis qui en ont résulté étaient les suivantes :

- Des boîtes de dialogue qui se distinguent du reste de la page Web, du moins la première fois que la case de protection intégrée des renseignements s'affiche;
- Des couleurs remarquables, comme le rouge;
- Des icônes claires, comme des panneaux d'arrêt;
- Des lettres majuscules et une police de grande taille.

Les participants ont aussi ajouté que la case en question devrait être pratique et conviviale, ce qui fait l'objet de discussions ultérieures dans la présente section. Alors que cette protection intégrée des renseignements personnels pourrait d'abord prendre la forme d'une fenêtre de dialogue dans un navigateur ou un téléphone intelligent la première fois qu'il est utilisé, par exemple, il devrait par la suite être accessible par le biais d'une icône dans la barre d'adresse Web ou d'un autre outil pratique.

La case relative à la protection des renseignements personnels doit être facile à utiliser et se souvenir des préférences en matière de vie privée

Les participants aux groupes de réflexion ainsi que les chercheurs universitaires ont convenu que la protection intégrée des renseignements devait être simple, facile à comprendre et à utiliser et rédigée en langage simple. Les participants ont évoqué le fait que les

consommateurs attachent de la valeur à la convivialité et pourraient trouver irritant si la fenêtre s'affiche constamment lorsqu'ils naviguent dans internet. Le caractère trop familier nuirait également à l'importance de la boîte. Les participants aux groupes de discussion ont recommandé une formulation claire et des préférences sans trop d'options dotées de liens et d'occasions de consulter de plus amples précisions ou d'adapter encore plus les préférences en matière de vie privée à d'autres endroits. Ils ont également proposé que la case de protection intégrée de renseignements personnels soit mémorisée aux fins d'activités futures et s'applique automatiquement aux sites Web et aux applications utilisés par l'internaute. En somme, la retroaction reçu du groupe comprenait :

- Un faible nombre d'options ou de paramètres;
- Un langage simple et convivial;
- Des préférences personnalisées mémorisables pour utilisation et activités futures. Toutefois, il faut pouvoir revoir ou modifier les paramètres;
- L'accès à des renseignements ou à des réglages complémentaires.

« Tu sais comment il y a beaucoup de sites Internet qui ont des virus et qui sont super dangereux et notre McAfee... disons que par imprudence il y a un lien puis là ça va déjà créer une page et là ça va dire 'oops are you sure you want to go here?' À cause qu'il y a des 'possible threats', c'est sûr et c'est rouge; oui je veux quitter la page, mais sors moi d'ici. Tu vas arriver sur quelque chose de même puis si tu embarques ici toute l'information ici va être partagée, est-ce que tu acceptes, oui ou non. »

« It would have to be standardized so you always know where to look, as opposed to trying to find it on any specific website. It's always in a different place. »

« Just something that comes up right away on your screen that you can't miss, like updating your virus software, those things, and then some kind of icon. »

« So, I like the concept of simplicity. So, here is your monitor. Here is your screen. Right next to the start menu, which everybody cannot miss, is a little lock. You hit the lock and you get a pop-up. »

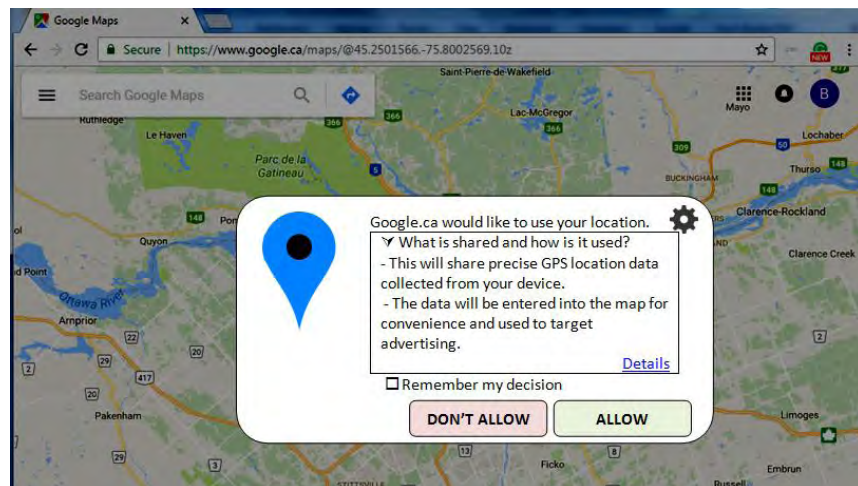
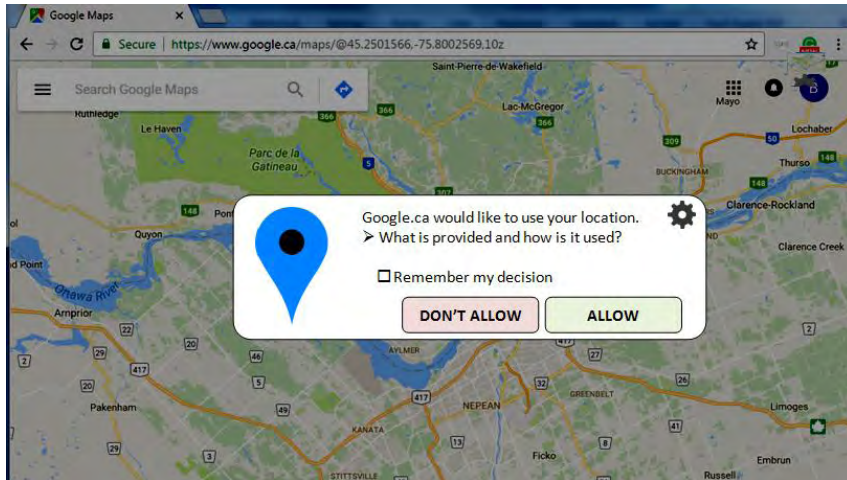
« I had two buttons that you could click on. Yes, for remember my profile. I guess, looking at it from a positive perspective, you'd want to be remembered for what things you were looking at... Underneath there would be a smaller button that would be more info about what information is being collected and that kind of thing, and maybe the cookie policy and that. Then you could also click, no, I'm only browsing. Then they'll be another button at the bottom that says, privacy policy, what our commitment is in terms of not tracking you if you click this button. »

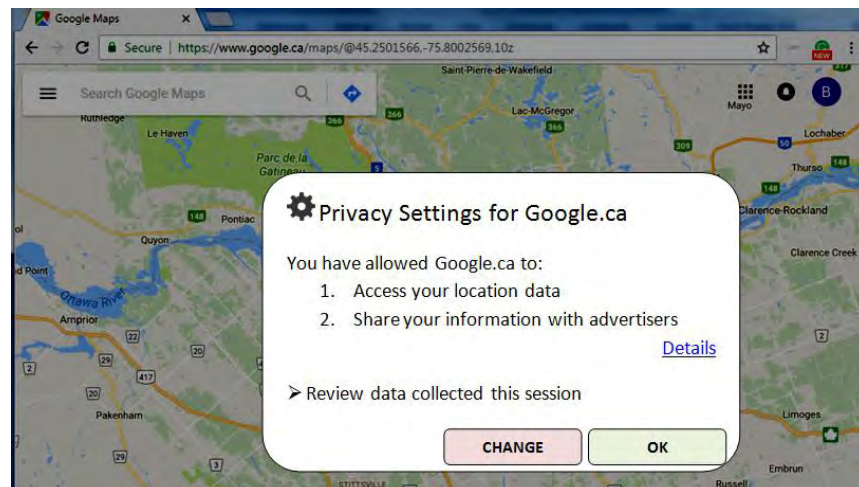
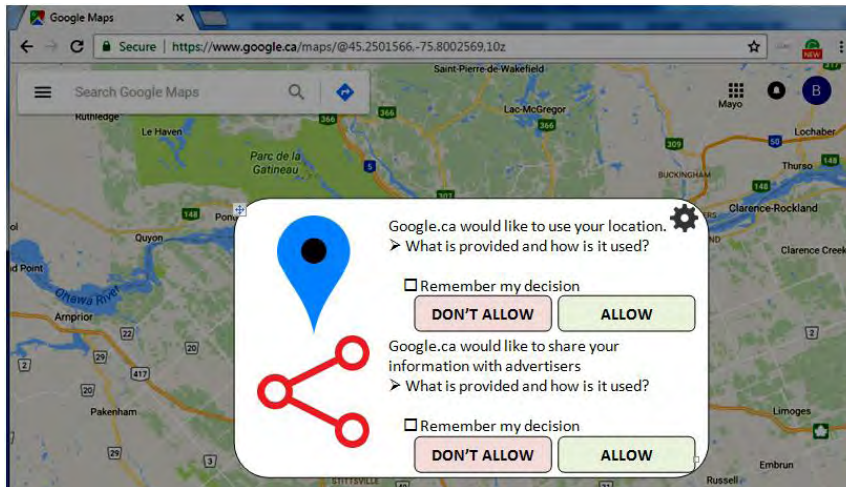
« Plain language. With check boxes. And don't put it in super script and font nine. Make it clear. Make it easy. Make it simple. »

– Participants au groupe de discussion du CDIP

En résumé, les participants aux groupes de discussion préfèrent une case relative à la vie privée visible, simple, facile à comprendre et dotée d'un nombre d'options limité. La case pourrait aussi, cependant, permettre aux utilisateurs de trouver des outils et des renseignements supplémentaires de protection. Si certains participants souhaiteraient exercer un contrôle accru sur leurs données, la plupart se souciaient plutôt du partage des données d'internautes avec des tierces parties. Ils se préoccupent aussi de la collecte de renseignements de nature délicate et désirent pouvoir interdire cette pratique entièrement. De nombreux participants s'intéressent aussi à consulter des données particulières récemment recueillies auprès d'eux par des organisations. Des exemples de conception possible de la case relative à la protection des renseignements figurant ci-dessous.

Figure 4-2. Échantillons de conception de la fenêtre respect de la vie privée





4.5 Existe-t-il un compromis en matière de protection des renseignements personnels?

Les recherches du CDIP ont également soulevé des questions controversées faisant l'objet de longues discussions. Le débat le plus courant concernait l'offre de services gratuits en échange des données de l'utilisateur et de publicités ciblées. Selon l'un des arguments, les consommateurs devraient être ouverts aux publicités et à la collecte de renseignements, car ils accèdent à un service sans frais et l'utilise sans coût supplémentaire.

Colin McKay, chef des politiques publiques et des relations gouvernementales chez Google Canada, a remarqué par exemple que la majorité des services en ligne

dépendent des revenus publicitaires et ne sont pas en mesure de générer des revenus d'abonnement ou autres pour la prise en charge de leurs services.

Selon un autre argument soulevé, des mesures strictes de protection de la vie privée pourraient entraver l'innovation en ligne par la prescription de modèles opérationnels, une décision qui devrait en fin de compte appartenir aux intervenants du marché.

De nombreux participants aux groupes de réflexion ont convenu que les consommateurs adorent les services dits gratuits et qu'ils seraient peu disposés à payer un service en ligne ou à s'en passer en vue de protéger leurs renseignements personnels. D'autres ont aussi reconnu que l'interdiction aux entreprises en ligne de suivre les utilisateurs ou de recueillir leurs données pourrait avoir des conséquences négatives sur les consommateurs ou les empêcher de profiter autant d'un service dit gratuit. Toutefois, nombre de participants estimaient tout de même que les utilisateurs devraient bénéficier d'autres choix ou options. Les participants étaient généralement d'avis que des limites du suivi des activités en ligne devraient être imposées et que les entreprises ne devraient pas avoir le droit de suivre l'ensemble des activités de l'internaute à leur seule discrétion — les utilisateurs devraient être en mesure d'interdire le suivi de certaines activités qu'ils considèrent comme privées.

L'offre de services gratuits en échange des données sur l'utilisateur et des publicités ciblées est couramment décrit comme une dichotomie — autrement dit, une situation tout ou rien. Or, les intérêts de la protection des renseignements personnels et des politiques relatives à la vie privée doivent tenir compte de détails et de nuances supplémentaires afin de s'aligner sur la perspective du consommateur en la matière. Les recherches et études sur la confidentialité montrent que celle-ci est contextuelle et que les personnes concernées adoptent naturellement divers comportements et s'adonnent à différentes activités en fonction de leurs situation ou interactions. Internet ne change pas nécessairement les valeurs ou les attentes associées à la protection de la vie privée, même s'il change de manière importante la portée des actions et activités individuelles. De nombreux participants aux groupes de discussion étaient particulièrement déçus du fait que nombre d'entreprises en ligne n'autorisaient pas les utilisateurs à accéder à un service, ou de l'utiliser, sans accepter les politiques et les pratiques de confidentialité de celui-ci. Cela contraint les consommateurs à choisir entre le respect de leur vie privée et l'accès à un service.

Dans le cadre des recherches préparatoires effectuées par le CDIP aux fins du présent rapport, la question de la publicité affichée en ligne a été distinguée du suivi et du partage des données d'utilisateurs individuels. Généralement, les participants ont compris que la publicité permettait aux entreprises de générer des revenus. Toutefois, la

publicité étant, ce qui les préoccupait le plus était la collecte et le partage de leurs renseignements en masse – qu'ils soient fournis volontairement ou non. Ils s'attendaient à ce qu'un service contacté ou consulté par l'utilisateur recueille de l'information, mais les consommateurs des groupes de discussion estimaient que la portée de la collecte devrait être limitée. Toutefois, les groupes de réflexion se préoccupaient particulièrement de la divulgation de ces renseignements à d'autres entreprises et parties non liées à l'entreprise initiale. Les participants ne s'opposaient pas autant aux publicités qu'à la collecte et à l'utilisation des renseignements à des fins multiples, y compris la publicité. L'anonymisation des données de l'utilisateur semble palier certaines inquiétudes du consommateur, mais il s'oppose tout à fait à la collecte et au partage de certains types d'information.

« J'aimerais que les gens, les sites soient plus transparents, pour ne pas dire plus honnêtes, à savoir si ils partagent ou non l'information. Les sites que je fréquente, j'y vais avec connaissance de cause, ça va être partagé, c'est un acquis, mais j'aimerais ça pouvoir restreindre jusqu'à un certain point oui. Comme il disait, c'est pas parce que j'ai quelque chose à cacher, c'est juste j'aime pas toujours l'idée qu'il y a quelqu'un par-dessus mon épaule. »

– Participant au groupe de réflexion du CDIP

Le CDIP a également demandé aux consommateurs du groupe de discussion et aux intervenants si les entreprises exploitées en ligne devraient être tenues de laisser les internautes accéder à un site Web ou à une application sans se soumettre au suivi de leurs renseignements et activités en ligne. Ce type d'option a été rejeté dans la plupart des cas à plusieurs motifs. Si certains participants aux groupes de discussion reconnaissent l'avantage de donner au consommateur un tel choix, de nombreuses personnes ont convenu qu'ils opteraient dans la plupart des cas pour le service gratuit. Dans certains cas, des doutes ont été exprimés quant à la mesure dans laquelle l'entreprise exploitée en ligne

respecterait l'entente. Certains intervenants du secteur s'inquiétaient de l'imposition de modèles organisationnels aux entreprises. Natasha Tusikov, professeur agrégée à l'Université York a également fait remarqué que ce type d'option pourrait créer un milieu où la vie privée est considérée comme un bien luxueux accessible aux seules personnes pouvant se le permettre.

En résumé, les services en ligne peuvent dépendre largement de revenus publicitaires. Toutefois, la mesure dans laquelle ces entreprises exigent la collecte, l'utilisation et la divulgation des données de l'utilisateur demeure un domaine où le choix et le contrôle accru de l'utilisateur est nécessaire. Les groupes de discussion et certains intervenants semblent favoriser l'approche d'autoriser les consommateurs à retirer leur consentement

à la collecte et au partage de renseignements, plutôt que d'envisager des options qui susciteraient la discrimination entre les consommateurs bien nantis ou non.

Le droit à la vie privée ne doit pas être considérée comme un compromis ou un échange en contrepartie de biens ou de services. Le respect de la vie privée doit plutôt être considéré comme un droit; il existe des lois régissant le respect de la vie privée et les organisations ne doivent pas être autorisées à les contourner par voie de contrat. Alors que les consommateurs sont prêts à accepter le suivi de certaines de leurs activités et informations en ligne, ils ne sont pas aptes à donner aux entreprises carte blanche, comme l'a dit l'un des participants au groupe de discussion, de suivre et de partager tous leurs renseignements. La vie privée ne doit pas constituer un scénario tout ou rien, mais reconnaître des attentes supérieures en matière de confidentialité dans certains contextes et inférieures dans d'autres cas. En outre, les paramètres par défaut de certains services en ligne devraient être d'abord axé sur la protection des renseignements personnels, plutôt qu'un partage et une permission larges visant le suivi et le partage de toute l'information.

Google, Facebook et d'autres grandes entreprises sophistiquées ont tenté d'améliorer leurs outils de confidentialité afin d'offrir davantage de choix et de contrôle en matière de renseignements personnels. Or, les consommateurs consultant un ensemble de sites Web et d'applications dotées d'une gamme de pratiques de confidentialité et ne sont pas en mesure de gérer seuls le volume des énoncés et des paramètres relatifs à la vie privée. Une protection intégrée normalisée des renseignements personnels pourrait permettre de promouvoir le choix et la sensibilisation de l'utilisateur au titre des options de confidentialité.

V. Sommaire et recommandations

5.1 Il y a place à de nouvelles initiatives de vie privée sur mesure, ce qui comprend la protection intégrée des renseignements personnels

Les recherches menées par le CDIP aux fins du présent rapport ont montré que les Canadiens attachent encore de la valeur à la protection de leur vie privée, c'est-à-dire la protection en soi des renseignements personnels. Ils font des choix conscients au quotidiens sur les données à partager ou non à leur sujet.

Le respect de la vie privée continue d'être valorisé peu importe la technologie ou la plateforme de choix. Toutefois, internet modifie le point de vue des consommateurs canadiens par rapport à cette question. Les Canadiens ne se soucient pas moins de leur vie privée, mais estiment qu'ils ont moins de contrôle sur la protection de leurs renseignements personnels. L'enquête de 2016 menée par le Bureau de la consommation montre que 74 % s'estiment moins protégés qu'il y a dix ans dans leur vie quotidienne en matière de renseignements personnels⁷⁹. Les groupes de discussion du CDIP ont également révélé un scepticisme important et une méfiance à l'égard des entreprises exploitées en

ligne relativement au suivi et à l'utilisation des données des consommateurs. Malgré l'existence de règlements en matière de respect de la vie privée, de nombreux consommateurs estiment que les entreprises les contournent et ne croient pas que ces entreprises défendent l'intérêt supérieur du consommateur.

Néanmoins, 90 % des Canadiens sont inquiets ou relativement inquiets du fait que leurs renseignements personnels seront utilisés par les entreprises afin de prendre des décisions à leur sujet, tandis que 87 % sont inquiets de l'utilisation de leurs renseignements par des entreprises de marketing afin d'analyser leurs préférences,

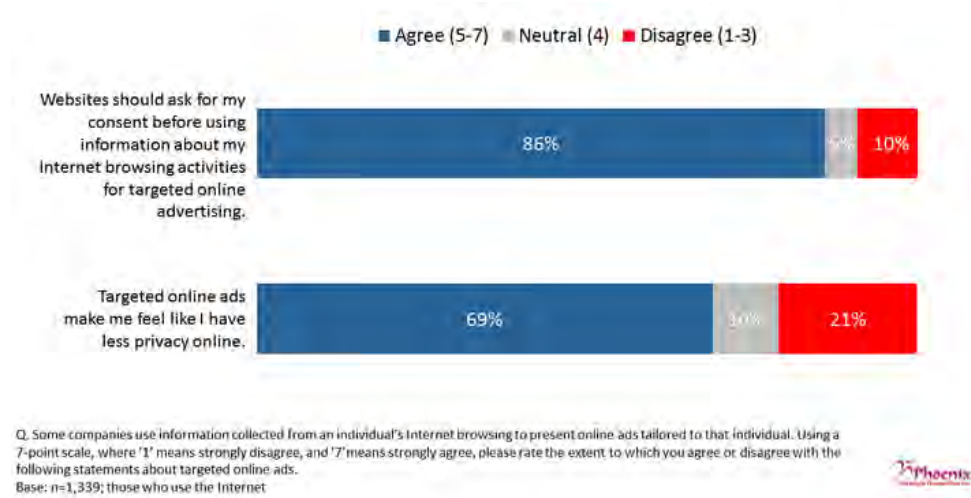
« When I approach surfing the web and that, I assume that everything is being tracked and everything is being stored. So, I already understand that. This [Privacy Box], I would like to have because, again, I would like to know exactly what specifically is being tracked from my habits or whatever on my computer, and have options of giving permission of what can be accessed... that, I feel, is a lot more important. But again, the whole privacy thing is just more like, I think there is a lot more that I don't understand about it as well. »

– Participant au groupe de discussion du CDIP

⁷⁹ Commissariat à la protection de la vie privée du Canada, *2016 Survey of Canadians on Privacy: Final Report* (2016), en ligne : Priv.gc.ca < https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12>, Figure 4.

quelles qu'elles soient⁸⁰. La grande majorité (86 %) estime toujours que les sites Web devraient demander leur consentement avant d'utiliser les données sur leur navigation dans internet aux fins des publicités ciblées en ligne.

Figure 5-1. Perspectives canadiennes sur les publicités ciblées en ligne



Source : Commissariat à la protection de la vie privée du Canada, 2016

De nombreuses entreprises, à l'exception des réseaux sociaux de grande ampleur plus sophistiqués ont tendance à se fier à des politiques ou à des énoncés de confidentialité afin d'informer les internautes et d'obtenir le consentement visant l'utilisation, la collecte et la divulgation de données. Toutefois, un nombre grandissant d'études montre que les politiques de confidentialité sont pour la plupart inefficace dans le cas du consommateur, notamment car elles sont difficiles à trouver, elles présentent un trop grand volume d'information et sont rédigées avec des formules vagues susceptibles de créer plusieurs interprétations. Certains services en ligne proposent des paramètres de confidentialité plus granulaires et sophistiqués. Alors que les consommateurs peuvent faire l'effort de personnaliser leurs réglages de protection de la vie privée, comme sur Facebook, de nombreux participants aux groupes de discussion se sont dits dépassés par le nombre de sites ou d'applications utilisés. Dans le cas des personnes qui ont tenté d'utiliser le mode de navigation en privé ou d'autres outils universels de protection de la vie privée, ils ont constaté que la fonctionnalité des sites Web consultés était touchée.

⁸⁰ *Ibid.*, Figures 6 et 7.

Est-il trop tard? Certains participants aux groupes de discussion estimaient qu'il était trop tard pour mitiger la collecte des données d'utilisateurs et lancer des mesures de sauvegarde de la vie privée en ligne. Selon eux, la collecte et l'utilisation de renseignements personnels est déjà si répandue et une source de revenu cruciale que les entreprises exploitées en ligne résisteraient avant de se désister de cette pratique. Toutefois, les participants ont également fait valoir que si une nouvelle initiative de protection des renseignements personnels existait, en particulier axée sur un choix et de l'information conviviaux destinés aux consommateurs, ils l'appuieraient. Certains participants ont remarqué que toute initiative de réglementation du respect de la vie privée constitue une pratique préférable à ne rien faire du tout.

Il semble donc y avoir place à des initiatives de protection intégrée des données, en particulier celles axées sur les valeurs, l'expérience et le contrôle du consommateur. Les participants aux groupes de discussion et les intervenants universitaires étaient très ouverts à l'idée d'une case de respect intégré de la vie privée qui simplifierait les renseignements initiaux et les outils mis à la disposition des internautes. Si cette solution ne constitue pas une panacée à la protection de la vie privée de l'utilisateur, de nombreux participants aux groupes de discussion estiment qu'il s'agirait d'un point de départ utile et d'un outil éducatif alors que peu de renseignements sont accessibles sur le suivi des données, leur utilisation et leur divulgation. Le CDIP recommande que les responsables de l'élaboration des politiques appuient activement la protection intégrée des renseignements personnels, en particulier celles entreprises par les organismes sans but lucratif et les chercheurs universitaires, grâce aux fonds publics, à des objectifs clairs, de même qu'à des lignes directrices ou normes concrètes en matière de données protégées par défaut (notamment des normes régissant le caractère raisonnable).

« I appreciate that fact that there is a privacy commissioner that cares about individual rights and privacy concerns and all of that, but the internet has been around now for 22, 23, 24 years. Now you're worried about our privacy? Really? Actually? Now? [...] Be real now. If you wanted to implement laws and all of this, twenty years ago might have been a good time. »

– Participant au groupe de discussion du CDIP

Les recherches du CDIP appuient l'élaboration et la mise en œuvre d'une case relative à la protection des renseignements personnels normalisée qui :

- ❖ permet aux consommateurs d'interdire le suivi de leur emplacement. Cette protection intégrée pourrait également donner aux

consommateurs la possibilité de sélectionner le type de renseignement qui peut ou non être recueilli ou suivi;

- ❖ permet aux consommateurs d'interdire le partage de données avec des tierces parties;
- ❖ propose des sommaires énonçant clairement : a) les tierces parties avec lesquelles les données de l'utilisateur sont partagées et l'emplacement des tiers, et b) le mode spécifique d'utilisation des données utilisateur;
- ❖ fournit aux utilisateurs des moyens d'accéder aux données récemment recueillies à leur sujet, par ordre d'organisation.

Les groupes de discussion ont également exprimé clairement que la case relative à la protection de la vie privée doit figurer de manière proéminente, être simple et conviviale et facile à utiliser et à comprendre – et comprennent des contrôles d'arrêt de niveau supérieur (goulets d'étranglement) tel que recommandé par Lederer *et al.*⁸¹ Alors que les participants des groupes de discussion attachent de la valeur au caractère pratique, la plupart estimaient que la case relative au respect de la vie privée devrait s'afficher comme un dialogue d'avertissement qui se souviendrait des préférences de l'utilisateur et lui donnerait la possibilité de consulter et de modifier les options de protection intégrée des renseignements personnels. Les consommateurs estimaient aussi qu'il serait avantageux et pratique de disposer d'une case exploitable sur plusieurs appareils et plateformes.

5.2 Recommandations finales

Le présent rapport avait pour principal objectif de contribuer au dialogue sur la protection intégrée des renseignements personnels sur mesure en examinant cette question du point de vue du consommateur. Le CDIP espère que les conclusions de recherche sur la protection intégrée des données sur la vie privée seront utiles à tous les intervenants, y compris les entreprises, les décideurs et les chercheurs. Ces conclusions ont été tirées d'un grand ensemble d'études de recherche, y compris des publications secondaires. Ces conclusions de recherche doivent être prises en compte par tous les intéressés puisque la portée et la gamme d'activités en ligne et la valeur des données massives ne fera qu'augmenter substantiellement à l'avenir. Dans ce contexte, la protection des droits individuels au respect de la vie privée est cruciale. Les organisations doivent poursuivre leur apprentissage afin de mettre au point des outils et

⁸¹ Scott Lederer et al., *Personal Privacy through Understanding and Action: Five Pitfalls for Designers* (2004), en ligne : Berkeley <<https://www2.eecs.berkeley.edu/bears/2004/STARS/lederer-personal.pdf>>.

des pratiques répondant aux besoins et aux attentes du consommateur. Si ce n'est pas réalisé par le marché à lui seul, une intervention réglementaire pourrait être requise.

Le CDIP recommande fortement que ses conclusions, y compris l'élaboration d'une protection intégrée des renseignements, soient envisagées et adoptées par toutes les entreprises et les organisations privées dotées d'une présence sur le Web. Si les préoccupations du consommateur ne sont pas traitées par les options du marché, une case obligatoire de protection intégrée des renseignements s'appliquerait à tous les services et applications en ligne offerts aux Canadiens et pourraient s'inscrire dans les lois et politiques de respect de la vie privée à l'avenir. De l'avis du CDIP, les responsables de l'élaboration de politiques ont un rôle essentiel à exercer dans la protection de la vie privée des Canadiens.

La protection intégrée de la vie privée est et deviendra de plus en plus importante en vue de protéger les renseignements personnels des Canadiens et de s'assurer qu'ils disposent d'un vrai choix et contrôle et qu'ils puissent donner un consentement significatif lié à la collecte, à l'utilisation et à la divulgation de renseignements. À mesure que l'innovation continue de constituer un objectif politique central du gouvernement fédéral actuel, le gouvernement du Canada doit fournir un appui accru à la protection intégrée des renseignements personnels. Le gouvernement doit consacrer des fonds publics supplémentaires aux projets de recherche et aux initiatives sur le respect de la vie privée sur mesure, en particulier ceux entrepris par les organismes sans but lucratif et les chercheurs universitaires. Il doit également intégrer les exigences de protection de la vie privée sur mesure au cadre législatif fédéral, notamment la *Loi sur la protection des renseignements personnels et les documents électroniques*⁸² (LPRPDE). Par exemple, le *Règlement général sur la protection des données*⁸³ de

⁸² L.C. 2000, c. 5.

⁸³ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (soulignement ajouté) :

Article 25

Protection des données dès la conception et protection des données par défaut

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la

l'Union européenne prévoit désormais des exigences de protection des données par défaut. Ces exigences de l'Union européenne qui sont suffisamment larges et applicables seraient tout aussi applicables au contexte canadien et devraient être intégrées à la LPRPDE.

En outre, les décideurs fédéraux et le Bureau de la consommation devraient mettre davantage l'accent sur la protection intégrée des renseignements personnels en publiant des études et des documents de recherche fournissant des lignes directrices et des exemples clairs, notamment la création de normes. Le CDIP recommande notamment au Bureau de la consommation d'élaborer des lignes directrices sur la mise en œuvre de la protection intégrée des données destinées aux organisations privées. Un processus de certification de la protection intégrée de la vie privée régi par le Bureau de la consommation pourrait également être utile.

Enfin, ce projet de recherche souligne également les principales difficultés associées aux processus actuels de sollicitation du consentement et de communication d'informations utiles sur les pratiques de respect de la vie privée. En ce sens, si la LPRPDE comprend une définition de *consentement valide*⁸⁴, l'utilité du consentement implicite doit être revue. De nombreux participants aux groupes de discussion estiment que les entreprises suivent leurs activités en ligne et leurs renseignements à leur insu et sans consentement, tandis que les services en ligne prétendraient sans doute qu'ils ont obtenu un consentement implicite. En outre, de nombreux consommateurs du groupe de

protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

3. Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article.

⁸⁴ *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5, s. 6.1.

discussion estimaient n'avoir aucun autre choix que d'accepter les politiques de confidentialité afin d'accéder à un service, mais n'ont pas entièrement lu ou compris le contenu des énoncés en question. Les législateurs fédéraux doivent envisager de regrouper les modalités de confidentialité aux modalités générales acceptées par un utilisateur en vue d'accéder à un service en ligne. Le CDIP constate que le règlement de l'Union européenne interdit désormais cette pratique⁸⁵.

L'utilité et la pertinence des politiques de confidentialité à titre de mesure de prestation des renseignements sur la vie privée aux internautes devrait également être réexaminées. Alors que le Bureau de la consommation propose des lignes directrices sur les déclarations de confidentialité⁸⁶, les conclusions du présent rapport remettent en question l'efficacité de ces politiques et énoncés de confidentialité relativement à la communication des renseignements sur la protection de la vie privée aux consommateurs. Le temps est peut-être venu de se concentrer moins sur les énoncés de confidentialité et davantage sur la protection intégrée des renseignements personnels sur mesure axée sur le choix, le contrôle et l'expérience de l'utilisateur.

Somme toute, la protection intégrée des renseignements personnels sur mesure est dotée d'un avenir pertinent et important et doit être publiquement soutenue et renforcée par les responsables de l'élaboration de politiques. Le présent rapport constitue l'une des premières études de recherche sur les mesures de protection de la vie privée sur mesure du point de vue du consommateur canadien. Or, des recherches supplémentaires en la matière sont nécessaires afin de faire fond sur les conclusions présentées dans le rapport.

⁸⁵ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. Voir par exemple le récita 43:

Le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce, ou si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution.

Voir aussi l'article 7(4):

Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

⁸⁶ Voir : Commissariat à la protection de la vie privée du Canada, *Privacy policies*, en ligne : Priv.gc.ca <<https://www.priv.gc.ca/en/privacy-topics/privacy-policies/>> (accessed 6 March 2017).

Le CDIP tient à remercier le Bureau de la consommation d'ISDC du Canada pour sa subvention de recherche qui a permis de financer ce projet.

Recommandations du CDIP

Recommandation n° 1

La « Protection intégrée des renseignements » développée dans le présent rapport doit être prise en compte par toutes les entreprises et les organismes privés dotés d'une présence en ligne et idéalement coordonnées par une association du secteur (telle que les Normes canadiennes de publicité ou la Network Advertising Initiative).

Recommandation n° 2

Le commissariat à la vie privée du Canada doit publier des lignes directrices sur l'adoption et la mise en œuvre de mesures de protection de la vie privée par les services et application en ligne, l'accent étant particulièrement mis sur les organisations privées. Il doit également, de manière générale, mettre en relief la protection intégrée des renseignements personnels sur mesure, notamment : a) la publication de rapports et de documents de recherche; b) l'instauration de lignes directrices claires et d'exemples ou la création d'une norme de protection intégrée des renseignements sur mesure.

Recommandation n° 3

Les exigences de protection des renseignements sur mesures doivent être inscrits dans la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) fédérale.

Recommandation n° 4

Le gouvernement de Canada doit consacrer un financement public aux initiatives et à la recherche sur la protection intégrée des renseignements personnels sur mesure, en particulier celles entreprises par des organismes sans but lucratif et des chercheurs universitaires.

Recommandation n° 5

Les législateurs et les décideurs fédéraux doivent envisager de retirer la permission d'obtenir un consentement implicite de la collecte, de l'utilisation et de la divulgation des renseignements personnels aux termes de la LPRPDE. Il y a également lieu d'envisager l'interdiction du regroupement des modalités de confidentialité que l'utilisateur doit accepter en vue d'accéder un service en ligne ou de s'en servir.

Recommandation n° 6

Le commissariat à la vie privée du Canada doit réexaminer l'efficacité et la pertinence des politiques de protection de la vie privée à titre de mode de communication des principales informations en la matière aux particuliers.

Le Centre pour la défense de l'intérêt public a reçu du financement en vertu du Programme de contributions pour les organisations sans but lucratif de consommateurs et de bénévoles d'Innovation, Sciences et Développement économique Canada.

Les opinions exprimées dans ce rapport ne sont pas nécessairement celles d'Innovation, Sciences et Développement économique Canada ou du gouvernement du Canada.

Bibliographie

Lois et règlements

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5.

Règlement (EU) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

The Privacy Act of 1974 , 5 U.S.C. § 552a.

Sources secondaires

Acquisti, Alessandro et Jens Grossklags. « What Can Behavioral Economics Teach Us About Privacy? » (2006), en ligne : Heinz.cmu.edu <<http://www.heinz.cmu.edu/~acquisti/papers/Acquisti-Grossklags-Chapter-Etries.pdf>>.

Acquisti, Alessandro, Laura Brandimarte et George Loewenstein. « Privacy and Human Behavior in the Age of Information » (2015) 347:6221 Science 509.

Bakos, Yannis, Florencia Marotta-Wurgler et David R. Trossen, « Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts » (2014) 43:1 J. Legal Studies 1.

Ben-Shahar, Omri et Adam S. Chilton, « Simplification of Privacy Disclosures: An Experimental Test » (2016), University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 737, en ligne : SSRN <<https://ssrn.com/abstract=2711474>>.

Borgesius, Frederik Zuiderveen. « Informed Consent: We Can Do Better to Defend Privacy » (2015), en ligne : IVIR.nl <<http://www.ivir.nl/publicaties/download/1795>>.

Bruening, Paula J. et Mary J. Culnan. « Through a Glass Darkly: From Privacy Notices to Effective Transparency » 17:4 North Carolina J.L. & Tech. 515.

- Cavoukian, Ann. *Privacy by Design* (2013), en ligne : CIPVP <<https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf>>.
- Cavoukian, Ann, Stuart Shapiro et R. Jason Cronk. *Privacy Engineering: Proactively Embedding Privacy, by Design* (janvier 2014), en ligne : CIPVP <<https://www.ipc.on.ca/wp-content/uploads/Resourc es/pbd-priv-engineering.pdf>>.
- Deloitte. *L'Université Ryerson et Deloitte s'associent pour offrir la certification de protection de la vie privée : Nouvelle norme de protection de la vie privée* (2015), en ligne : Deloitte <<https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-fr-ers-privacy-by-design-brochure.PDF>>.
- Executive Office of the President, President's Council of Advisors on Science and Technology. *Report to the President on Big Data and Privacy: A Technological Perspective* (2014), en ligne : HSDL <<https://www.hsdl.org/?view&did=755569>>.
- European Commission Directorate-General for Justice and Consumers. *Special Eurobarometer 431: Data Protection Report* (2015), en ligne : Europa.eu <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf>.
- Facebook, *Consentement et protection de la vie privée : Commentaires de Facebook sur le document de discussion du Commissariat à la protection de la vie privée du Canada* (2016), en ligne : CPVP <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultation-sur-le-consentement-en-vertu-de-la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques/memoires-recus-dans-le-cadre-de-la-consultation-sur-le-consentement-en-vertu-de-la-lrpde/sub_consent_32/>.
- Feigenbaum, Joan et al. « Privacy Engineering for Digital Rights Management Systems », dans Tomas Sander, ed., *Revised Papers from the ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management* 79 (2002), en ligne : Université Yale <<http://www.cs.yale.edu/homes/jf/FFSS.pdf>>.
- Goldberg, Rafi. « Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities » (13 mai 2016), en ligne : NTIA <<https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>>.

- Conseil des technologies de l'information et des communications. *Big Data and the Intelligence Economy: Canada's Hyper Connected Landscape* (2015), en ligne : CTIC <<http://www.ictc-ctic.ca/wp-content/uploads/2015/12/BIG-DATA-2015.pdf>>.
- International Data Corporation. « Worldwide Big Data and Business Analytics Revenues Forecast to Reach \$187 Billion in 2019, According to IDC » (23 mai 2016), en ligne : IDC <<https://www.idc.com/getdoc.jsp?containerId=prUS41306516>>.
- Lederer, Scott et al. *Personal Privacy through Understanding and Action: Five Pitfalls for Designers* (2004), en ligne : Berkeley <<https://www2.eecs.berkeley.edu/bears/2004/STARS/lederer-personal.pdf>>.
- Libert, Timothy. « Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites » (2015) 9 International Journal of Communication 3544.
- Madden, Mary et Lee Rainie. *Americans' Attitudes About Privacy, Security and Surveillance* (2015), Pew Research Center <<http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>>.
- Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, Stanford Law Books, 2010).
- Commissariat à la protection de la vie privée du Canada. *Sondage auprès des Canadiens sur la protection de la vie privée de 2016 : Rapport final* (2016), en ligne : Priv.gc.ca <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/por_2016_12/>.
- Commissariat à la protection de la vie privée du Canada. *Dix conseils pour améliorer votre politique de confidentialité en ligne et la transparence de vos pratiques en matière de protection de la vie privée* (2013), en ligne : CPVP <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/politiques-de-confidentialite/02_05_d_56_tips2/>.
- École d'art et de design de l'Ontario. *Understanding, Discovering and Asserting Personal Privacy Preferences: A Feasibility Study*, en ligne :

[https://wiki.fluidproject.org/display/fluid/\(Floe\)+Privacy+Needs+and+Preferences](https://wiki.fluidproject.org/display/fluid/(Floe)+Privacy+Needs+and+Preferences).

Option consommateurs. *Le prix de la gratuité. Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne?* (2015), en ligne : Option consommateurs https://option-consommateurs.org/documents/principal/fr/File/option_consommateurs_2014_2015_gratuite_rapport.pdf.

Rainie, Lee et Maeve Duggan. *Privacy and Information Sharing* (2016), en ligne : Pew Research Center http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf.

Reidenberg, Joel R. et al. « Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding » (2015) 30:1 Berkeley Tech. L.J. 39.

Rubinstein, Ira S. « Regulating Privacy by Design » (2011) 26 Berkeley Tech. L.J. 1409.

Rubinstein, Ira S. et Nathaniel Good. « Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents » (2013) 28:2 Berkeley Tech. L.J. 1333.

Schaub, Florian *et al.* « A Design Space for Effective Privacy Notices » (2015), USENIX Association 2015 Symposium on Usable Privacy and Security, en ligne : USENIX <https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf>.

Solove, Daniel J. « Introduction: Privacy Self-Management and the Consent Dilemma » (2013) 126 Harvard L. Rev. 1880.

Spiekermann, Sarah et Lorrie Faith Cranor. « Engineering Privacy » (2009) 35:1 *IEEE Transactions on Software Engineering* 67.

U.S. Department of Health, Education & Welfare. *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington D.C. : Department of Health, Education, and Welfare, 1973).

Van der Sloot, Bart, Dennis Broeders et Erik Schrijvers, eds. *Exploring the Boundaries of Big Data* (Amsterdam : Amsterdam University Press, 2016).

White, Geoff. *Déconnecté du réseau? Repérage des technologies basées sur la localisation et la Loi* (Ottawa : Centre pour la défense de l'intérêt public, 2015), en ligne : CDIP <http://www.CDIP.ca/wp-content/uploads/2015/09/OCA-2014-15-Off-the-Grid-Location-based-technologies-and-the-law-Final-Report_FR.pdf>.