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?

RAPPORT DE RECHERCHE

Rapport réalisé par Option consommateurs
et présenté au Bureau de la consommation d'Industrie Canada

Juin 2015

Option consommateurs a reçu un financement en vertu du programme de contributions pour les organisations sans but lucratif de consommateurs et de bénévoles d'Industrie Canada. Les opinions exprimées dans ce rapport ne sont pas nécessairement celles d'Industrie Canada ou du gouvernement du Canada.

Rédigé par : Alexandre Plourde

Dépôt légal
Bibliothèque nationale du Québec
Bibliothèque nationale du Canada
978-2-89716-024-1

Option consommateurs
50, rue Ste-Catherine Ouest, Bureau 440
Montréal (Québec)
H2X 3V4
Téléphone : 514 598-7288
Télécopieur : 514 598-8511

Adresse électronique : info@option-consommateurs.org
Site Internet : www.option-consommateurs.org

Table des matières

Option consommateurs

MISSION

Option consommateurs est une association à but non lucratif qui a pour mission de promouvoir et de défendre les droits et les intérêts des consommateurs et de veiller à ce qu'ils soient respectés.

HISTORIQUE

Issue du mouvement des associations coopératives d'économie familiale (ACEF), et plus particulièrement de l'ACEF de Montréal, Option consommateurs existe depuis 1983. En 1999, elle a regroupé ses activités avec l'Association des consommateurs du Québec (ACQ) qui existait depuis plus de 50 ans et accomplissait la même mission qu'Option consommateurs.

PRINCIPALES ACTIVITÉS

Option consommateurs aide les consommateurs qui vivent des difficultés, les reçoit en consultation budgétaire et donne des séances d'information sur le budget, l'endettement, le droit de la consommation et la protection de la vie privée. Nous effectuons aussi des visites gratuites chez des ménages à faible revenu afin d'améliorer l'efficacité énergétique de leur logement.

Chaque année, nous réalisons des rapports de recherche sur des enjeux de consommation d'importance. Nous intervenons également auprès des décideurs et des médias pour dénoncer des situations inacceptables. Lorsque nécessaire, nous intentons des recours collectifs contre des commerçants.

MEMBERSHIP

Pour faire changer les choses, les actions d'Option consommateurs sont multiples : recherches, recours collectifs et pressions auprès des instances gouvernementales et des entreprises. Vous pouvez nous aider à en faire plus pour vous en devenant membre d'Option consommateurs au www.option-consommateurs.org

Remerciements

Cette recherche a été réalisée et rédigée par M^e^ Alexandre Plourde, sous la supervision de Mme Maryse Guénette, responsable du service de recherche et de représentation d'Option consommateurs. Elle a été rendue possible grâce au soutien financier du Bureau de la consommation d'Industrie Canada.

L'auteur tient à souligner le travail des employés, stagiaires et bénévoles qui œuvrent chez Option consommateurs et qui, de près ou de loin, ont collaboré à cette recherche. Il remercie plus particulièrement Mivania Henry et Joanie Provost Brisebois, stagiaires en techniques juridiques du Collège Ahuntsic, de même qu'Amadou Barry, François Boillat-Madfouny et Linh Nguyen, étudiants en droit à l'Université de Montréal.

L'auteur souhaite aussi remercier chaleureusement toutes les personnes qui ont accepté de lui accorder une entrevue dans le cadre de cette recherche : Manon Arcand, professeure en marketing à l'UQAM, Stéphane Gauvin, professeur en marketing à l'Université Laval, Éloïse Gratton, avocate associée et Cochef National, groupe de pratique Respect de la vie privée chez Borden Ladner Gervais LLP, Jacques Nantel, professeur en marketing à HEC Montréal, Pierrot Péladeau, expert en évaluation sociale de systèmes d'information, Alexandre Sagala, vice-président chez Publipage, Jacques St Amant, chargé de cours en droit de la consommation à l'UQAM et Nicolas Vermeys, professeur à la Faculté de droit de l'Université de Montréal.

Enfin, l'auteur tient à remercier, pour son soutien méthodologique, M. Bruno Marien, sociologue et chargé de cours au département de science politique et de droit de l'Université du Québec à Montréal. Il remercie également le professeur Jean-Pierre Beaud, doyen de la Faculté de science politique et de droit de cette même institution, qui a effectué l'évaluation du rapport.

Résumé

Google, Facebook, Yahoo!, YouTube… la plupart des sites que les internautes consultent quotidiennement n'exigent pas le moindre sou de leurs utilisateurs. Ces fournisseurs de services sans frais financent notamment leurs activités grâce à la publicité comportementale en ligne (PCL), une forme de publicité dans laquelle on dresse le profil d'un internaute à partir de ses activités de navigation afin d'afficher des annonces y correspondant sur les sites qu'il fréquente.

L'analyse des politiques de protection de la vie privée des plus importants fournisseurs de services sans frais sur Internet au Canada révèle que ces fournisseurs recueillent une quantité fulgurante de données sur leurs utilisateurs, et peuvent attribuer au profil d'un internaute un nombre considérable d'étiquettes. Ces politiques imposent bien peu de limites aux entreprises quant à l'utilisation des renseignements personnels des internautes à des fins publicitaires.

En groupes de discussion, les consommateurs canadiens se sont dits surpris de l'ampleur de la collecte et de l'utilisation de leurs renseignements personnels dans le cadre de la PCL. De manière générale, ils ont affirmé que plus un renseignement se rapproche de leur sphère d'intimité, moins ils souhaitent qu'on l'utilise pour des fins de PCL. Ils ont également formulé le souhait d'être mieux informés sur la PCL et de pouvoir y consentir valablement.

Contrairement à ce que laissent entendre certaines politiques analysées, les données recueillies sur les internautes dans le cadre de la PCL seront généralement considérées comme des renseignements personnels au sens de la loi. Alors que ces renseignements personnels constituent une monnaie d'échange permettant aux consommateurs d'accéder aux services sans frais en ligne, on note une certaine discordance entre l'obligation légale des entreprises de ne recueillir que les renseignements personnels nécessaires aux fins qu'elles énoncent et la quantité presque illimitée de données qu'elles affirment recueillir. De même, compte tenu des lacunes dans l'information divulguée et des défaillances des mécanismes de refus disponibles, on peut douter que le consentement obtenu des consommateurs est véritablement éclairé.

Bien que la loi n'établisse pas de catégories fixes de renseignements personnels dont la collecte ou l'utilisation serait interdite dans le cadre de la PCL, elle prévoit des exigences de consentement plus élevées quant aux renseignements personnels qualifiés de sensibles. Alors que la loi adopte une définition contextuelle de la sensibilité d'un renseignement, les entreprises, dans le contexte virtuel, déterminent elles-mêmes des catégories de renseignements personnels qu'elles estiment être sensibles. En conséquence, les interprétations peuvent varier d'une entreprise à l'autre. De plus, plusieurs entreprises ne semblent pas considérer *a priori* comme sensibles certains types de renseignements pourtant délicats, tels que la géolocalisation et le contenu de la correspondance privée.

Afin de mieux guider les entreprises, Option consommateurs recommande notamment d'adopter des lignes directrices désignant explicitement des catégories de renseignements personnels comme étant de nature sensible, sans toutefois limiter la portée et la flexibilité de la loi. Afin de s'assurer que les consommateurs donnent un consentement éclairé à la PCL, Option consommateurs recommande, entre autres, de mettre en œuvre des mécanismes simples, efficaces et harmonisés permettant aux consommateurs de consentir valablement et activement à la collecte de leurs renseignements personnels dans le cadre de la PCL.

Interrogator: Would you say Mr. Pickwick reminded you of Christmas?

Witness: In a way.

Interrogator: Yet Christmas is a winter's day, and I do not think Mr. Pickwick would mind the comparison.

Witness: I don't think you're serious. By a winter's day one means a typical winter's day, rather than a special one like Christmas.

– Alan M. TURING, *Computing Machinery and Intelligence* (1950)[1]

Introduction

Google, Facebook, Yahoo!, YouTube… la plupart des sites que les internautes consultent quotidiennement n'exigent pas le moindre sou de leurs utilisateurs. Pourtant, cette apparente gratuité a un coût pour le consommateur.

En échange d'un compte Facebook ou d'une requête sur Google, il doit accepter de divulguer un nombre considérable de renseignements personnels : historique web, termes recherchés, achats en ligne, adresse IP[2], etc. Ces renseignements, une fois combinés, permettent de dresser le profil du consommateur, de deviner ses habitudes, ses champs d'intérêts… et d'afficher des publicités y correspondant sur les sites qu'il fréquente.

Cette pratique, nommée publicité comportementale en ligne (ci-après « PCL »), contribue à financer le contenu en ligne offert sans frais. Puisque ce type de publicité serait deux fois plus efficace que la publicité en ligne non ciblée[3], on peut penser que plus les entreprises en ligne en apprennent sur leurs utilisateurs, et plus elles se servent des informations qu'elles détiennent pour leur attribuer des caractéristiques, plus elles peuvent générer de revenus publicitaires.

Bien sûr, il est légitime pour une entreprise de chercher à rentabiliser ses activités. Cependant, la quantité et le type de renseignements personnels recueillis à cette fin ainsi que l'utilisation qui en est faite demeurent préoccupants.

Questions de recherche

Au Canada, des études exposent plusieurs difficultés soulevées par la PCL en matière de protection de la vie privée, telles que les lacunes dans l'information divulguée au consommateur

[1] Alan M. TURING, « Computing Machinery and Intelligence », (1950) 59-236, *Mind*, 433, p. 446

[2] Une adresse IP (*Internet Protocol*) est un numéro d'identification attribué à chaque appareil utilisant le réseau Internet et qui rend possible la communication des informations sur le réseau.

[3] Howard BEALES, *The Value of Behavioral Targeting*, étude présentée au Network Advertising Initiative, 2010

quant à la collecte de ses renseignements personnels ou dans l'obtention de son consentement[4].

Cependant, malgré la grande variété de renseignements que les entreprises peuvent recueillir sur les internautes, on en sait peu sur les types de renseignements que les consommateurs sont prêts à divulguer ou non dans le cadre de la PCL, ou plus généralement sur les problématiques liées à la collecte de chaque type de renseignement personnel. Pourtant, des études réalisées à l'étranger laissent penser que l'acceptabilité sociale de cette pratique peut varier selon les renseignements collectés : aux États-Unis, par exemple, une étude indique que les internautes seraient moins enclins à divulguer certains types de renseignements que d'autres à des fins de PCL, tels que leurs coordonnées ou leur géolocalisation[5].

Qu'en est-il au Canada? Quelles sont les pratiques des principaux fournisseurs de services sans frais sur Internet? Quels renseignements personnels les consommateurs sont-ils prêts à divulguer pour obtenir un service « gratuit » sur Internet, et quels autres renseignements ne veulent-ils pas partager? Y a-t-il des renseignements qui ne devraient pas être recueillis pour des fins de PCL? Quelles collectes et utilisations de renseignements personnels sont légitimes pour offrir un service sans frais? Le droit canadien est-il adapté à ces enjeux?

Méthodologie

Pour répondre à ces questions, nous avons d'abord esquissé le portrait du fonctionnement de la PCL (section 1). Nous avons ensuite analysé les politiques de confidentialité des plus importants fournisseurs de services sans frais sur Internet (section 2). Afin d'obtenir le point de vue des consommateurs, nous avons tenu des groupes de discussion (deux groupes à Toronto et deux autres à Montréal) avec des Canadiens de tous âges utilisant Internet régulièrement (section 3). Finalement, nous avons effectué une recherche juridique au Canada, aux États-Unis et en Union européenne sur les normes encadrant les informations pouvant être recueillies dans le cadre de la PCL (section 4).

Pour nous éclairer dans notre analyse, nous avons également réalisé des entrevues avec des experts en marketing, en nouvelles technologies et en protection de la vie privée. Nous avons ainsi interviewé Manon Arcand, professeure en marketing à l'UQAM, Stéphane Gauvin, professeur en marketing à l'Université Laval, Éloïse Gratton, avocate associée et Cochef National, groupe de pratique Respect de la vie privée chez Borden Ladner Gervais LLP, Jacques Nantel, professeur en marketing à HEC Montréal, Pierrot Péladeau, expert en évaluation sociale de systèmes d'information, Alexandre Sagala, vice-président chez Publipage, Jacques St Amant, chargé de cours en droit de la consommation à l'UQAM et Nicolas Vermeys, professeur à la Faculté de droit de l'Université de Montréal.

[4] Voir notamment : Janet LO, *A "Do Not Track List" for Canada?*, rapport présenté au Bureau de la consommation d'Industrie Canada par le CDIP, 2009; Mary FOSTER, Tina WEST, Avner LEVIN, *The Next Frontier: Targeted Online Advertsing and Privacy*, rapport présenté au Commissariat à la protection de la vie privée du Canada par l'Université Ryerson, 2011

[5] Pedro GIOVANNI LEON, Blase UR, Yang WANG, Manya SLEEPER, et al., « What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers », *Proceedings of the Ninth Symposium on Usable Privacy and Security*, article No. 7, 2013

1. Quelques notes sur le fonctionnement de la PCL

Le déploiement de bannières, de fenêtres intruses ou d'autres promotions sur Internet paraît chose bien triviale. Pour les internautes, la publicité n'est généralement qu'une marque sans intérêt du paysage virtuel. Pourtant, nombre de ces annonces cachent une mécanique complexe, impliquant une multitude d'acteurs et s'articulant en quelques fractions de seconde lorsqu'un internaute se transporte d'une page web à une autre.

1.1. Définition

Schématiquement, le fonctionnement de la PCL est simple : en pistant un internaute sur les sites qu'il consulte, des entreprises colligent ses activités de navigation, telles que les pages qu'il visite, le temps qu'il y passe, les requêtes de recherche et les achats qu'il effectue[6]. Ces données sont ensuite traitées par des algorithmes qui permettent aux publicitaires de deviner ses préférences, ses intérêts ou ses appétences. Le profil qui en résulte servira à présenter à l'internaute des publicités ciblées[7]. Ainsi, l'amateur de science-fiction verra s'afficher des publicités du dernier coffret DVD de David Cronenberg; le passionné de physique, des annonces sur les ouvrages d'Albert Einstein.

Le profil constitué sur les activités d'un internaute ne comportera pas nécessairement son nom, ses coordonnées ou des identifiants précis. L'internaute peut être identifié « pseudonymement », c'est-à-dire en ayant recours à diverses informations telles que le numéro d'un cookie, une adresse IP ou un identifiant unique d'appareil. En ceci, c'est plus souvent le fureteur ou l'appareil qu'un internaute utilise qui fait, à proprement parler, l'objet d'un suivi. L'objectif ultime du publicitaire n'est pas en soi d'identifier un consommateur, mais simplement de lui présenter la publicité la plus pertinente possible : toutefois, la quantité d'informations recueillies permettrait généralement d'identifier assez aisément la personne qui fait l'objet du profilage dans le cadre de la PCL[8].

La théorie distingue, aux côtés de la PCL, d'autres formes de publicités en ligne. Celles-ci sont désignées sous différents vocables. Par exemple, on qualifie de « contextuelle » la publicité affichée en fonction de la page où se trouve l'internaute; une annonce, par exemple, pour du lave-glace sur un site de voitures. La publicité « socio-démographique » cible les internautes en fonction de leur âge, leur sexe, ou tout autre critère démographique. La publicité dite « géolocalisée » s'adapte en fonction du lieu où se trouve le consommateur.

[6] Janet LO, *A "Do Not Track List" for Canada?*, rapport présenté au Bureau de la consommation d'Industrie Canada par le CDIP, 2009, p. 20

[7] Julia ZUKINA, « Accountability in a Smoke-Filled Room: The Inadequacy of Self Regulation Within the Internet Behavioral Advertising Industry », (2012) 7 *Brook. J. Corp. Fin. & Com. L.* 277, p. 278; Qi ZHAO, Yi ZHANG, Lucian VLAD LITA, « Have Your Cake and Eat It Too! Preserving Privacy while Achievig High Behavorial Targeting Performance », in *ADKDD '12 Proceedings of the Sixth International Workshop on Data Mining for Online Advertising and Internet Economy*, Article No. 6, 2012

[8] Nous reviendrons sur cet aspect à la section 4.1

En pratique, les distinctions entre ces divers types de publicité en ligne demeurent fort diffuses. Les entreprises ont pour pratique d'amalgamer bien des types de renseignements pour mieux cibler les consommateurs – et non seulement des renseignements issus *stricto sensu* du suivi de leurs activités sur la toile. Par exemple, les politiques de confidentialité de Google et de Facebook les autorisent à combiner des données comportementales avec d'autres types de renseignements, tels que des données démographiques ou la géolocalisation[9].

Compte tenu de ce mélange des genres, nous considérerons, dans le présent rapport, que toute publicité impliquant le suivi de l'activité du consommateur dans le temps, en combinaison ou non avec d'autres renseignements sur celui-ci, constitue de la PCL. Ce suivi peut être effectué autant directement par le site que l'internaute consulte que par un tiers-partie partenaire avec ce site. En conséquence, notre définition pourra inclure des pratiques qui ne sont pas toujours considérées comme étant de la PCL dans la littérature, telles que le profilage pour des fins publicitaires effectué par les médias sociaux[10].

1.2. Une industrie invisible

L'industrie de la PCL répond à une logique de marché. Les publicitaires[11] demandent de l'espace pour afficher leurs annonces; des sites Internet[12] leur en offrent, moyennant rémunération. En théorie, rien n'empêche un publicitaire d'entrer directement en relation avec un site pour négocier les termes de l'affichage d'annonces, et vice-versa. Cependant, cette approche est peu efficiente dans un univers aussi étiolé que le web, où négocier des ententes publicitaires à la pièce avec des milliers de sites s'avérerait une tâche titanesque, que seuls quelques grands joueurs pourraient relever avec brio.

Les publicitaires et les sites ont donc besoin d'aide pour arrimer l'offre des uns à la demande des autres. Pour ce faire, deux types d'entreprises, les « réseaux publicitaires »[13] et les « échanges publicitaires », agissent comme intermédiaires[14]. Les réseaux publicitaires colligent et mettent en vente les espaces publicitaires offerts par les sites, réalisant du coup une commission sur

[9] Nous verrons plus en détail le contenu de ces politiques à la section 2

[10] Notre définition est effectivement plus large que celle utilisée, par exemple, par Janet Lo, dans : Janet LO, *A "Do Not Track List" for Canada?*, rapport présenté au Bureau de la consommation d'Industrie Canada par le CDIP, 2009, p. 20-21. Dans ce rapport, l'auteure réfère à la définition de la FTC, aux États-Unis, expliquant que sa définition inclut uniquement la collecte par des tiers-parties. *A contrario*, la définition de la PCL qu'on trouve sur Wikipédia est large et inclusive, et se rapproche davantage de notre interprétation, voir : http://en.wikipedia.org/wiki/Behavioral_targeting. Le Commissariat à la protection de la vie privée du Canada (ci-après « CPVP ») demeure aussi assez large dans sa définition de la PCL, voir : CPVP, *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et l'infonuagique*, 2011, p. 14-15

[11] On les appellera également les « annonceurs » ou « acheteurs »

[12] On les appellera également les « éditeurs » ou « vendeurs »

[13] On les appellera également les « régies publicitaires »

[14] Il existe en fait nombre de typologies et de dénominations pour désigner ces divers intervenants, qui varient d'un auteur à l'autre. Voir : Mary FOSTER, Tina WEST, Avner LEVIN, *The Next Frontier: Targeted Online Advertsing and Privacy*, rapport présenté au Commissariat à la protection de la vie privée du Canada par l'Université Ryerson, 2011, p. 8-11

chaque vente d'espace[15]. Les échanges publicitaires offrent un service semblable, mais les emplacements publicitaires y sont plutôt vendus aux enchères, en temps réel et en quelques millièmes de seconde.

Ce sont principalement ces intermédiaires entre les sites Internet et les publicitaires qui rendent possible le suivi et le profilage des internautes. En effet, chaque fois qu'une publicité est affichée sur un site par l'entremise d'un réseau ou d'un échange publicitaire, ce dernier en profite pour recueillir des renseignements sur l'internaute qui voit la publicité. Il enregistre ces renseignements et s'en sert pour dresser le profil de cet internaute; c'est sur la base de ce profil qu'on choisira quelles annonces il est le plus pertinent de lui présenter. Dans certains cas, un acteur peut combiner ces rôles, en offrant en vente des espaces publicitaires et en agissant comme site publiant des annonces. Par exemple, Facebook recueille elle-même les renseignements de ses utilisateurs afin de cibler les annonces des publicitaires qui souhaitent promouvoir leurs produits sur cette plate-forme.

Puisque la plupart des sites d'importance ont des partenariats avec plusieurs intermédiaires à la fois[16], les données de navigation d'un internaute peuvent être expédiées à plusieurs tiers-parties chaque fois qu'il se transporte d'une page de la toile à une autre[17]. Parallèlement, comme ces intermédiaires ont également des partenariats avec de nombreux sites, ils seront en mesure de pister un internaute en bien des recoins de la toile. Cela leur permettra aussi de faire paraître les publicités ciblées sur des sites qui n'ont pas nécessairement de lien avec les produits annoncés.

À ce corpus déjà complexe de sites, d'annonceurs et de tiers-parties se greffe une myriade d'autres entreprises qui se spécialisent dans des rôles précis dans le cadre de la PCL tels que le reciblage publicitaire[18], l'exploration de données[19] ou l'optimisation du ciblage. D'autres offrent des services connexes, tels que l'évaluation du placement des publicités, de façon à s'assurer que l'argent des annonceurs est judicieusement dépensé[20]. D'autres encore offrent aux sites ou aux publicitaires des interfaces leur permettant de vendre ou d'acheter des espaces publicitaires *via* plusieurs réseaux publicitaires ou échanges publicitaires à la fois[21].

---

[15] Le lecteur désirant mieux connaître les distinctions entre ces deux types d'intermédiaires trouvera intérêt dans cet article de Nitin Narang : http://www.mediaentertainmentinfo.com/2014/02/5-concept-series-what-is-the-difference-between-ad-exchange-and-ad-network.html/

[16] Par exemple, en 2009, le CDIP mentionnait que Yahoo! Canada avait des relations avec près de 50 réseaux publicitaires. Voir : Janet LO, *A "Do Not Track List" for Canada?*, rapport présenté au Bureau de la consommation d'Industrie Canada par le CDIP, 2009, p. 26-27. Aux États-Unis, le rapport *KnowPrivacy*, publié en 2009, révélait éloquemment l'ampleur de la collecte d'information sur les utilisateurs des plus importants sites américains. Voir : Joshua GOMEZ, Travis PINNICK, Ashkan SOLTANI, *KnowPrivacy*, UC Berkeley, School of Information, 2009

[17] Une simple session de navigation avec l'extension Ghostery, qui sert à identifier les cookies enregistrés sur le fureteur d'un internaute, permet de constater la quantité impressionnante de mouchards publicitaires de tiers-parties. On trouve parmi ceux-ci des noms tels que AdGear, AppNexus, ADTECH, Datalogix ou DoubleClick.

[18] Le « reciblage publicitaire », ou « *remarketing* », vise à rejoindre des consommateurs qui se sont montrés intéressés à acheter un produit, par exemple en naviguant jusqu'à la page d'achat de ce produit, mais qui n'ont finalement pas fait l'achat en question.

[19] CPVP, *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et l'infonuagique*, 2011, p. 30

[20] Par exemple, AdExpose, société appartenant à ComScore, est un joueur qui offre ce service.

[21] Pour faciliter les choses pour chaque partie, ces entreprises permettent aux annonceurs et aux sites d'accéder à l'offre ou à la demande de plusieurs plateformes à la fois. On nomme ces entreprises « *demand-side platform* » (DSP) lorsqu'elles offrent des services aux publicitaires et « *supply-side platform* » (SSP) lorsqu'elles s'adressent aux sites.

Compte tenu de la quantité d'acteurs présents et du nombre d'activités qu'ils peuvent y exercer, il demeure difficile de cerner les pourtours et les ramifications exacts de l'industrie de la PCL[22]. D'une part, une myriade d'acteurs peut traiter les données d'un internaute ou fournir des services en lien avec la PCL[23]. D'autre part, plusieurs de ces entreprises cumulent plusieurs rôles à la fois; par exemple, Google fournit des services aux internautes tout en opérant comme réseau publicitaire.

Cette multiplicité des acteurs et des rôles ne devrait toutefois pas occulter le fait qu'il s'agit d'une industrie qui, au cours des dernières années, a connu simultanément une forte concentration et une augmentation phénoménale de ses revenus. Un petit nombre d'intermédiaires ont été en mesure de s'accaparer une part importante du marché publicitaire en ligne; en l'absence de concurrence, leurs annonces peuvent désormais apparaître sur encore plus de sites, leur permettant du coup d'effectuer le suivi sur de très grandes portions de l'Internet[24]. Parallèlement, au cours de la dernière décennie, soit de 2003 à 2013, les revenus de publicité en ligne au Canada sont passés de 364 millions à plus de 3,5 milliards de dollars; selon le Bureau de la publicité interactive du Canada, Internet est d'ailleurs devenu le média pour lequel les revenus publicitaires sont les plus importants au pays[25]. Certes, l'industrie publicitaire en ligne est invisible et complexe; cela n'empêche qu'il s'y transige des sommes importantes entre quelques acteurs privilégiés.

1.3. Une mécanique inextricable

Plusieurs technologies permettent aux entreprises de pister les internautes sur la toile. Le plus souvent, elles recourent à un « *cookie*[26] », soit un petit fichier enregistré sur l'ordinateur d'un

[22] Même le CPVP, lors de ses consultations sur la PCL en 2011, affirmait ne pas avoir été en mesure d'obtenir un portrait complet de l'environnement de la PCL au Canada. Voir : CPVP, *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et l'infonuagique*, 2011, p. 34

[23] Pour donner une idée de la complexité de ce système publicitaire, IAB Canada en brosse un portrait sous forme de schéma : http://iabcanada.com/files/IABCanada-Le_paysage_canadien_de_la_programmatique.pdf. Ce schéma, apparemment incomplet et limité au contexte canadien, s'inspire de celui de la firme LUMA Partners, aux États-Unis, qui donne une vue d'ensemble encore plus détaillée des interactions et de la complexité de cette industrie : http://www.lumapartners.com/resource-center/lumascapes-2/

[24] Les chiffres du Bureau de la publicité interactive du Canada mentionnent ainsi que les 20 joueurs les plus importants du marché publicitaire en ligne au Canada s'accaparent, en 2013, 89 % des revenus. Voir : Bureau de la publicité interactive du Canada, *Canadian Internet Advertising Revenue Survey*, 2014, p. 10. L'événement marquant de ce phénomène de concentration aura probablement été l'achat du réseau publicitaire DoubleClick par Google en 2007. Au Canada, à la suite de cette transaction, la Clinique d'intérêt public et de politique d'internet du Canada (CIPPIC) a notamment porté plainte au Bureau de la concurrence alléguant que cet achat entraverait la compétition dans le marché publicitaire en ligne, mais ses arguments n'ont pas été retenus par le Bureau. Voir : Janet LO, *A "Do Not Track List" for Canada?*, rapport présenté au Bureau de la consommation d'Industrie Canada par le CDIP, 2009, p. 28-31

[25] Ces revenus représenteraient 28 % des dépenses publicitaires au pays. En comparaison, les revenus de publicité dans les quotidiens imprimés sont passés, dans le même intervalle, de 2,6 milliards de dollars à 1,7 milliards de dollars; quant aux revenus générés en télévision et en radio, ils sont restés sensiblement stables. Voir : Bureau de la publicité interactive du Canada, *Canadian Internet Advertising Revenue Survey*, 2014, p. 16

[26] On emploiera également l'expression « témoin », « témoin de navigation » ou « mouchard ».

internaute qui visite une page web. Généralement, un cookie contient un identifiant unique qui permet au réseau publicitaire ou à l'échange publicitaire de reconnaître un internaute sur les différents sites qu'il visite. Certains cookies, dits « persistants », sont également programmés pour demeurer indéfiniment dans l'ordinateur de l'internaute, sans s'autodétruire. Cela permet aux entreprises d'identifier de manière permanente le profil virtuel d'un internaute et de lui attribuer continuellement les données qu'elles colligent sur ses activités en ligne.

Puisque le suivi en ligne repose sur l'utilisation de cookies, une stratégie instinctive pour s'en défaire serait tout simplement de configurer le fureteur de façon à ce qu'il en refuse l'installation, ou du moins qu'il les supprime automatiquement à la fin de chaque session de navigation. Cependant, cette méthode ne donnera pas forcément les résultats escomptés. D'une part, les cookies ne servent pas seulement à réguler les systèmes publicitaires; ces petits fichiers rendent nombre de services aux internautes, et les refuser peut grandement perturber l'expérience de navigation[27]. D'autre part, le cookie n'est pas la seule technologie utilisée par les entreprises pour pister les internautes, loin s'en faut : en conséquence, les bloquer ou les supprimer ne permettra pas de mettre fin complètement au suivi en ligne.

En effet, aux côtés des cookies usuels, les entreprises déploient un arsenal de moyens technologiques pour s'assurer d'être en mesure de pister les internautes quelle que soit la configuration de leur fureteur ou de leur appareil[28]. On compte parmi ces moyens : les « témoins Flash », qui s'installent sur l'ordinateur d'un internaute *via* le module d'extension mis au point par la société Adobe pour la lecture de fichiers multimédias; les « supertémoins », qui utilisent de nouveaux emplacements de mémoire intégrés aux navigateurs afin d'enregistrer des renseignements sur un utilisateur; ou encore les « pixels invisibles », c'est-à-dire de petits fichiers image qui, lorsque téléchargés par le fureteur, permettent de retrouver la trace de l'internaute[29]. On peut aussi, pour pister un internaute, utiliser son adresse IP ou l'identifiant unique de son appareil. Des auteurs évoquent même la possibilité de recourir à l'« empreinte digitale » des fureteurs[30] ou à l'inspection approfondie de paquets[31].

---

[27] Les cookies permettent en effet de retenir des informations sur un internaute d'une page web à une autre, ce qui rend possible toutes sortes de fonctionnalités, telles que le magasinage en ligne.

[28] Pour un portrait de ces technologies, voir notamment : CPVP, *Les témoins sous la loupe*, 2011, en ligne : https://www.priv.gc.ca/resource/fs-fi/02_05_d_49_01_f.asp; Janet LO, *A "Do Not Track List" for Canada?*, rapport présenté au Bureau de la consommation d'Industrie Canada par le CDIP, 2009, p. 20-47

[29] Cette technologie peut être désignée sous différents vocables, tels que « balise web » ou « pixel espion ». On pourra trouver plus d'information sur son fonctionnement sur une page de l'Electronic Frontier Foundation, *The Web Bug FAQ*, en ligne : https://w2.eff.org/Privacy/Marketing/web_bug.html

[30] L'empreinte digitale d'un fureteur ou d'un appareil consiste en une méthode d'identification (complète ou partielle) se basant sur la configuration d'un appareil. Elle peut donc être utilisée même lorsque les cookies sont désactivés. En 2010, une étude de l'Electronic Frontier Foundation indiquait que cette méthode d'identification peut atteindre un important niveau de précision. Voir : Peter ECKERSLEY, *How Unique Is Your Web Browser?*, Electronic Frontier Foundation, 2010

[31] L'inspection approfondie des paquets consiste en la lecture, par un fournisseur de services de télécommunications, des transmissions qui passent par son réseau. Voir : CPVP, *Qu'est-ce que l'inspection approfondie de paquets?*, en ligne : https://www.priv.gc.ca/information/research-recherche/dpi_intro_f.asp. À notre connaissance, l'inspection approfondie des paquets n'est pas actuellement utilisée à des fins publicitaires au Canada. Cependant, les modifications récentes à la politique de confidentialité de Bell Canada, qui l'autorisent à utiliser un grand nombre de données sur l'activité de ses clients pour des fins publicitaires, peut soulever des doutes à cet égard. Voir : Philippe MERCURE, « Renseignement personnels : Bell s'attire les critiques », *La Presse*, Montréal, 22 octobre 2013

En somme, compte tenu qu'un grand nombre d'entreprises pistent les internautes, et que chacune d'entre elles peut utiliser concurremment un nombre considérable de technologies pour ce faire, il est en pratique fort difficile d'échapper au suivi en ligne.

Bien sûr, certaines de ces entreprises proposent aux internautes, sur leurs sites Internet respectifs, des options leur permettant de demander de mettre fin au suivi qu'elles effectuent ou de retirer des catégories d'intérêts affublées à leur profil virtuel (voir section 2). Or, le recours à ces divers mécanismes dépareillés pour éluder le suivi en ligne laisse perplexe. Entre autres difficultés, cela demandera d'abord à un internaute d'identifier les nombreuses entreprises qui le pistent en ligne, lesquelles lui sont pour la plupart inconnues. Cela lui demandera aussi de souscrire à chacun des mécanismes de retrait offerts par celles-ci, un par un – une tâche fastidieuse pour un internaute profane. C'est sans compter que rien ne garantit l'efficacité de ces options de retrait, ni que cet exercice pourra couvrir l'ensemble des entreprises qui le pistent en ligne.

Face à ces écueils, l'Alliance de la publicité numérique du Canada (APNC) a développé une solution plus réaliste pour les internautes. Le Programme canadien d'autoréglementation pour la publicité comportementale en ligne, un code volontaire qu'elle a élaboré, prévoit l'inclusion d'une icône *AdChoices* (voir Figure 1) aux côtés des publicités comportementales diffusées par les entreprises participantes. En cliquant sur cette icône ou en se rendant sur le site de l'APNC, un internaute peut accéder à une page où, promet-on, il pourra refuser en bloc que les entreprises participantes suivent son activité en ligne pour des fins publicitaires[32].

Figure 1 : Icône *Adchoices*

Certes commode, cette option offerte par l'industrie demeure perfectible[33]. D'emblée, rappelons qu'il s'agit d'une norme volontaire dont la mise en œuvre repose sur le bon vouloir des seuls adhérents au Programme[34]. Ajoutons que les entreprises participantes sont autorisées,

[32] http://youradchoices.ca/fr/retrait

[33] Nous verrons également, dans la section 3, qu'il s'agit d'un mécanisme par *opt-out* peu connu des consommateurs. Dans bien des cas, ceux-ci continuent de faire l'objet du suivi en ligne en ignorant leur droit de retirer leur consentement.

[34] Aux États-Unis, par exemple, l'étude *Tracking the trackers* du Center for Internet and Society de la Stanford Law School révélait, en 2011, que certaines entreprises n'arrêtaient pas le suivi des consommateurs même après que ceux-ci aient utilisé le formulaire de retrait du suivi en ligne offert par une association de l'industrie : http://cyberlaw.stanford.edu/blog/2011/07/tracking-trackers-early-results. Voir aussi : Pedro GIOVANNI LEON, Blase UR, Yang WANG, Manya SLEEPER, et al., « What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers », *Proceedings of the Ninth Symposium on Usable Privacy and Security*, article No. 7, 2013, p. 2

sous divers motifs, à poursuivre le suivi des consommateurs ayant souscrit au mécanisme, par exemple pour compter le nombre de fois qu'une publicité a été présentée dans un fureteur[35]. De même, elles demeurent aussi autorisées à utiliser certains types de renseignements pour des fins publicitaires, tels que des informations « démographiques » ou « de localisation »[36]. Finalement, les assises technologiques de ce mécanisme, qui fonctionne par l'installation d'un cookie sur l'appareil de l'internaute, posent des difficultés quant à la durabilité du choix effectué par le consommateur[37].

Bref, même si un internaute se prévaut des mécanismes de refus offerts par l'industrie, il pourra subsister des brèches dans son anonymat en ligne. Pour les combler, les plus chevronnés pourront encore tenter quelques autres astuces. Entre autres, ils peuvent activer le paramétrage « *Do Not Track* » de leur fureteur, qui envoie un signal aux serveurs publicitaires comme quoi l'utilisateur ne souhaite pas être pisté[38]; cependant, comme nous le verrons plus loin, bien des entreprises ne respectent pas ce signal[39]. Ou encore, ils peuvent installer dans leur fureteur des logiciels tels que AdBlock Plus ou Ghostery, qui permettent soit de bloquer l'affichage des publicités, soit de bloquer certains cookies; cependant, ces logiciels ne permettent pas nécessairement de mettre fin au suivi en ligne sous-jacent.

Les internautes peuvent donc déployer divers moyens pour éluder le suivi en ligne, mais ceux-ci risquent généralement de ne s'avérer que partiellement efficaces. De plus, ces divers moyens demeurent fort mal connus du public, sont inactifs par défaut (et requièrent donc une action positive des utilisateurs qui veulent s'en prévaloir) et nécessitent parfois des connaissances techniques avancées pour être mis en œuvre.

[35] http://youradchoices.ca/fr/fr-faq

[36] http://youradchoices.ca/fr/fr-faq

[37] En effet, le mécanisme de retrait repose sur l'installation d'un cookie persistant, lequel pourrait facilement disparaître lors d'une reconfiguration du fureteur.

[38] Ce signal est une initiative du World Wide Web Consortium, un organisme de normalisation du web à but non lucratif : http://www.w3.org/2011/tracking-protection/drafts/tracking-dnt.html. Il ne faut pas confondre le signal *Do Not Track* avec le mode de navigation privée offert par certains fureteurs, lequel, de l'aveu même des développeurs de Firefox, ne garantit pas l'anonymat en ligne : https://support.mozilla.org/fr/kb/navigation-privee-naviguer-sans-conserver-infos-sites. Il faut également se garder de confondre ce signal avec la « *Do Not Track List* », c'est-à-dire un mécanisme de retrait basé sur une liste centralisée de personnes ne souhaitant pas faire l'objet de suivi s'apparentant à la liste nationale de numéros de télécommunication exclus, et dont la mise en œuvre a été soutenue par plusieurs organismes de défense des consommateurs aux États-Unis.

[39] À cet effet, voir aussi : Pedro GIOVANNI LEON, Blase UR, Yang WANG, Manya SLEEPER, et al., « What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers », *Proceedings of the Ninth Symposium on Usable Privacy and Security*, article No. 7, 2013, p. 2

2. Analyse des politiques de protection de la vie privée

Pour en savoir davantage sur les pratiques des entreprises en ligne au Canada, sur les renseignements qu'elles recueillent et sur ce qu'elles en font, nous avons analysé les politiques de confidentialité des plus importants fournisseurs de services sans frais sur Internet au pays.

Nous avons défini un « service sans frais sur Internet » comme étant un service offert aux internautes dont l'accès aux principales caractéristiques n'a pas de coût monétaire pour l'utilisateur, et dont au moins une partie du modèle d'affaires repose sur la PCL telle que définie dans le présent rapport[40]. Cela inclut autant les engins de recherche, tels que Google, que les médias sociaux, tels que Facebook. Cela peut aussi inclure tout site offrant du contenu gratuitement aux internautes, tel qu'un site d'actualités ou un site offrant des vidéos en ligne. Les sites fonctionnant sous une formule « *freemium* », c'est-à-dire qui combinent un accès payant et un accès gratuit (par exemple : LinkedIn), peuvent aussi être inclus dans cette définition dans la mesure où ils effectuent également de la PCL.

Pour établir notre échantillon, nous avons sélectionné, parmi les sites les plus consultés par les Canadiens, ceux qui correspondent à cette définition de fournisseur de service sans frais[41]. Nous avons rapidement constaté que, sauf exception[42], la plupart des sites les plus populaires au Canada ont adopté un modèle d'affaires faisant appel à la PCL. De même, plusieurs de ces sites appartiennent à une même entreprise et dirigent les consommateurs vers une même politique de confidentialité. Par exemple, le site YouTube, qui appartient à Google, réfère à la même politique que le moteur de recherche Google et le service de courriel Gmail. Pour éviter les doublons, nous avons considéré la politique utilisée par plusieurs entreprises comme une seule composante de notre échantillon.

Finalement, nous avons analysé les politiques des dix entreprises suivantes : Google[43], Facebook[44], Microsoft[45], Yahoo![46], LinkedIn[47], Twitter[48], Kijiji[49], Amazon[50], Pinterest[51], Imgur[52].

---

[40] Cette définition est inspirée de celle que l'on retrouve dans Kent SEBASTIAN, *Un repas gratuit, ça n'existe pas : les contrats de consommation et les services « gratuits »*, rapport présenté au Bureau de le consommation d'Industrie Canada par le CDIP, 2014, qui définit un service gratuit comme « un service en ligne gratuit qui monétise la valeur fournie par les utilisateurs ».

[41] Pour ce faire, nous avons recouru aux données de eMarketer et celles du classement Alexa, qui obtiennent des résultats similaires. Voir: eMarketer, *Top 10 Websites Among Internet Users in Canada, Ranked by Market Share of Visits*, juin 2014; http://www.alexa.com/topsites/countries/CA. D'aucuns pourraient arguer que, puisque que ce sont souvent des tiers-parties qui recueillent et utilisent les renseignements des internautes dans le cadre de la PCL, il eût été préférable d'étudier directement les pratiques de ces entreprises. Cependant, nous avons considéré que notre approche nous permettait véritablement de nous placer dans la position du consommateur qui cherche à obtenir de l'information, et qui ne connaît pas d'emblée l'existence des tiers-parties. Quoi qu'il en soit, les entreprises qui ont été retenues dans notre échantillon cumulent généralement plusieurs rôles et mentionnent effectuer un suivi des activités comportementales de l'utilisateur.

[42] Exception notable, Wikipédia se trouve en cinquième position du classement, mais ne présente pas de publicité en ligne. Son modèle d'affaires repose essentiellement sur un financement participatif.

[43] La politique de Google couvre autant les activités de l'engin de recherche que celles des autres services de cette entreprise, tels que YouTube et Gmail. Nous avons consulté la politique de Google datée du 19 décembre 2014, disponible à cette adresse : https://www.google.ca/intl/fr/policies/. Il s'agit d'une section du site de Google qui contient de nombreuses pages explicatives sur les pratiques de cette entreprise, dont la plus importante s'intitule « Politique de confidentialité ». On y trouve aussi d'autres pages pertinentes, dont : « Technologies et principes », « FAQ » et « Conditions d'utilisation ».

Comme il s'agit d'une industrie concentrée, nous avons limité notre échantillon à dix politiques. En effet, selon le Bureau de la publicité interactive du Canada (IAB Canada), les dix principaux joueurs de la publicité Internet ont généré 82 % des revenus totaux de la publicité Internet au Canada en 2013[53]. Bien que le rapport du Bureau n'indique pas quelles sont ces entreprises, on se doutera que Google et Facebook occupent une place prépondérante dans ce classement. Un

[44] Nous avons étudié deux versions de la politique de Facebook. Nous avons essentiellement basé notre analyse sur la plus récente, datée du 30 janvier 2015, qu'on trouve à cette adresse : https://www.facebook.com/about/privacy/. Nous avons de plus consulté des pages connexes telles que « Contrôles publicitaires », « Politique d'utilisation des cookies » et les conditions d'utilisation du service. Nous avons également étudié la version antérieure de cette politique, datée du 15 novembre 2013.

[45] Plusieurs services gravitent dans le giron de Microsoft, dont Windows Live Mail, live.com, Bing et MSN Canada. Ceux-ci se rapportent à la « Déclaration de confidentialité Microsoft », datée de janvier 2015, qu'on trouve à cette adresse : http://www.microsoft.com/privacystatement/fr-ca/core/default.aspx. Cependant, les services Bing et MSN réfèrent à une politique distincte : « Déclaration de confidentialité Bing et MSN », datée de janvier 2015 et disponible à cette adresse : http://www.microsoft.com/privacystatement/fr-fr/bingandmsn/default.aspx. Ces deux documents contiennent moult détails et pointent occasionnellement vers d'autres pages, dont une page de retrait de la PCL générale de Microsoft et la politique de protection de la vie privée de Microsoft Advertising, le réseau publicitaire exploité par Microsoft. Malgré ces distinctions, nous avons analysé tous les services de Microsoft de manière concurrente, en faisant les nuances qui s'imposaient, lorsque nécessaire.

[46] Yahoo! Canada dispose d'une politique générale pour tous ses services. Fort brève, cette politique, datée du 12 juillet 2010, est disponible à cette adresse : http://info.yahoo.com/privacy/ca/yahoo/. Yahoo! Mail a aussi une courte politique distincte, qui réfère à la politique générale de Yahoo! pour plus de détails : http://info.yahoo.com/privacy/ca/yahoo/mail/ymail/details.html. On trouve quelques pages complémentaires qui définissent certains termes employés, de même qu'un lien vers la page de retrait de la PCL de Yahoo! Les conditions d'utilisation sont publiées à cette adresse : https://info.yahoo.com/legal/ca/yahoo/utos/utos-ca01.html.

[47] Nous avons consulté la politique de LinkedIn, datée du 23 octobre 2014, figurant à cette adresse : https://www.linkedin.com/legal/privacy-policy. Nous avons également consulté les conditions d'utilisation de ce service à cette adresse : https://www.linkedin.com/legal/user-agreement.

[48] Nous avons consulté la politique de Twitter, datée du 8 septembre 2014, à cette adresse : https://twitter.com/privacy. Twitter met aussi à la disposition de ses utilisateurs des pages complémentaires abordant des sujets connexes tels que « Utilisation des cookies et des technologies similaires par Twitter » ou « Vos paramètres de confidentialité en matière de publicités personnalisées ». Les conditions d'utilisation, datées du 8 septembre 2014, sont publiées à cette adresse : https://twitter.com/tos.

[49] Nous avons consulté la politique de Kijiji, datée du 25 juillet 2014, figurant à cette adresse : http://aide.kijiji.ca/centredaide/politiques/politique-de-confidentialite. Les conditions d'utilisation sont disponibles à cette adresse : http://aide.kijiji.ca/centredaide/politiques/conditions-d-utilisation.

[50] Nous avons consulté la politique d'Amazon, datée du 3 mars 2014, figurant à cette adresse : http://www.amazon.ca/gp/help/customer/display.html/180-9291331-5703514?nodeId=918814. Une page spécifique traite des pratiques d'Amazon en matière de PCL : https://www.amazon.ca/gp/BIT/InternetBasedAds. Les conditions d'utilisation, datées du 17 décembre 2012, sont disponibles à cette adresse : https://www.amazon.ca/gp/help/customer/display.html?nodeId=918816.

[51] Nous avons consulté la politique de Pinterest, datée du 19 octobre 2014, figurant à cette adresse : https://about.pinterest.com/fr/privacy-policy-0. On trouve aussi des pages complémentaires, entre autres « Personnalisation et données issues d'autres sites Web » et « Informations que les annonceurs partagent avec Pinterest ou qu'ils collectent sur Pinterest ». Les conditions d'utilisation sont disponibles à cette adresse : https://about.pinterest.com/fr/terms-service. Notre dernière consultation de cette page remonte au 9 janvier 2015.

[52] Nous avons consulté la très courte politique de Imgur, datée du 14 janvier 2014, à cette adresse : http://imgur.com/privacy. Les conditions d'utilisation, datées du 22 octobre 2014, sont disponibles à cette adresse : http://imgur.com/tos.

[53] Bureau de la publicité interactive du Canada, *Résultats 2013 + estimation 2014 : Enquête sur les revenus de la publicité Internet au Canada*, Enquête menée par Ernst & Young et commanditée par le Bureau de la publicité interactive du Canada, 17 septembre 2014, p. 10

regard sur le marché américain suffit d'ailleurs à s'en convaincre : selon eMarketer, Google trône au sommet avec 38,1 % des revenus publicitaires Internet aux États-Unis en 2014; Facebook suit avec une part de 9,8 %[54]. C'est dire que Google et Facebook représenteraient à eux seuls, aux États-Unis, près de la moitié du marché publicitaire en ligne. Puisque le marché canadien présente des caractéristiques similaires au marché américain, on peut réalistement suggérer qu'on y retrouve un partage des revenus en des proportions semblables; d'ailleurs, ce sont aussi ces entreprises qui y obtiennent le plus grand nombre de visites des internautes.

2.1. Des documents épars

Nous avons généralement retrouvé les liens vers les politiques de confidentialité des services sélectionnés dans des mentions discrètes en bas de page. Malgré que certaines politiques se présentent dans un verbiage lourd et difficile à comprendre, d'autres adoptent une forme et un langage plus accessibles : c'est le cas des politiques de Google et de Facebook, dans lesquelles les efforts pour vulgariser les pratiques et présenter clairement l'information sont perceptibles. Par exemple, Facebook, qui a pris soin d'inclure une icône pointant vers des raccourcis sur la protection de la vie privée dans sa barre de navigation, présente les informations destinées aux utilisateurs sous une forme généralement conviviale.

Le plus souvent, l'entreprise publie deux documents principaux : un document expliquant les conditions d'utilisation du service[55], et un autre portant sur la politique de gestion des renseignements personnels de l'utilisateur[56]. Parfois, les informations pertinentes sont divisées en rubriques et s'étalent sur plusieurs pages. Par exemple, Amazon rend disponible, aux côtés de sa politique de protection de la vie privée, une page distincte expliquant spécifiquement ce qu'est la publicité ciblée par centres d'intérêts[57]. Dans plusieurs cas, les politiques étudiées disent s'appliquer aussi lorsque l'utilisateur accède au service *via* une application mobile.

Puisque ce qui constitue exactement la politique de confidentialité de chaque service demeure parfois imprécis, nous avons également, lorsque nécessaire, étudié d'autres documents connexes, dont les conditions d'utilisation de ces services, les pages explicatives complémentaires mises à la disposition des internautes, et même les pages d'achat d'espace publicitaire en ligne destinées aux annonceurs.

2.2. Une collecte sans limites

La lecture de ces politiques suffit à s'en convaincre : afin de cibler la publicité, la moindre bribe d'information sur les internautes est colligée par les entreprises étudiées. Rien n'échappe à la collecte, que l'on parle des données obtenues par le suivi des activités des internautes, ou de

[54] eMarketer, *Net US digital Ad Revenues, by Company, 2013-2016*, 2014

[55] On reconnaîtra ces modalités sous différents vocables, tels que « Conditions d'utilisation », « Contrat de services », « Conditions générales » ou « *Terms of Service* »

[56] Encore là, ces documents pourront prendre différents noms, tels que « Politique de confidentialité », « Politique d'utilisation des données » ou « Déclaration de confidentialité »

[57] http://www.amazon.com/b/?&node=5160028011

celles qui ont été obtenues, le cas échéant, lors de l'ouverture d'un compte d'utilisateur par ceux-ci.

D'abord, on recueille les informations sur l'activité de l'internaute. Cela inclut, bien entendu, les pages qu'il visite et le temps qu'il passe sur chacune[58]. On peut aussi enregistrer, entre autres, les vidéos qu'il visionne sur YouTube, les achats qu'il fait en ligne ou les annonces qui suscitent son attention. Bref, tous les clics de l'internaute sont pistés.

Chaque service recueille aussi des données propres aux fonctionnalités qu'il offre. Les moteurs de recherche Google et Bing retiennent les mots clefs recherchés par l'internaute. Sur les médias sociaux, on s'intéresse aux mentions « J'aime » (ou « +1 » chez Google), aux commentaires et au contenu partagés par l'utilisateur. Les plateformes d'achat en ligne ne sont pas en reste : par exemple, la politique d'Amazon laisse entendre que la liste d'articles qu'un consommateur souhaite se procurer pourra être utilisée pour des fins publicitaires.

On s'intéresse également aux relations entre leurs utilisateurs d'un service, en cherchant à deviner le type de relations qu'un internaute entretient avec chacun de ses contacts. Facebook, incontournable lieu de socialisation en ligne, explique en ces termes cette pratique :

> « Nous recueillons des informations sur les personnes et les groupes avec lesquels vous êtes en contact, ainsi que la manière dont vous interagissez avec eux (par exemple, les personnes avec qui vous communiquez le plus ou encore les groupes au sein desquels vous aimez vous exprimer).[59] »

Même la correspondance des internautes peut servir au ciblage, à l'aide d'algorithmes qui en retiendront certains mots-clefs ou d'autres éléments. Yahoo! l'explique comme suit :

> « *When you use Yahoo! Mail, our automated systems scan and analyze your communications and also the content sent and received from your account to detect, among other things, certain words and phrases (we call them "keywords") within these communications. In addition to using the keywords to show you contextually relevant content and ads, these keywords may also contribute to our understanding of things that interest you.*[60] »

Le lieu où se trouve le consommateur est aussi une information prisée[61]. Pour découvrir cette information, les entreprises peuvent déployer un arsenal de moyens. Google, par exemple, en mentionne une liste non exhaustive :

---

[58] On explique souvent en des termes larges la collecte des activités de navigation de l'utilisateur. Par exemple, Google adopte une définition très large du concept de « Données que nous recueillons lors de votre utilisation de nos services », en y incluant les « renseignements sur les services que vous utilisez et la manière dont vous les utilisez, comme lorsque vous regardez une vidéo sur YouTube, que vous visitez un site Web qui utilise nos services de publicité ou que vous interagissez avec nos annonces et notre contenu ». Chez Twitter, on affirme encore plus généralement s'intéresser à « la façon dont vous interagissez avec les liens dans nos Services ».

[59] https://www.facebook.com/about/privacy/update/

[60] http://info.yahoo.com/privacy/ca/yahoo/opt-outfaq/

[61] Nous avons trouvé des mentions explicites quant à la collecte d'informations liées à la localisation dans sept des dix politiques analysées : Amazon, Facebook, Google, LinkedIn, Microsoft, Pinterest, Twitter. Dans les trois autres politiques (Yahoo!, Kijiji, Imgur), il n'est pas exclu, compte tenu de la généralité des termes des politiques, que la

> « Lorsque vous utilisez les services de Google, nous pouvons recueillir et traiter de l'information sur votre position réelle. Nous utilisons diverses technologies pour déterminer la position, y compris l'adresse IP, les données GPS et d'autres capteurs qui peuvent, par exemple, fournir à Google des renseignements sur les appareils, les points d'accès Wi-Fi et les tours cellulaires à proximité.[62] »

Plusieurs entreprises mentionnent recueillir, entre autres, des données provenant du GPS d'un appareil mobile ou d'un réseau Wi-Fi, des « informations concernant les réseaux sans fil[63] » ou sur des « antennes-relais à proximité de votre appareil mobile[64] ». Dans d'autres cas, il est aussi possible de recourir à l'adresse IP de l'internaute pour deviner l'endroit où il se trouve[65].

Les entreprises peuvent aussi chercher à déduire le lieu où se trouve un consommateur en analysant ses activités en ligne. Par exemple, on pourrait présumer qu'un utilisateur qui recherche des informations sur la tour Eiffel se trouve à Paris[66]. C'est ce que Google nomme des « données de localisation implicites » :

> « Les données de localisation implicites ne nous indiquent pas réellement où se trouve votre appareil, mais nous permettent de déduire que vous êtes intéressé par le lieu ou que vous êtes susceptible de vous y trouver. Une requête de recherche d'un endroit particulier, entrée manuellement, constitue un exemple de données de localisation implicites.[67] »

À toutes ces informations viennent également se greffer une multitude d'autres données techniques. Ainsi, la plupart des collectes de renseignements vues ci-haut sont aussi l'occasion de recueillir des métadonnées, c'est-à-dire des données qui fournissent de l'information sur une autre donnée[68]. Par exemple, lors d'une requête sur un moteur de recherche, on enregistrera

---

localisation du consommateur soit recueillie; certaines d'entre elles mentionnent d'ailleurs recueillir l'adresse IP. Google laisse croire qu'elle peut également colliger l'historique des lieux où s'est trouvé un consommateur pour des fins publicitaires : « Vos informations de localisation peuvent en outre être utilisées par les applications ou les services Google, notamment dans le cadre des annonces affichées. » Voir : https://support.google.com/gmm/answer/3118687?hl=fr&ref_topic=3137371

[62] https://www.google.ca/intl/fr/policies/privacy/

[63] https://twitter.com/privacy?lang=fr

[64] https://twitter.com/privacy?lang=fr

[65] L'adresse IP, un numéro attribué à chaque poste connecté au réseau Internet, peut certes fournir de précieuses indications géographiques, mais un fournisseur de service peut parfois attribuer des adresses IP de secteurs géographiques autres à certains clients. De plus, l'adresse IP d'un poste peut varier au cours d'une même période. Notamment pour ces diverses raisons techniques, la géolocalisation sur la base de l'adresse IP demeure généralement une méthode de localisation plus approximative que celles utilisant les données d'un appareil mobile : un rapport d'IAB Canada explique ainsi que cette méthode de ciblage atteindrait un niveau de précision de 88 % dans un rayon de 40 kilomètres. Voir : IAB CANADA, *Géociblage en ligne*, en ligne : http://iabcanada.com/files/IABCanada_GeociblageEnLigne.pdf

[66] Cet exemple est tiré de la politique de Google.

[67] https://www.google.ca/intl/fr/policies/technologies/location-data/

[68] CPVP, *Métadonnées et vie privée : un aperçu technique et juridique*, octobre 2014, p. 1

non seulement les mots clefs utilisés, mais aussi le moment et le lieu où ceux-ci ont été utilisés[69].

Plus généralement, on peut aussi recueillir diverses données informatiques ou technologiques sur l'appareil utilisé par un internaute : le modèle d'appareil, son identifiant unique[70], le système d'exploitation utilisé, le réseau cellulaire ou même le numéro de téléphone assigné à l'appareil. Google affirme aussi recueillir « des données relatives aux communications téléphoniques, comme votre numéro de téléphone, celui de l'appelant, les numéros de transfert, l'heure et la date des appels, leur durée, les données de routage des textos et les types d'appels[71] ». Facebook ajoute colliger « le niveau de la batterie et l'intensité du signal[72] ». Amazon renchérit :

> « *During some visits we may use software tools such as JavaScript to measure and collect session information, including page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page*.[73] »

C'est dire que même les espaces sur lesquels le curseur de l'internaute se balade ou le défilement d'une page peuvent être enregistrés.

A priori, on penserait qu'une collecte si large de renseignements ne peut s'effectuer que lorsque l'internaute utilise les services de l'entreprise, c'est-à-dire lorsqu'il se trouve sur la plateforme ou les sites Internet de celle-ci. Cependant, certaines entreprises ont aussi l'occasion de suivre ses activités à l'extérieur de leur territoire immédiat. Ainsi, les entreprises exploitant des réseaux publicitaires, dont Google[74], indiquent être en mesure de suivre le consommateur en bien d'autres endroits du web, lorsqu'il visite une des nombreuses pages qui affiche des publicités par leur intermédiaire.

Les médias sociaux ne sont pas en reste. Facebook, par exemple, laisse entendre qu'elle est en mesure d'effectuer un suivi de l'« activité sur les sites web et les applications en dehors de Facebook[75] » lorsque ces sites intègrent les « boutons J'aime ou Se connecter[76] » – ce que l'on nomme les « modules sociaux » dans le jargon virtuel – ou lorsqu'ils font appel à ses services publicitaires. Twitter, de son côté, explique qu'elle pourra recourir aux données de suivi provenant de tiers-parties pour bonifier son ciblage publicitaire :

> « Les partenaires annonceurs tiers nous communiquent des informations, comme les identifiants de cookie relatifs à un navigateur, les URL des sites Web visités, les

[69] On peut également enregistrer un grand nombre d'autres informations contextuelles. Au nombre de ces informations, Google mentionne l'adresse IP, la configuration du navigateur, la situation géographique et tout identificateur unique contenu dans les cookies. Bing mentionne des informations similaires.

[70] L'identifiant unique d'un appareil est une suite de caractères qui permet d'identifier un appareil, tel qu'un téléphone mobile. Un appareil peut avoir plusieurs de ces identifiants pour des fins diverses, dont la publicité.

[71] https://www.google.ca/intl/fr/policies/privacy/

[72] https://www.facebook.com/about/privacy/update/

[73] http://www.amazon.ca/gp/help/customer/display.html/180-9291331-5703514?nodeId=918814

[74] Google exploite notamment les réseaux Google Adworks et DoubleClick.

[75] https://www.facebook.com/about/privacy/update/

[76] https://www.facebook.com/about/privacy/update/

> identifiants d'appareil mobile ou de compte (tels qu'une adresse email) sous forme cryptée, afin de nous aider à mesurer et à personnaliser les publicités. Cela nous permet par exemple d'afficher des publicités relatives à des domaines auxquels vous avez déjà manifesté de l'intérêt.[77] »

Certaines entreprises se réservent aussi la possibilité d'acheter des renseignements auprès d'autres sources. C'est le cas de Microsoft, qui affirme : « on peut obtenir des renseignements supplémentaires vous concernant, telles que des renseignements démographiques que nous achetons auprès d'autres sociétés[78] ».

En somme, la plupart des entreprises étudiées ont des tentacules pouvant s'étendre bien au-delà de la simple orbite de la prestation de leurs services. Elles sont en mesure, par divers moyens, de suivre l'activité de leurs utilisateurs même lorsqu'ils n'utilisent pas leurs services.

2.3. L'étiquetage des consommateurs

Les politiques que nous avons parcourues autorisent les entreprises à traiter les données qu'elles recueillent de toutes les façons possibles pour optimiser le ciblage publicitaire. Aucune d'entre elles ne rattache directement chaque type de renseignement recueilli avec l'utilisation précise qui en sera faite. On opte plutôt pour énoncer une longue liste de renseignements pouvant être recueillis, suivie d'un énoncé général affirmant que toutes ces données pourraient servir à des fins publicitaires. La politique de Facebook l'affirme ainsi sans ambages :

> « Nous voulons que nos publicités soient aussi pertinentes et intéressantes que les autres informations que vous trouvez au sein de nos services. Dans cette optique, nous nous servons de toutes les informations dont nous disposons à votre sujet afin de vous présenter des publicités pertinentes.[79] »

Cela inclut non seulement les données concernant l'activité en ligne du consommateur, mais aussi d'autres renseignements que l'entreprise détient déjà, telles que les informations que l'utilisateur a divulguées lors de l'inscription au service (sexe, âge, emploi). Bref, tout ce qui peut être appris sur le compte d'un internaute peut servir à affubler à son double virtuel des champs d'intérêts.

Ceci étant dit, malgré la largesse des énoncés, notons que beaucoup d'entreprises prennent soin de donner des explications complémentaires ou des exemples concrets à leurs utilisateurs pour démystifier leurs pratiques publicitaires. Plusieurs multiplient les pages connexes explicatives[80] ou parsèment leurs politiques d'exemples concrets, lesquels peuvent s'avérer rafraîchissants au milieu d'une lecture souvent aride. Facebook donne ainsi cette illustration de ses pratiques publicitaires :

---

[77] https://twitter.com/privacy?lang=fr

[78] http://www.microsoft.com/privacystatement/fr-ca/core/default.aspx

[79] https://www.facebook.com/about/privacy/update/

[80] Par exemple, Yahoo! prévoit une « FAQ » explicative pour ses pratiques publicitaires quant à son service de courriel : http://info.yahoo.com/privacy/ca/yahoo/mail/ymailfaq/

> « par exemple, si une personne « aime » la Page « Star Trek » et mentionne « La guerre des étoiles » en indiquant se trouver dans un cinéma, nous pouvons en déduire que cette personne est sûrement un fan de science-fiction et les annonceurs pour des films de science-fiction pourraient nous demander de cibler cette catégorie.[81] »

Des entreprises donnent aussi des illustrations de certaines pratiques plus particulières. Par exemple, Google explique ce qu'est le reciblage publicitaire en ces termes :

> « Des annonces concernant des produits que vous avez consultés précédemment peuvent s'afficher en raison d'un procédé appelé « remarketing ». Supposons que vous consultiez un site Web qui vend des bâtons de golf, mais que vous ne les achetiez pas lors de votre première visite. Le propriétaire du site Web souhaite peut-être vous inciter à revenir et à finaliser votre achat. Nous proposons des services qui permettent aux exploitants de sites Web de cibler les internautes ayant consulté leurs pages.[82] »

Des données provenant de tiers peuvent aussi être croisées avec des données détenues par l'entreprise afin de cibler un groupe de personnes. Twitter l'explique ainsi :

> « Voici un exemple. Imaginons qu'un fleuriste souhaite publier une offre spéciale Saint-Valentin sur Twitter. Il préfère cibler en priorité les amateurs de fleurs abonnés à sa newsletter. Afin de proposer cette offre spéciale aux abonnés qui disposent d'un compte Twitter, la boutique peut nous communiquer un groupe d'adresses email cryptées tirées de sa liste de diffusion. Nous pouvons alors recouper cette liste avec les adresses email cryptées associées aux comptes de nos utilisateurs, afin de leur proposer un Tweet sponsorisé contenant l'offre spéciale Saint-Valentin.[83] »

Cependant, malgré ces quelques exemples épars, force est de constater qu'on s'en tient à des généralités. Si on sait que les données des consommateurs seront recueillies et serviront à affubler à leur profil des centres d'intérêt, on comprend mal les données exactes utilisées pour ce faire, et on connait encore moins les algorithmes qui seront utilisés pour en arriver à catégoriser le consommateur dans un créneau donné**.**

À défaut de rendre publics leurs algorithmes, certaines entreprises laissent connaître des listes de catégories d'intérêts qu'elles peuvent attribuer à un profil[84]. C'est le cas de Google et Yahoo!, qui permettent aux consommateurs de consulter de telles listes. Chez Facebook, nous avons également pu obtenir un aperçu des attributs de profilage utilisés en consultant les représentations faites aux annonceurs[85]. Ces listes, qui diffèrent d'une entreprise à l'autre, sont

[81] Cet extrait est tiré de la politique de confidentialité de Facebook datée du 15 novembre 2013.

[82] https://www.google.ca/intl/fr/policies/technologies/ads/

[83] https://support.twitter.com/articles/20171551-vos-parametres-de-confidentialite-en-matiere-de-publicites-personnalisees

[84] On trouvera les « centres d'intérêt » de Google ici : https://support.google.com/ads/answer/2842480?hl=fr; Celles de Yahoo! sont disponibles *via* ce lien : https://info.yahoo.com/privacy/ca/yahoo/opt_out/targeting/asc/details.html

[85] Nous avons trouvé les critères de ciblage de Facebook à cette adresse : https://www.facebook.com/ads/create/. Les pages destinées aux annonceurs éventuels donnent un aperçu très compréhensible de la façon dont les renseignements personnels des consommateurs peuvent être utilisés pour les cibler. Voir : https://www.facebook.com/business/a/online-sales/ad-targeting-details

organisées en grandes catégories, lesquelles se subdivisent par la suite en des ramifications très précises[86].

Les premières catégories sont de grands thèmes fort divers qui couvrent de vastes champs d'intérêts. Google en énumère plus d'une vingtaine, tels que « Alimentation et boissons », « Animaux et animaux de compagnie », « Automobiles et véhicules », « Soins du corps et remise en forme » ou encore « Emploi et enseignement »[87]. Facebook propose une dizaine de thèmes similaires, notamment « Divertissement », « Passe-temps et activités », « Sports et activités d'extérieur » ou « Technologie »[88]. L'entreprise offre de même la possibilité de cibler les consommateurs en fonction de leurs comportements présumés, tels que le fait de jouer à des jeux en ligne ou d'effectuer fréquemment un même trajet. Yahoo! propose aussi une quinzaine de thèmes du même acabit, désignés sous d'autres vocables : « *Consumer Packaged Goods* », « *International Interest* », « *Life Stages* »…[89]

Si la plupart de ces critères de ciblage tombe sous le sens, certains d'entre eux demeurent plus obscurs. Ainsi, la catégorie « Affaires et industrie », chez Facebook, vise des intérêts pouvant notamment toucher le crédit ou les finances personnelles; la catégorie « Famille et relations » touche à des intérêts tels que le mariage; « Santé » subsume des intérêts pour les régimes, le conditionnement physique ou le culturisme. Chez Google, la catégorie « Individus et société » traite autant d'éducation des enfants que de problèmes sociaux et de militantisme, alors que la catégorie « Justice et administrations » inclut des intérêts aussi divers que les affaires militaires ou le droit en général.

Sous ces premières grandes catégories, on trouve, regroupées en sous-catégories, des centaines, voire des milliers, de niches précises cernant une myriade de centres d'intérêts, allant de « Insectes et entomologie » à « Huiles et carburants pour véhicules », en passant par « Yoga et Pilates ». Par exemple, on trouvera dans « Hobbies et loisirs », regroupés sous la bannière « Activités de plein air », des intérêts tels que « Chasse et tir », « Pêche », « Randonnées et camping » ou « Équitation ». Dans le thème «Arts et divertissements », la sous-catégorie « Musique et audio » en annonce une autre, « Rock », où se trouvent les centres d'intérêt « Métal », « Punk » et « Vieux classiques du rock ».

[86] Notons que les typologies que nous avons pu parcourir s'arriment assez bien avec les normes *Network & Exchanges Quality Assurance Guidelines*, développées par la branche américaine de l'IAB, qui prévoient une typologie standardisée pour rendre l'industrie plus efficiente. Cette typologie compte plus d'une vingtaine de thèmes principaux, chacun comprenant quelques sous-catégories de deuxième niveau. L'entreprise qui souhaite adhérer à cette norme n'a pas à respecter intégralement les catégories qui y sont suggérées, « *as long as the taxonomy can be clearly mapped back to the taxonomy outlined within this document and explained to and understood by an advertiser with sufficient detail.* » Voir : IAB, Network & Exchanges Quality Assurance Guidelines, 2010, p. 10-12

[87] Les 25 grandes catégories énumérées par Google sont les suivantes : actualités, alimentation et boissons, animaux et animaux de compagnie, arts et divertissements, automobiles et véhicules, communautés en ligne, emploi et enseignement, finance, hobbies et loisirs, immobilier, individus et société, informatique et électronique, internet et télécoms, jeux, justice et administrations, livres et littérature, localités dans le monde, maison et jardinage, marchés commerciaux et industriels, références, sciences, shopping, soins du corps et remise en forme, sports, voyages.

[88] Les 9 grandes catégories énumérées par Facebook sont les suivantes : affaires et industrie, alimentation, divertissement, famille et relations, mode, passe-temps et activités, santé, sports et activités d'extérieur, technologie.

[89] Les 16 grandes catégories énumérées par Yahoo! sont : Automotive, Consumer Packaged Goods, Entertainment, Finance, General Health, International Interest, Issues and Causes, Life Stages, Miscellaneous, Politics, Retail, Small Business and B2B, Sports, Technology, Telecommunications, Travel.

Pour le publicitaire, il s'agira donc de choisir, parmi toutes ces niches précises, celles qui correspondent au public visé par une campagne. Si on ne sait guère par quel procédé exact un consommateur se trouve ainsi étiqueté, on comprend que la collecte massive de renseignements sur les utilisateurs de services sans frais en ligne permet, en bout de piste, d'offrir une précision de ciblage presque chirurgicale aux annonceurs.

2.4. Tous les usages sont permis… ou presque

Mais y a-t-il des limites? Y a-t-il des types de renseignements que les entreprises se refusent à recueillir ou à utiliser? Des étiquettes qu'elles se refusent à affubler à un profil? Bien qu'ils se fassent rares, on trouve quelques engagements à limiter le traitement des renseignements personnels des consommateurs à des fins publicitaires.

D'emblée, la plupart des politiques étudiées qualifieront de « données personnelles[90] » ou de données « personnellement identifiables[91] » les renseignements qu'elles estiment susceptibles d'« identifier personnellement et directement[92] » l'utilisateur. Or, on semble donner une interprétation très étroite de ce qui peut permettre d'identifier une personne, en regroupant exclusivement dans ces données « les informations telles que votre nom ou votre adresse électronique, pouvant être utilisées pour vous contacter ou vous identifier[93] ». Par exemple, Google définit les « données personnelles » en ces termes :

> « Il s'agit de renseignements que vous nous avez fournis qui peuvent vous identifier personnellement comme votre nom, votre adresse de courriel, votre adresse de facturation ou toute autre donnée susceptible d'être associée à ce type de renseignement par Google. »

La politique de Microsoft fournit une autre illustration de cette interprétation :

> « nos systèmes de publicité ne reçoivent pas ou n'utilisent pas d'informations susceptibles de vous identifier personnellement et directement (comme vos nom, adresse de messagerie ou numéro de téléphone). »

De tels énoncés laissent sous l'impression que les entreprises considéreront que toutes les données qu'elles détiennent, en dehors de quelques identifiants précis tels que le nom ou le courriel d'une personne, sont dépersonnalisées – et qu'elles nécessitent donc des précautions moindres lors de leur traitement. Pour cette raison, plusieurs entreprises affirment ne pas communiquer à des tierces parties des données personnelles à des fins publicitaires… mais ne s'empêchent aucunement de communiquer tout autre type de renseignement à de telles fins. Facebook, entre autres exemples, l'énonce comme suit :

[90] Nous avons trouvé cette expression chez Google, LinkedIn, Yahoo! et Twitter

[91] Nous avons trouvé cette expression chez Imgur et Pinterest

[92] http://www.microsoft.com/privacystatement/fr-ca/core/default.aspx

[93] https://www.facebook.com/about/privacy/update/

> « Nous ne partageons pas les informations qui permettent de vous identifier personnellement (les informations qui permettent de vous identifier personnellement sont les informations telles que votre nom ou votre adresse électronique, pouvant être utilisées pour vous contacter ou vous identifier) avec nos prestataires de services de publicité, de mesure et d'analyse, à moins d'obtenir votre autorisation. »

Une telle approche gomme peut-être rapidement les risques de ré-identification des données, lesquels sont de mieux en mieux documentés par la littérature – sans compter, bien entendu, l'inadéquation de cette conception avec ce que la loi définit comme un renseignement personnel (nous reviendrons sur cet aspect à la section 4.1).

Peu d'espoir, donc, de trouver dans ces définitions permissives de véritables limites à la collecte de renseignements personnels dans le cadre de la PCL. Une autre piste, plus prometteuse celle-là, tient peut-être dans la politique de Google, qui affirme explicitement restreindre la collecte et l'utilisation d'informations qu'elle qualifie de sensibles : « Lorsque nous vous proposons des annonces personnalisées, affirme l'entreprise, nous n'associons aucun cookie ni identifiant anonyme à des données sensibles[94] ». Selon Google, une donnée sensible embrasse « les informations confidentielles relatives à la santé, à une origine raciale ou ethnique, à des opinions politiques, à des croyances religieuses ou à la sexualité d'une personne.[95] » L'entreprise évoque également les mêmes restrictions à l'égard de ce qu'elle nomme des « catégories sensibles » d'annonces :

> « Lorsque nous vous proposons des annonces sur mesure, nous pouvons associer un cookie ou un identifiant anonyme à des centres d'intérêts tels que "Cuisine et recettes" ou "Voyage en avion", mais jamais à des catégories sensibles. Nous imposons une politique similaire à nos annonceurs.[96] »

En cherchant bien, on trouve également des restrictions chez Facebook, dont la politique réfère aux « règles publicitaires » de l'entreprise, destinées à encadrer les pratiques des annonceurs. L'examen de ces règles dévoile que les publicités des annonceurs « ne doivent pas faire valoir ou impliquer, directement ou indirectement, dans le contenu de la publicité ou en les ciblant[97] » des « caractéristiques personnelles » d'un utilisateur incluant « la race, l'origine ethnique, la religion, les croyances, l'âge, l'orientation ou les pratiques sexuelles, l'identité sexuelle, le handicap, l'état de santé (y compris la santé physique ou mentale), la situation financière, l'appartenance à un syndicat, le casier judiciaire ou le nom d'une personne.[98] »

---

[94] https://www.google.ca/intl/fr/policies/privacy/

[95] http://www.google.com/intl/fr/policies/privacy/key-terms/

[96] http://www.google.com/intl/fr/policies/privacy/key-terms/; On notera que ces mentions sont conformes aux demandes du CPVP présentées dans une conclusion de 2014, qui portait sur l'utilisation de renseignements personnels sensibles dans le cadre du reciblage publicitaire effectué par Google. Voir : *L'utilisation par Google de renseignements sensibles sur l'état de santé aux fins de l'affichage de publicités ciblées soulève des préoccupations en matière de vie privée*, Rapport des conclusions en vertu de la LPRPDE no 2014-001, 14 janvier 2014 (CPVP). Google prend même soin de préciser que des restrictions s'appliquent en matière de remarketing concernant les données sensibles, conformément aux demandes de cette conclusion. Voir : https://www.google.ca/intl/fr/policies/technologies/ads/

[97] https://www.facebook.com/ad_guidelines.php

[98] https://www.facebook.com/ad_guidelines.php

Chez LinkedIn, on évoque également les informations dites sensibles, mais non pas pour en limiter l'utilisation. On informe plutôt le consommateur que c'est lui qui choisit de les communiquer, le cas échéant, et qu'apparemment il le fait à ses risques et périls :

> « En nous communiquant des données considérées comme "sensibles" en application de la loi, vous agissez de manière entièrement volontaire. À tout moment, vous avez la liberté de retirer ou modifier votre consentement à notre collecte et notre traitement des données que vous nous avez communiquées, conformément aux conditions de la présente Politique de confidentialité et aux Conditions d'utilisation, en modifiant les préférences de votre compte ou votre profil sur LinkedIn ou SlideShare, ou en clôturant vos comptes LinkedIn, SlideShare et Pulse. »

En plus de ces quelques raretés en matière d'informations sensibles, plusieurs entreprises affirment restreindre leurs pratiques concernant les enfants. Certaines exigent que leurs utilisateurs aient au moins 13 ans[99], ou du moins qu'ils aient obtenu le consentement d'un parent pour utiliser les services qu'elles offrent[100]. De son côté, Yahoo! n'exclut pas les enfants de moins de 13 ans, mais affirme ne pas les « contacter » pour des fins publicitaires sans la permission d'un parent. L'entreprise ajoute : « *Yahoo! does not ask a child under age 13 for more personal information, as a condition of participation, than is reasonably necessary to participate in a given activity or promotion*.[101] » Si on comprend que le mineur, soit par interdiction, soit par restriction, ne sera pas exposé à des publicités, on peut se demander jusqu'à quel point une telle déclaration peut constituer un vœu pieux, dans un contexte virtuel où le contrôle et la vérification de l'âge d'une personne, entre autres caractéristiques, sont bien souvent illusoires.

2.5. Consentement et retrait

« En utilisant nos services, vous acceptez que Google puisse utiliser ces données conformément à ses politiques de confidentialité.[102] » C'est ainsi que Google, et la plupart des autres services étudiés, obtiennent le consentement des consommateurs. En substance : les consommateurs acceptent que leurs renseignements personnels soient utilisés pour leur présenter de la PCL dès lors qu'ils choisissent d'utiliser un service en ligne[103].

Quelques entreprises prennent soin de justifier leurs procédés. Certaines, comme Microsoft, expliquent que la publicité est nécessaire à la fourniture gratuite du service[104]. Sur Pinterest, on présente la collecte des renseignements comme inévitable, voire tout simplement banale :

---

[99] Nous avons trouvé ces exigences chez Twitter, Pinterest. LinkedIn, dans ses conditions d'utilisation, demande plutôt que l'utilisateur ait atteint l'âge de 14 ans.

[100] Cette approche est préconisée par Microsoft et le moteur de recherche Bing.

[101] http://info.yahoo.com/privacy/ca/yahoo/

[102] https://www.google.ca/intl/fr/policies/terms/regional.html

[103] Comme nous le verrons à la section 4.4.1, il s'agit là manifestement d'un consentement dit implicite

[104] Par exemple, on trouve ceci dans la politique de Microsoft : « Microsoft fournit un grand nombre de nos sites et services gratuits, car ils sont supportés par la publicité. Afin de rendre ces services largement disponibles, les renseignements que nous collectons peuvent être utilisés pour aider à améliorer les publicités que vous voyez en les rendant plus pertinents pour vous. »

« Aujourd'hui, chaque fois que vous utilisez un site Internet, une application mobile ou tout autre service Internet, certaines informations sont presque toujours créées et enregistrées automatiquement.[105] »

À défaut d'offrir un choix explicite aux consommateurs, la plupart des politiques étudiées énumèrent nombre de façons de limiter le suivi pour des fins publicitaires. Bien que la majorité affirme ne pas tenir compte du signal « *Do Not Track* » des fureteurs, Twitter et Pinterest mentionnent cesser le suivi lorsque celui-ci est activé. Certaines instruisent les consommateurs de la possibilité de bloquer les cookies dans leur navigateur, de même que des conséquences de les bloquer[106] – toutefois, on apprend dans le même document qu'elles utilisent des supertémoins, des pixels invisibles ou d'autres méthodes de suivi que la simple suppression des cookies ne permettra pas d'éluder. D'autres ajoutent que les consommateurs ont toujours le loisir de fermer leur compte ou de ne plus utiliser le service s'ils ne souhaitent pas être pistés.

Dans quelques cas, des entreprises offrent des mécanismes à leurs utilisateurs pour désactiver ou limiter l'utilisation de certains types précis de renseignement. Par exemple, les « Paramètres Google » des appareils mobiles fonctionnant sous le système d'exploitation Android offrent une option pour refuser que les applications utilisent l'identifiant unique de l'appareil pour des fins publicitaires, ou pour réinitialiser celui-ci. Divers paramétrages permettent aussi de bloquer l'utilisation des données de localisation issues du système GPS ou des réseaux Wi-Fi. Ces options peuvent être disséminées en plusieurs endroits, autant dans les options générales de l'appareil mobile que dans les paramètres des applications offertes par certains services[107]. L'application mobile Twitter, par exemple, contient une case que le consommateur peut cocher pour désactiver l'utilisation de la localisation[108].

Plusieurs entreprises mettent elles-mêmes à la disposition des consommateurs des mécanismes de retrait de la PCL, à partir de leur propre plate-forme[109]. Cependant, cette formule « à la pièce », qui exige de demander à chaque entreprise qui piste un internaute de cesser le suivi, atteint rapidement ses limites compte tenu du nombre d'acteurs pouvant participer à la PCL. Par exemple, en plus d'offrir une page pour se désinscrire du suivi publicitaire qu'elle effectue[110], LinkedIn invite les internautes à visiter les pages de huit autres intermédiaires qui peuvent effectuer un suivi :

> « Merci de prendre connaissance des politiques de confidentialité de nos partenaires (liens ci-dessous) afin de déterminer si leur usage des cookies vous convient. Nous avons également mis à votre disposition les liens pour désactiver leurs services, si vous le souhaitez.[111] »

[105] https://about.pinterest.com/fr/privacy-policy-0

[106] Par exemple, Google LinkedIn, Twitter, Kijiji, Amazon et Pinterest donnent de l'information à ce sujet.

[107] https://support.google.com/accounts/topic/6179443?hl=fr&ref_topic=3100928

[108] https://support.twitter.com/articles/20170767-utiliser-les-services-de-localisation-sur-les-appareils-mobiles

[109] De tels mécanismes existent chez : Google, Microsoft (https://choice.microsoft.com/fr-FR), Yahoo!, LinkedIn (« Gérer les préférences pour les publicités »), Twitter, Amazon (http://www.amazon.com/gp/dra/info), Pinterest

[110] https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out

[111] https://www.linkedin.com/legal/cookie-policy

Par la force des choses, parmi toutes les options offertes par les entreprises, le moyen paraissant le plus simple et efficace pour refuser la PCL tient probablement dans la page de retrait de l'Alliance de la publicité numérique du Canada, laquelle permet de se désinscrire en bloc du suivi des nombreuses entreprises participantes[112]. L'*opt-out* effectué *via* les mécanismes de l'industrie promet de désactiver toutes les publicités dites « par centres d'intérêt ». Toutefois, des publicités dites « génériques[113] » ou « contextuelles », utilisant toujours certains types de renseignements obtenus du consommateur, continueront à s'afficher. Amazon l'explique en ces termes :

> « Même si vous désactivez les annonces par centre d'intérêt, des annonces basées sur des facteurs tels que votre position géographique (obtenue à partir de votre adresse IP), le type de navigateur et les dernières recherches effectuées en rapport avec celle en cours peuvent quand même continuer à s'afficher[114]. »

De surcroît, ces options de retrait semblent avoir une portée inégale d'un service à l'autre. Sur les médias sociaux, l'option de retrait du ciblage publicitaire semble plus limitée. En effet, une interprétation littérale des explications données dans les politiques de Facebook, Twitter ou LinkedIn laisse entendre que l'option de retrait mettra fin au suivi du consommateur uniquement quant à son activité à l'extérieur de la plate-forme. Autrement dit, des données de suivi provenant de ses activités lorsqu'il utilise le service seront toujours utilisées, mais pas celles issues de sa navigation sur le reste de la toile.

Figure 2 : Retrait de la personnalisation des publicités de Twitter

L'entreprise explique cette fonctionnalité en ces termes : « Lorsque cette case est décochée, Twitter cesse d'associer votre compte aux informations fournies par ses partenaires publicitaires à des fins de personnalisation des publicités. Cela signifie que nous n'associerons plus votre compte aux informations fournies par nos partenaires à des fins de personnalisation des publicités, y compris vos informations de navigation, vos identifiants d'appareil mobile et vos adresses email cryptées.[115] » À la lecture même de ce texte, on comprend donc que Twitter pourra continuer à suivre l'activité du consommateur lorsqu'il utilise le service; à cet égard, aucun échappatoire ne semble possible.

[112] Nous avons trouvé un lien vers le site de l'APNC chez les entreprises suivantes : Google, Facebook, Microsoft, LinkedIn, Twitter, Kijiji, Amazon, Imgur, Yahoo!

[113] https://choice.microsoft.com/fr-fr/opt-out

[114] http://www.amazon.ca/gp/dra/info?ie=UTF8&*Version*=1&*entries*=0

[115] https://support.twitter.com/articles/20171551-vos-parametres-de-confidentialite-en-matiere-de-publicites-personnalisees

En plus de l'option de retrait de la PCL pure et simple, Google et Yahoo! offrent aux consommateurs un choix plus nuancé : supprimer les centres d'intérêts qu'ils ne souhaitent pas voir affublés à leur profil. Ceci permet aux consommateurs, dans une certaine mesure, de purger les annonces portant sur des sujets qui leur déplaisent ou les attributions qui pourraient porter atteinte, d'une façon ou d'une autre, à leur vie privée. Il s'agit là du contrôle le plus fin offert aux consommateurs que nous avons pu observer.

Figure 3 : Contrôle granulaire offert par Google

Cette page de Google permet à l'internaute de supprimer des centres d'intérêts affublés à son profil.

Toutefois, chez la majorité des entreprises étudiées, un tel contrôle granulaire n'est pas offert. Facebook en évoque la possibilité, mais cette fonctionnalité n'était toujours pas disponible au Canada au moment d'écrire ces lignes[116].

[116] https://www.facebook.com/about/ads/

3. Groupes de discussion avec les consommateurs

L'analyse des politiques révèle que les fournisseurs de services sans frais recueillent une quantité fulgurante de données sur leurs utilisateurs, et peuvent attribuer au profil d'un internaute un nombre considérable d'étiquettes. Mais qu'en pensent les consommateurs? Quels renseignements personnels sont-ils prêts à divulguer pour obtenir un service « gratuit » sur Internet, et quels autres renseignements ne veulent-ils pas partager?

Au Canada et de par le monde, nombre d'études documentent le point de vue des consommateurs concernant la PCL. De ces études, il ressort généralement que la majorité des internautes sont préoccupés ou inconfortables par le suivi en ligne[117]. Souvent, ils ignorent l'ampleur des pratiques qui ont cours à l'égard de leurs renseignements personnels[118]. Malgré cela, une majorité d'entre eux ne souhaiterait pas débourser d'argent pour mettre fin au suivi en ligne pour des fins publicitaires[119].

Les études s'intéressant particulièrement aux perceptions des consommateurs quant aux types de renseignements recueillis dans le cadre de la PCL se font plus rares. Aux États-Unis, une étude de 2013 révèle que la moitié des consommateurs sondés ne veulent tout simplement pas partager leurs données pour des fins de PCL; l'autre moitié serait prête à divulguer leur sexe, leur localisation générale (et non précise), le système d'opération de leur appareil et leur historique web plus que tout autre information[120]. D'autres études indiquent que les consommateurs s'opposent fortement à la divulgation des renseignements qui concernent leur santé[121]. Au Canada, dans le cadre du programme GéoConnexions, Ressources naturelles Canada a publié en 2009 une étude sur la collecte des données de géolocalisation. On y conclut notamment que les Canadiens sont peu à l'aise de divulguer leur emplacement en temps réel pour des fins de commercialisation sélective[122].

---

[117] Le CDIP, en 2009, révélait que la majorité des Canadiens affirme être inconfortables avec les pratiques de ciblage publicitaire comportemental : Janet LO, *A "Do Not Track List" for Canada?*, rapport présenté au Bureau de la consommation d'Industrie Canada par le CDIP, 2009, p. 10-16. Pour des résultats semblables, voir aussi : Blase UR et al., *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising*, Carnegie Mellon University, CMU-CyLab-12-007, 2012. Les proportions exactes de consommateurs varient évidemment selon les études, et selon les méthodes employées.

[118] Blase UR et al., *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising*, Carnegie Mellon University, CMU-CyLab-12-007, 2012; Mary FOSTER, Tina WEST, Avner LEVIN, *The Next Frontier: Targeted Online Advertsing and Privacy*, rapport présenté au Commissariat à la protection de la vie privée du Canada par l'Université Ryerson, 2011

[119] À cet égard, nous invitons le lecteur à consulter la revue de littérature dans : Kent SEBASTIAN, *Un repas gratuit, ça n'existe pas : les contrats de consommation et les services « gratuits »*, rapport présenté au Bureau de la consommation d'Industrie Canada par le CDIP, 2014, p. 14. Voir aussi : Pedro GIOVANNI LEON, Blase UR, Yang WANG, Manya SLEEPER, et al., « What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers », *Proceedings of the Ninth Symposium on Usable Privacy and Security*, article No. 7, 2013, p. 9

[120] Pedro GIOVANNI LEON, Blase UR, Yang WANG, Manya SLEEPER, et al., « What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers », *Proceedings of the Ninth Symposium on Usable Privacy and Security*, article No. 7, 2013, p. 5

[121] Gaurav BANSAL et al., « The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online », (2010) 49-2 *Decision Support Systems* 138

[122] Phase 5 Consulting Group Inc., *Recherche sur la confidentialité et l'utilisation des données géospatiales*, document préparé pour Ressources naturelles Canada, 2009

Pour donner un meilleur portrait du point de vue des consommateurs canadiens, nous avons tenu quatre groupes de discussion, deux à Montréal et deux à Toronto. Dans ces groupes, nous avons cherché à connaître le niveau d'acceptabilité des participants en ce qui a trait aux collectes et à l'utilisation de leurs renseignements personnels dans le cadre de la PCL. Nous avons discuté avec des personnes de tous âges utilisant Internet régulièrement, en tenant, dans chaque ville, un groupe avec des personnes de 18 à 40 ans, et un autre avec des personnes de 40 ans et plus[123]. Voici les résultats de ces discussions.

3.1. Une ampleur surprenante

Les consommateurs ne sont pas dupes. Sans même leur avoir expliqué le fonctionnement de la PCL, plusieurs affirment avoir remarqué qu'on leur propose des annonces concernant des produits ou des sujets sur lesquels ils ont fait des recherches auparavant, tels des meubles ou des voyages. Pour la majorité d'entre eux, le fait que des publicités sont ciblées en fonction de leur activité en ligne est une évidence. « *It's blatantly obvious* », tranche l'un d'eux. Plusieurs comprennent également que les publicitaires font des déductions à partir de leur activité en ligne pour leur affubler des catégories d'intérêts : « *Google has a profile for us. They anticipate our gender, and they know what we search, what we like, our interests, and they focus advertisement towards that*. »

Mais quel niveau d'invasion de leur vie privée les consommateurs sont-ils prêts à accepter en échange de contenus sans frais en ligne? Y a-t-il des renseignements qu'ils ne souhaitent pas divulguer dans le cadre de la PCL? Pour trouver des pistes de réponses à ces questions, nous leur avons exposé les rouages de la PCL. Nous leur avons expliqué que des renseignements tels que leur historique de navigation, leur activité sur les médias sociaux, le contenu de leurs courriels ou encore les informations qu'ils donnent lorsqu'ils ouvrent un compte pouvaient être recueillis à des fins publicitaires[124]. Nous leur avons ensuite demandé leur avis sur la collecte de ces renseignements.

Bien qu'ils aient déjà la puce à l'oreille sur le suivi de leurs activités en ligne, les consommateurs ont paru surpris de l'ampleur de cette pratique. Ils ont affirmé que le suivi en ligne et la collecte de leurs renseignements personnels avaient une portée bien plus grande que ce qu'ils avaient perçu[125]. Par exemple, plusieurs se sont montrés étonnés que le contenu de leurs courriels puisse être scruté pour des fins publicitaires : « Ça donne l'impression qu'ils ont pris la peine de décoller l'enveloppe, lire le contenu, recoller l'enveloppe et la remettre dans le courrier. »

Un suivi si rapproché préoccupe plusieurs d'entre eux : « *It's like you walk down the street and someone follows you. Well, you're at home doing your stuff and somebody else knows what you're doing. It's a scary thing*. » Certains craignent, par exemple, que leur vie privée soit

[123] Nous avons choisi de diviser les groupes en fonction de l'âge des participants après avoir consulté d'autres études qui obtenaient des résultats différents selon l'âge des répondants. Voir, par exemple : Joseph TUROW, Jennifer KING, Chris Jay HOOFNAGLE, Amy BLEAKLEY et Michael HENNESSY, *Americans Reject Tailored Advertising and Three Activities that Enable It*, 2009, en ligne : http://ssrn.com/abstract=1478214

[124] Le guide de discussion complet figure aux annexes 1 et 2

[125] Ce résultat est similaire à celui obtenu par le CDIP dans Janet LO, *A "Do Not Track List" for Canada?*, rapport présenté au Bureau de la consommation d'Industrie Canada par le CDIP, 2009

compromise par des publicités révélatrices de leurs activités en ligne : « *If you have a shared computer and you're trying to get a gift for somebody else, like your boyfriend, your spouse, your kids, you don't want them seeing. This was supposed to be a surprise*. » Beaucoup craignent aussi les dérives de l'utilisation de leurs renseignements personnels, évoquant des images d'une société dystopienne, « *Big Brother* » ou « 1984 ».

Néanmoins, malgré leurs préoccupations, les consommateurs semblent aussi trouver un intérêt dans le modèle d'affaires des entreprises en ligne, dont le financement repose en partie sur la PCL. « *We're getting this amazing free service called the Internet, and it's only possible because of money generated through the advertisers. As long as it's used in that harmless fashion, that is good. But I think there's a certain ethical line, and if that is crossed, then I think we need to re-evaluate*. » Quelques-uns ajoutent que cette forme de publicité peut même s'avérer avantageuse, leur permettant de connaître des rabais pertinents, de découvrir de nouvelles idées d'achat ou de comparer les produits. « Si nous sommes obligés de voir les publicités, mieux vaut en voir sur des sujets qui nous intéressent. »

3.2. Esquisse d'une typologie

Nous avons poursuivi la discussion en demandant aux consommateurs leur opinion quant à la collecte et l'utilisation de 18 types de renseignements, qui recoupent principalement des champs d'intérêts pouvant être utilisés pour les cibler. Établir une liste circonscrite n'a pas été une mince affaire car, comme l'a montré notre analyse des politiques de confidentialité, les entreprises recueillent toutes sortes de renseignements sur les internautes. De plus, les champs d'intérêts qu'elles utilisent sont très nombreux, couvrent un large spectre et varient significativement d'une entreprise à l'autre[126].

Pour nous aider à faire une synthèse représentative de ces divers types de renseignements, nous avons fait appel à la littérature. Nous avons d'abord consulté d'autres études qui s'intéressent aux perceptions des consommateurs sur les types de renseignements utilisés dans le cadre de la PCL[127]. À la suite à notre recherche juridique (section 4), nous nous sommes également assurés que les catégories de renseignements qui sont généralement considérées comme sensibles par la doctrine figurent dans notre synthèse[128]. De plus, certains experts qui nous ont accordé une entrevue nous ont aidés à identifier des types de renseignements pertinents.

Finalement, nous avons demandé aux participants s'ils accepteraient que les entreprises en ligne, pour leur présenter des publicités, utilisent les types de renseignements suivants :

- Le type de nourriture que vous aimez et vos restaurants préférés

[126] Voir section 2.3

[127] La plus importante de celles-ci a été : Pedro GIOVANNI LEON, Blase UR, Yang WANG, Manya SLEEPER, et al., « What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers », *Proceedings of the Ninth Symposium on Usable Privacy and Security*, article No. 7, 2013

[128] Nous avons principalement consulté deux sources doctrinales sur cet aspect : Éloïse GRATTON, *Understanding personal information : managing privacy risks*, LexisNexis Canada, 2013; Paul OHM, « Sensitive Information », (2015) 88 *S. Cal. L. Rev.* [à venir]

- Vos divertissements préférés (par exemple : films, musique, jeux vidéo, sports, etc.)
- Vos préférences d'achats (par exemple : vêtements, automobiles, électronique, etc.)
- Le fait que vous cherchez un nouvel emploi
- Le fait que vous vous mariez bientôt
- Vos passe-temps et loisirs (par exemple : jardinage, randonnée, sports, bricolage, etc.)
- Le fait que vous vous entrainez ou que vous fréquentez un centre de conditionnement physique
- Des informations financières comme votre salaire approximatif, vos plans de retraite ou le fait que vous avez fait des demandes de crédit
- Les endroits où vous avez voyagé ou les endroits où vous planifiez voyager
- Les enjeux auxquels vous vous intéressez, tels que la protection de l'environnement, les affaires étrangères, la politique, etc.
- Votre situation médicale ou votre état de santé en général
- Le fait que vous êtes inscrit à une agence de rencontre
- Votre vie amoureuse, votre orientation sexuelle ou vos préférences sexuelles
- Votre état matrimonial et votre statut familial – par exemple, le fait que vous êtes divorcé ou que vous avez des enfants
- Vos croyances religieuses ou vos opinions politiques
- Votre origine ethnique
- Le contenu de vos messages privés et avec qui vous correspondez
- L'emplacement exact où vous vous trouvez

Certes approximative, cette liste permet néanmoins de couvrir la plupart des thèmes que nous avons trouvés chez les entreprises, tout en présentant des exemples concrets aux consommateurs. Par exemple, le type « divertissements préférés » subsume un grand nombre d'éléments que nous avons relevés dans le cadre de notre analyse des politiques de confidentialité, comme le cinéma, la littérature, les jeux vidéo ou le sport. À noter que les deux derniers éléments de cette liste, portant sur la correspondance des consommateurs et leur géolocalisation, ont été ajoutés après la consultation de la doctrine, qui insiste sur ces deux types de données[129].

Évidemment, les groupes de discussion sont l'occasion de laisser s'exprimer les consommateurs et de les amener à soulever de nouveaux points. Une telle énumération se voulait aussi un guide de discussion, permettant aux participants de réfléchir à d'autres types de situations possibles.

3.3. Une affaire de contexte

Le plus souvent, les participants ont identifié peu de renseignements dont ils considéraient l'utilisation à des fins publicitaires en ligne comme acceptable. Cependant, rares sont ceux qui ont affirmé d'emblée ne vouloir divulguer aucune information, dans aucune circonstance. Ce résultat contredit certaines études antérieures qui concluent qu'au moins la moitié des consommateurs ne souhaite aucunement voir leurs activités en ligne suivies pour des fins

[129] Pour plus de détails, voir section 4.4.2

publicitaires[130]. Cet écart peut s'expliquer par les méthodologies employées : alors que plusieurs de ces études se basaient sur des sondages, nous avons obtenu le point de vue des consommateurs dans des groupes de discussion. Ainsi, notre méthode de collecte a peut-être permis d'obtenir des réponses plus nuancées, dans un contexte où les répondants ont été davantage sensibilisés au modèle d'affaires des entreprises en ligne et aux options qui leur sont offertes.

Cela est peut-être aussi le signe d'un glissement récent dans la conception de la vie privée en ligne; ainsi, les plus jeunes consommateurs, généralement plus avides des nouvelles technologies, ont semblé manifester moins d'appréhensions quant à la collecte et à l'utilisation de leurs renseignements personnels en ligne. Plusieurs d'entre eux ont ainsi affirmé qu'ils n'avaient « rien à cacher », « rien à se reprocher » ou qu'ils n'avaient pas de « comportements immoraux » – et qu'en conséquence, le suivi pour des fins publicitaires les préoccupait peu[131].

Quoi qu'il en soit, l'utilisation de certaines catégories de renseignements à des fins publicitaires a paru acceptable pour une large majorité de consommateurs, peu importe leur âge. Ainsi, la plupart des participants étaient prêts à divulguer leurs préférences en matière de cuisine, de divertissements, d'achats ou de passe-temps. Pour eux, il semble que ces informations demeurent relativement banales, et portent peu à conséquence.

Pour certaines catégories, les avis deviennent toutefois rapidement plus partagés. Ainsi, le fait qu'une personne se mariera sous peu, les enjeux auxquels elle s'intéresse, les endroits où elle envisage faire un voyage ou le fait qu'elle se cherche un nouvel emploi ont suscité davantage de réticences : « *When I'm looking for a job, that's not something that I want out there, even though this is an advertiser.* » Même le fait qu'une personne s'entraîne ou fréquente un studio de santé a paru moins acceptable : « C'est relié à ma santé, au médical, à un paquet de choses qui ne concernent pas les autres. »

Majoritairement, les participants ont aussi estimé que l'utilisation de renseignements tels que leur état matrimonial, leur statut familial, leur origine ethnique, leurs croyances religieuses ou le fait d'être inscrit à une agence de rencontre n'est pas acceptable dans le cadre de la PCL. « Je trouve que c'est trop personnel… ce n'est pas seulement le fait que j'aime les roses. » Plusieurs ont particulièrement insisté sur les informations concernant leurs enfants, qu'ils ne souhaiteraient en aucun cas voir partagées pour des fins publicitaires. Ils craignent également que les plus jeunes utilisateurs d'Internet ne protègent pas suffisamment leur vie privée en ligne, ou qu'ils soient exposés à des publicités inappropriées pour leur âge.

---

[130] Voir notamment : Pedro GIOVANNI LEON, Blase UR, Yang WANG, Manya SLEEPER, et al., « What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers », *Proceedings of the Ninth Symposium on Usable Privacy and Security*, article No. 7, 2013, p. 2 ; Joseph TUROW, Jennifer KING, Chris Jay HOOFNAGLE, Amy BLEAKLEY et Michael HENNESSY, *Americans Reject Tailored Advertising and Three Activities that Enable It*, 2009, en ligne : http://ssrn.com/abstract=1478214

[131] À cet égard, la chercheuse danah boyd propose des pistes très intéressantes. Celle-ci considère que, contrairement à la croyance populaire, les jeunes se préoccupent grandement de leur vie privée en ligne : « *I had been overwhelmingly told, 'Kids these days don't care about privacy'* [...] *And yet when I wandered around talking to young people, I found that young people care deeply about privacy, even in an online environment.* » Elle explique que ceux-ci ont développé nombre d'astuces pour protéger leur vie privée en ligne, et qu'ils manipulent même les algorithmes des entreprises à leur avantage. Voir : http://knowledge.wharton.upenn.edu/article/teens-privacy-online/

Certains types de renseignements ont été rejetés presque unanimement. Ainsi, les consommateurs ont manifesté une forte réticence à ce que l'on utilise des renseignements médicaux ou encore des renseignements portant sur leur vie amoureuse ou sexuelle. On affirme que ces informations peuvent s'avérer « gênantes » et on comprendra assez facilement pourquoi un tel consensus s'est manifesté chez les participants. Un même consensus a aussi été observé quant aux informations sur la situation financière, telles que le salaire approximatif, les plans de retraite ou le fait que la personne a présenté des demandes pour obtenir du crédit : « Mes demandes de crédit, ça ne regarde personne d'autre que moi. » L'utilisation du contenu des messages privés ou de l'emplacement exact où se trouve le consommateur a également suscité une forte opposition, même si certains ont estimé que l'utilisation de la localisation puisse comporter des avantages, par exemple pour trouver des commerces.

On le remarque aisément : les renseignements qu'on considère généralement comme plus délicats sont, bien naturellement, ceux que les consommateurs sont le moins enclins à partager. À première vue, la conclusion paraît donc simple : plus un renseignement se rapprochera de la sphère d'intimité d'une personne, moins cette personne considérera qu'il est acceptable de l'utiliser dans le cadre de la PCL. Ainsi, l'utilisation de renseignements concernant les divertissements préférés semble acceptable pour les consommateurs, alors que l'utilisation de ceux concernant la situation médicale ou les affaires financières est à proscrire.

Cependant, une telle conclusion est hâtive, et oublie que la perception de ce qu'est l'intimité varie d'une personne à l'autre; ce qui est acceptable dépendra donc aussi, et surtout, du contexte et de la perception de la personne concernée. Dans certains cas, l'utilisation d'une information anodine aux yeux d'un grand nombre de consommateurs deviendra, pour une personne dans une situation particulière, un élément révélateur et préjudiciable. Par exemple, un participant a affirmé avoir été blessé par des annonces liées à des recherches qu'il avait effectuées : « *My father-in-law died from prostate cancer, so I was looking up things about prostate. And, after a while, I keep getting these ads about prostate*. » Pourtant, dans un autre contexte, cette utilisation n'aurait peut-être pas causé un même émoi.

Qu'est-ce que l'intimité, exactement? S'il existe des points de consensus quant à l'acceptabilité de l'utilisation de certaines catégories de renseignements, force est de constater qu'il s'agit là d'un concept protéiforme. Les participants n'ont d'ailleurs pas manqué de le souligner : « *Everyone has their own idea of what is sacred knowledge to them. Every single questionnaire here is different, you could ask everyone in the building to fill it out and it would be different*. » Alors que chacun a sa propre conception de l'intimité, il demeure difficile – voire impossible – de trancher définitivement quelles catégories de renseignements font l'objet de la plus grande acceptabilité sociale. Manifestement, bien qu'on puisse tracer de grandes lignes, tout est affaire de contexte et, ultimement, l'analyse devra toujours être faite au cas par cas, selon les circonstances.

3.4. Choix, information, éducation

Après avoir questionné les participants sur les types de renseignements pouvant être utilisés dans le cadre de la PCL, nous les avons questionnés sur le contrôle qu'ils croyaient avoir sur ceux-ci.

Lorsque nous leur avons demandé s'ils savaient quoi faire pour que les entreprises cessent de suivre leurs activités en ligne pour des fins publicitaires, les participants ont hasardé diverses réponses. D'emblée, plusieurs doutent qu'ils puissent complètement échapper au suivi en ligne : « *There's nothing private anymore. Whatever you do, it's all recorded somewhere*. » D'autres, plus terre-à-terre, ont pointé vers les options de leur fureteur Internet, telles que la suppression des cookies, le mode de navigation privé ou la simple suppression de l'historique de navigation du fureteur. D'autres encore ont évoqué la possibilité de recourir à des services en ligne qui n'effectuent pas de suivi, tels que l'engin de recherche *DuckDuckGo*[132].

Quant aux options de retrait de la PCL offertes par les entreprises, elles demeurent peu connues des consommateurs. Ainsi, bien que quelques participants soient familiers avec l'icône *AdChoices*, peu ont été en mesure d'expliquer la fonctionnalité qu'elle offrait. Un même constat s'impose à l'égard du formulaire de retrait granulaire de Google, que les participants ne connaissent généralement pas. « *I've seen it, but I thought it was just asking me questions about myself. I didn't realise it had anything to do with what ads that they are going to use to cater to me*. »

Toutefois, les participants étaient enthousiastes d'apprendre que de telles options leur étaient offertes : « C'est un bon choix à avoir. » Cela fait écho à une volonté qu'ils ont exprimée maintes fois au cours des groupes de discussion : avoir le choix d'accepter ou de refuser que leurs renseignements soient recueillis à des fins publicitaires[133]. « J'aimerais qu'il y ait un système qui me donne le libre choix, que je pourrais cliquer quand il y a une annonce. »

Plus généralement, les participants déplorent ne pas être suffisamment informés sur les pratiques des entreprises en ligne. On le sait, l'information sur ces pratiques figure souvent dans des politiques de confidentialité abstraites et soporifiques, que la majorité des consommateurs ne lisent tout simplement pas. « Je voudrais avoir accès à de l'information adaptée que je pourrais facilement comprendre. » Au-delà de la simple divulgation par les entreprises, on perçoit aussi une volonté d'éducation : « On devrait non seulement nous renseigner, mais aussi nous former. Il devrait y avoir un cours à l'école, que tout le monde devrait suivre. »

Certes, certains consommateurs ont affirmé qu'ils seraient prêts à payer afin que des services en ligne qu'ils utilisent n'effectuent pas de suivi pour des fins publicitaires. Cependant, la plupart étaient également conscients que la publicité permet de financer les services en ligne, et trouvaient des avantages à ce modèle d'affaires : « Si on enlève la publicité de YouTube, il faudra payer plus d'argent chaque mois sur notre compte Internet. Puis c'est déjà cher. » À cet égard, leurs principales réticences ne tiennent pas nécessairement dans le fait d'être suivis ou non sur Internet; c'est plutôt l'impression que la pratique s'effectue subrepticement, sans leur autorisation, qui suscite chez eux les réactions les plus vives. « Je crois que ce doit être un choix conscientisé qu'on fait. Les gens ne le savent pas et je trouve que c'est la responsabilité des gouvernements, des instances, des compagnies qui gèrent ça. »

---

[132] https://duckduckgo.com/

[133] Plusieurs autres études indiquent d'ailleurs que les consommateurs souhaitent avoir davantage de contrôle sur leurs renseignements personnels dans le cadre de la PCL. Par exemple : Lalit AGARWAL et al., « Do Not Embarrass: Re-Examining User Concerns for Online Tracking and Advertising », *Symposium on Usable Privacy and Security (SOUPS)*, Newcastle, Royaume-Uni, 2013

4. Analyse juridique

4.1. Données informatiques et renseignements personnels

Le principe est simple : on collige sur l'internaute des informations qui, une fois traitées, permettront de faire apparaître sous son regard des publicités sur lesquelles il est le plus susceptible de cliquer. Pour arriver à ce résultat, on recueille toutes sortes de données : les adresses des sites que l'internaute consulte, le temps qu'il passe sur ceux-ci, les achats qu'il effectue en ligne, son emplacement géographique, les publications qu'il aime sur les médias sociaux. On recueille aussi des données plus techniques, telles que son adresse IP ou des informations sur l'appareil ou les logiciels qu'il utilise. En substance, on recueille tout ce qu'il est possible de capter sur l'internaute.

La collecte et le traitement de ces données ne s'effectuent pas dans un vide juridique. Au Canada, toute entreprise qui recueillie, utilise ou communique des renseignements personnels dans le cadre d'activités commerciales doit se conformer aux obligations de la Loi sur la protection des renseignements personnels et les documents électroniques[134] (ci-après la « Loi fédérale ») ou de lois provinciales équivalentes[135]. Cela est vrai autant dans le monde physique que dans le monde virtuel.

Ces lois trouveront application dès lors que l'entreprise traitera des renseignements personnels – c'est-à-dire, selon les termes de la Loi fédérale, « tout renseignement concernant un individu identifiable[136] ». La jurisprudence donne une interprétation large à cette définition, considérant qu'un renseignement concerne un individu identifiable lorsqu'il y a « une possibilité sérieuse qu'un individu puisse être identifié au moyen du renseignement, que ce renseignement soit pris seul ou en combinaison avec d'autres renseignements disponibles[137] ».

---

[134] *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5 (ci-après « Loi fédérale »)

[135] L'article 26(2)b) de la Loi fédérale permet au gouvernement fédéral d'en exclure l'application dans les limites d'une province qui a adopté une loi dite « essentiellement similaire » à celle-ci, sauf concernant les « entreprises fédérales » et la collecte, l'utilisation ou la communication de renseignements personnels à l'extérieur de la province, pour lesquelles la Loi fédérale continue de trouver application. Trois provinces canadiennes ont adopté des lois équivalentes, c'est-à-dire prévoyant des dispositions et des droits similaires à ceux prévus dans la Loi fédérale : le Québec, avec la *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1; l'Alberta, avec le *Personal Information Protection Act*, S.A. 2003, c. P-6.5; la Colombie-Britannique, avec le *Personal Information Protection Act*, S.B.C. 2003, c. 63. De même, trois autres provinces ont adopté des lois essentiellement équivalentes, mais seulement applicables aux dépositaires de renseignements sur la santé : l'Ontario, avec la *Loi de 2004 sur la protection des renseignements personnels sur la santé*, L.O. 2004, c. 3, annexe A; le Nouveau-Brunswick, avec *la Loi sur l'accès et la protection en matière de renseignements personnels sur la santé*, L.N.-B. 2009, c. P-7.05; Terre-Neuve-et-Labrador, avec le *Personal Health Information Act*, S.N.L. 2008, c. P-7.01. Notre analyse juridique portera principalement sur la Loi fédérale pour deux raisons : d'abord, puisque les lois provinciales sont équivalentes, on peut penser valablement que l'état du droit sera similaire dans toutes les provinces canadiennes, même si les lois applicables diffèrent; ensuite, la PCL, qui s'articule sur Internet, implique nécessairement la communication de renseignements à l'extérieur des limites physiques d'une province, ce qui soulève des doutes quant à l'applicabilité effective des lois provinciales sur ces activités.

[136] *Loi fédérale*, art. 2. Au sens de cette loi, un renseignement personnel exclut toutefois le nom et le titre d'un employé d'une organisation et les adresse et numéro de téléphone de son lieu de travail.

[137] CPVP, *Bulletin d'interprétation : Renseignements personnels*, en ligne : https://www.priv.gc.ca/leg_c/interpretations_02_f.asp. Le CPVP étaye de nombreux exemples jurisprudentiels faisant

Au vu de cette interprétation libérale, les données recueillies sur les internautes dans le cadre de la PCL seront généralement considérées comme des renseignements personnels au sens de la loi – avec pour conséquence que les entreprises qui les traitent devront respecter les lois sur la protection des renseignements personnels. Bien entendu, des données telles que le numéro de série d'un cookie ou l'adresse IP d'un internaute ne permettent pas nécessairement, à elles seules, d'identifier directement une personne. Cependant, dans le cadre de la PCL, celles-ci sont combinées à d'autres données pour composer un profil révélateur d'un consommateur, profil qui permet aisément de l'identifier. En conséquence, le CPVP a déjà conclu qu'une adresse IP[138], des informations stockées dans un cookie[139] ou encore l'identifiant unique d'un appareil[140] pouvaient constituer des renseignements personnels au sens de la loi. En 2013, le CPVP concluait qu'il en allait de même des renseignements contenus dans le message de statut d'un utilisateur des médias sociaux[141].

La même logique s'applique aux informations déduites sur une personne dans le cadre de la PCL, tels que les centres d'intérêts qu'on affuble à son profil. On considère en effet que même les renseignements subjectifs concernant une personne, qu'ils soient exacts ou non, peuvent se qualifier à titre de renseignements personnels[142]. Dans une conclusion de 2014, le CPVP estimait, par exemple, que Google avait recueilli des renseignements personnels sur l'état de santé d'un internaute en recueillant l'historique de ses visites sur des sites concernant des appareils pour le traitement de l'apnée du sommeil[143].

Cette interprétation libérale a aussi été énoncée par le CPVP dans des lignes directrices sur la publicité comportementale en ligne qu'il a émises en 2012 :

> « en général, l'information recueillie à des fins de PCL constitue des renseignements personnels, *étant donné* que le but de la collecte de renseignements est de créer des profils de personnes qui, à leur tour, permettent d'offrir des publicités ciblées, de puissants moyens disponibles pour recueillir et analyser les bits de données disparates

foi des largesses d'interprétation des tribunaux quant au concept de renseignement personnel, dont l'affaire *Gordon c. Canada (ministre de la Santé)*, 2008 CF 258

138 *Mesures anti-pourriel du FSI contestées*, Résumé de conclusions d'enquête en vertu de la LPRPDE no 2005-319, 3 novembre 2005 (CPVP); *La commissaire adjointe recommande à Bell Canada d'informer les clients au sujet de l'inspection approfondie des paquets*, Résumé de conclusions d'enquête en vertu de la LPRPDE no 2009-010, septembre 2009 (CPVP); voir aussi : CPVP, *Ce qu'une adresse IP peut révéler à votre sujet*, Rapport préparé par la Direction de l'analyse des technologies du Commissariat à la protection de la vie privée du Canada, 2013

139 *Un client se plaint de la présence de « témoins » sur le site Web d'une compagnie aérienne*, Résumé de conclusions d'enquête en vertu de la LPRPDE no 2003-162, 16 avril 2003 (CPVP)

140 *Apple est sommée de fournir davantage de précisions sur l'utilisation et la communication des identifiants uniques d'appareils aux fins de la publicité ciblée*, Rapport de conclusions en vertu de la LPRPDE no 2013-017, 20 novembre 2013 (CPVP), par. 35

141 *Enquête sur les pratiques de traitement des renseignements personnels de WhatsApp Inc.*, Rapport des conclusions en vertu de la LPRPDE no 2013-001, 15 janvier 2013 (CPVP), par. 61

142 *Enquête sur les pratiques de traitement des renseignements personnels de WhatsApp Inc.*, Rapport des conclusions en vertu de la LPRPDE no 2013-001, 15 janvier 2013 (CPVP), par. 59

143 *L'utilisation par Google de renseignements sensibles sur l'état de santé aux fins de l'affichage de publicités ciblées soulève des préoccupations en matière de vie privée*, Rapport des conclusions en vertu de la LPRPDE no 2014-001, 14 janvier 2014 (CPVP), par. 25-28

> et la possibilité bien réelle d'identifier les personnes concernées et du caractère potentiellement très personnalisé de la publicité en résultant.[144] »

L'état du droit convainc donc aisément de l'impertinence de la distinction opérée, dans la plupart des politiques de confidentialités analysées, entre les données dites « personnelles », qu'elles restreignent à quelques identifiants du consommateur, et tous les autres types de données qu'elles recueillent. Manifestement, un renseignement personnel englobe, au sens de la loi, autant le nom et les coordonnées d'une personne que ses activités de navigation colligés dans le cadre de la PCL. En ceci, les entreprises qui traitent des informations dans le cadre de la PCL ne pourront éluder valablement le champ d'application de la loi en présumant de la dépersonnalisation des données qu'elles recueillent.

4.2. Une monnaie d'échange pour les consommateurs

Le sens courant du mot « gratuit », selon le Petit Robert, s'entend de ce que « l'on donne sans faire payer; dont on jouit sans payer.[145] » Or, bien que le verbe « payer » ne réfère pas qu'à un paiement en argent, plusieurs entreprises en ligne semblent pourtant en réduire le sens uniquement à une question d'argent. La page d'accueil de Facebook, par exemple, invite les consommateurs à s'inscrire au service en clamant : « C'est gratuit (et ça le restera toujours) ».

Gratuit, vraiment? Notre analyse des politiques de confidentialité révèle pourtant qu'il y a bel et bien un coût pour les utilisateurs de services sans frais en ligne – même si celui-ci ne se matérialise pas en espèces sonnantes et trébuchantes. En effet, c'est seulement en échange de leurs renseignements personnels qu'on offre aux consommateurs l'accès à ces services. Selon plusieurs auteurs, dont Chris Jay Hoofnagle[146], il y a là une réciprocité entre l'entreprise et le consommateur qui s'éloigne grandement du principe de la gratuité :

> « *Clearly, online firms' business models recognize the current and potential future value of consumers' personal information. Many firms with freemium business models have products to sell, yet devote remarkable amounts of attention and investment to the collection of data from and about free-riding consumers of their products. Social networking services, whose business model is premised on the value of personal information, transfer the cost of running the network to consumers through revenue and data-sharing agreements with third parties.*[147] »

[144] CPVP, *Position de principe sur la publicité comportementale en ligne*, 2012, en ligne : https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_f.asp. Ces lignes directrices donnent des indications précieuses sur le cadre juridique applicable à la PCL au Canada.

[145] Nous avons consulté l'édition 2004 de cet ouvrage.

[146] M. Hoofnagle est professeur à l'Université de Californie, Berkeley - School of Law

[147] Chris Jay HOOFNAGLE et Jan WHITTINGTON, « *Free: Accounting for the Costs of the Internet's Most Popular Price* », (2014) 61 *UCLA L. Rev.* 606, p. 634

Du coup, en acceptant de divulguer ses renseignements personnels, le consommateur doit supporter une myriade de risques dont il n'a peut-être pas entièrement conscience[148]. Entre autres, il s'expose au péril qu'on découvre et exploite indûment ses vulnérabilités; pensons, par exemple, au consommateur ayant des problèmes de jeu qui verrait apparaître des publicités de casino en ligne. Une connaissance poussée des désirs du consommateur pourrait aussi paver la voie à des pratiques discriminatoires, par exemple en donnant l'occasion à des commerçants de moduler leurs prix de vente selon les profils des consommateurs à qui on présente leurs publicités.

Les consommateurs risquent également de voir leur vie privée exposée de diverses manières. Entre autres, l'affichage de publicités personnalisées dans le fureteur d'un internaute pourrait susciter de l'embarras si s'offrait à des tiers l'occasion de les apercevoir, et de deviner des informations compromettantes sur ce dernier. Plus préoccupant, le nombre important d'acteurs impliqués dans la PCL pose des dangers d'atteinte à la sécurité des données sur les consommateurs qu'ils colligent et s'échangent; même lorsque ces données sont dépersonnalisées dans les règles de l'art, des études ont exposé de manière frappante la facilité de les ré-identifier[149].

En somme, l'échange survenant entre le consommateur et le commerçant s'apparente surtout à un contrat d'adhésion. Dans un contexte de déséquilibre informationnel, le consommateur n'a guère le choix d'accepter les termes de l'entreprise pour bénéficier de services qui sont parfois incontournables et indispensables, tels que l'engin de recherche Google. Ils doivent alors se plier à une collecte presque illimitée de leurs renseignements personnels, sans connaître l'ampleur et les ramifications du traitement qui leur sera réservé – et supportent ce faisant des risques d'atteinte à la vie privée, de fraude ou de vol d'identité.

Le droit canadien tarde pourtant à reconnaître ce déséquilibre contractuel. D'une part, les tribunaux n'ont toujours pas confirmé l'applicabilité des lois relatives à la protection du consommateur – qui pourraient offrir certains remèdes – à la relation unissant le consommateur au fournisseur de service sans frais. D'autre part, comme nous le verrons à la section suivante, l'interprétation dominante des lois sur la protection des renseignements personnels demeure floue quant aux limites – si limites il y a – à la quantité de renseignements personnels pouvant être recueillis dans le cadre du modèle d'affaires prétendument gratuit financé par la PCL.

Autant au Québec qu'en Ontario, les lois sur la protection du consommateur n'exigent pas que la contrepartie offerte en échange d'un service soit une somme d'argent pour qu'un contrat y

[148] Pour une nomenclature exhaustive des préjudices et des risques soulevés par la PCL, voir : Janet LO, *A "Do Not Track List" for Canada?*, rapport présenté au Bureau de la consommation d'Industrie Canada par le CDIP, 2009, p. 49-56

[149] Plusieurs études fascinantes sur la ré-identification de données dépersonnalisées ont été conduites au cours des dernières années, lesquelles pointent vers une assez grande facilité d'identifier une personne à partir de ces données. Au nombre de ces études, les chercheurs Alessandro Acquisti, Ralph Gross et Fred Stutzman ont, en 2011, démontré la possibilité d'inférer des renseignements sensibles sur une personne à partir d'une simple photo de son visage, en combinant des logiciels de reconnaissance de visage, des algorithmes d'exploration de données et des techniques d'identification statistique : http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/. Voir aussi : Latanya SWEENEY, « k-anonymity : a model for protecting privacy », (2002) 10-5 *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems* 557; John BOHANNON, « Credit card study blows holes in anonymity », (2015) 347-6221 *Science* 468

soit assujetti. En Ontario, la Loi de 2002 sur la protection du consommateur définit la « convention de consommation » comme un contrat « que le fournisseur conclut avec le consommateur selon laquelle il convient de fournir des marchandises ou des services moyennant paiement[150] ». Un tel « paiement », au sens de la loi ontarienne, n'implique pas nécessairement une somme d'argent, mais bien une « contrepartie de toute nature ». Au Québec, la définition de « contrat de consommation » prévue au Code civil ouvre la porte à une interprétation similaire; encore là, un « paiement » ne se limite pas uniquement à une somme d'argent et peut s'entendre d'autres formes d'obligations[151].

Cependant, la jurisprudence demeure imprécise quant à l'applicabilité des lois sur la protection du consommateur aux contrats dans lesquels l'utilisateur échange un service contre ses renseignements personnels. Jusqu'ici, ce sont principalement dans des jugements d'autorisation de recours collectifs, où les litiges ne sont pas tranchés sur le fond, que la question a été évoquée. Dans plusieurs cas, ces recours collectifs ont été autorisés par les tribunaux[152]. Cependant, en 2011, la Cour supérieure du Québec a rejeté une demande d'autorisation d'exercer un recours collectif contre Facebook, sous motif que le contrat d'utilisateur conclu avec cette entreprise n'était pas un « contrat de consommation », l'utilisation de ce service étant selon le tribunal « gratuite »[153].

Selon plusieurs commentateurs, il s'agit là d'une décision qui aurait mérité d'être portée en appel[154]. Nicolas Vermeys, professeur à l'Université de Montréal, commente :

> « Nos renseignements personnels ont une valeur. S'ils n'en avaient pas, les entreprises ne les recueilleraient pas. Il est faux de dire que c'est gratuit; ce n'est pas une donation de la part de Facebook, c'est un troc, un contrat d'échange. D'un côté, il y a un service, contre, de l'autre côté, vos renseignements personnels. »

Malgré ces quelques aléas du droit qu'on ne souhaite qu'éphémères, force est de constater que la logique économique demeure implacable : les renseignements personnels sont une monnaie d'échange pour les consommateurs. Ce sont leurs données qui permettent aux services en ligne de générer des revenus en offrant des services payants aux annonceurs.

---

[150] *Loi de 2002 sur la protection du consommateur*, L.O. 2002, chap. 30, annexe A, art. 1

[151] *Code civil du Québec*, art. 1553. Pour plus de développements sur ces questions, voir : Anthony HÉMOND, *Perspectives canadiennes sur le «Cloud Computing» et les consommateurs*, rapport présenté au Bureau de la consommation d'Industrie Canada par l'Union des consommateurs, 2011, p. 22-28; Luc THIBAUDEAU, « Le I-consommateur à la recherche de la protection adéquate », *Colloque national sur les recours collectifs : développements récents au Québec, au Canada et aux États-Unis* (2014), vol. 380, Barreau du Québec - Service de la Formation continue, Cowansville, Ed Yvon Blais, p. 588-590; Kent SEBASTIAN, *Un repas gratuit, ça n'existe pas : les contrats de consommation et les services « gratuits »*, rapport présenté au Bureau de la consommation d'Industrie Canada par le CDIP, 2014 p. 30-34

[152] Voir, par exemple : *Albilia c. Apple inc*., 2013 QCCS 2805 (applications mobiles gratuites); *Neale c. Groupe Aéroplan inc.*, 2012 QCCS 902 (programme de fidélisation). Dans *Option Consommateurs c. Corporation Shoppers Drug Mart*, 2012 QCCS 1078, par. 44-45, la Cour supérieure autorise le recours collectif en reléguant sa décision sur la qualification du contrat à une étape ultérieure des procédures.

[153] *St-Arnaud c. Facebook inc*., 2011 QCCS 1506, par. 50-56

[154] Rappelons que cette affaire a fait l'objet d'une transaction avant d'avoir pu être portée en appel.

4.3. Le prix de la gratuité

Dès lors que les renseignements personnels sont une monnaie d'échange pour les consommateurs, on peut tenter de poser le problème sous un angle quantitatif. Si le prix d'un service se fixe en termes de données plutôt qu'en dollars, combien de renseignements personnels est-il légitime d'exiger du consommateur pour qu'il puisse bénéficier de ces services? En somme : quel est le juste prix?

Les lois sur la protection des renseignements personnels, et plus particulièrement le principe de la limitation de la collecte qui y est énoncé[155], fournissent quelques pistes de réponse. Selon la loi, la collecte, l'utilisation ou la communication de renseignements personnels doivent viser des fins qu'une personne raisonnable estimerait « acceptables dans les circonstances[156] ». Ces fins doivent non seulement être précisées à la personne qui fait l'objet de la collecte, mais l'entreprise qui fournit un service ne pourra exiger de la personne « qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées[157] ».

Dans une conclusion de 2009, le CPVP a reconnu le besoin de Facebook générer des revenus par la publicité, et estimé qu'il était raisonnable « qu'on oblige les utilisateurs à consentir à la publicité Facebook comme condition de service.[158] » Dans ses lignes directrices sur la PCL, l'organisme réitère cette interprétation et en précise quelque peu les paramètres :

> « Toutefois, la publicité comportementale en ligne ne devrait pas être considérée comme une condition permettant aux personnes d'utiliser Internet en général. Les sites Web peuvent compter sur d'autres formes de publicité. Un consentement valable et des limites sur les types de renseignements recueillis et utilisés à des fins de profilage sont nécessaires. La protection de l'information est également cruciale, tout comme l'est la limitation de la durée de conservation des données.[159] »

Si ces nuances apportées par le CPVP évoquent la limitation des types de renseignements recueillis et utilisés, notons que le critère de nécessité y demeure encore là bien peu exploré. D'un côté, notre analyse des politiques de confidentialité révèle que les services en ligne recueillent, à toutes fins pratiques, toute bribe d'information pouvant être captée sur leurs utilisateurs. De l'autre, pourtant, les conclusions du CPVP à l'égard de la PCL effectuée dans le cadre de la fourniture d'un service sans frais semblent occulter le fait que, même si les fins de la

[155] *Loi fédérale*, principe 4.4

[156] *Loi fédérale*, art. 5(3)

[157] *Loi fédérale*, principes 4.2.2 et 4.3.3

[158] Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques par Elizabeth Denham Commissaire adjointe à la protection de la vie privée du Canada, Résumé de conclusions d'enquête en vertu de la LPRPDE no 2009-008, 16 juillet 2009 (CPVP), par. 134

[159] CPVP, *Position de principe sur la publicité comportementale en ligne*, 2012, en ligne : https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_f.asp

collecte d'un renseignement sont acceptables, une entreprise « ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées[160] ».

On peut ici se demander si le critère de nécessité, aussi légitimes les fins soient-elles, n'a pas été trop expéditivement gommé. Est-il vraiment nécessaire de colliger toutes les informations générées par un internaute pour atteindre la rentabilité commerciale? En pratique, force est d'admettre que, sous couvert d'une fin acceptable, on semble imposer aux consommateurs un prix sans aucun plafond pour obtenir des services en ligne.

Dans un tel contexte, il n'est peut-être pas déraisonnable d'espérer que le principe de limitation de la collecte dans le cadre de la PCL soit revisité. L'exercice, bien entendu, s'avérerait fastidieux et dépasserait largement le cadre de la présente recherche. Cela exigerait non seulement l'accès aux algorithmes des entreprises en ligne, mais aussi le déploiement de ressources technologiques et juridiques importantes afin d'analyser ceux-ci. Cependant, les autorités gouvernementales devront peut-être envisager sérieusement de s'y astreindre si elles souhaitent évaluer plus qu'approximativement la conformité des entreprises à la loi.

4.4. Catégoriser les renseignements personnels

À défaut de trouver dans le critère de nécessité des limites tangibles à la collecte de renseignements personnels dans le cadre de la PCL, on peut espérer en trouver dans les jalons posés par l'exigence légale du consentement du consommateur, dont la forme variera selon la sensibilité des renseignements personnels recueillis. Si considérer les renseignements personnels comme monnaie d'échange posait la question en des termes quantitatifs, les limites qu'on explorera ici sont plutôt qualitatives, car leur portée varie selon le type de renseignement.

4.4.1. Les écueils du consentement implicite

Aux termes de la loi, les consommateurs doivent être informés de la collecte, de l'utilisation et de la communication de leurs renseignements personnels, et y consentir[161]. Ces principes d'information et de consentement forment la clef de voûte des lois canadiennes en matière de protection des renseignements personnels, et permettent, du moins en théorie, de poser des jalons à ce que les fournisseurs de services sans frais sont autorisés à faire avec leurs données.

On l'a vu, les plus importants fournisseurs de services sans frais sur Internet remplissent ces obligations en obtenant des consommateurs un consentement qu'on qualifie d'implicite (ou négatif)[162] : « à moins que la personne ne prenne des mesures pour exprimer un consentement

[160] *Loi fédérale*, principe 4.4

[161] Ces obligations sont énoncées en nombre d'endroits de l'annexe 1 de la Loi fédérale, voir : principes 4.2, 4.3, 4.4

[162] On oppose le consentement implicite (ou négatif, ou par *opt-out*) au consentement explicite (ou actif, ou par *opt-in*), ce dernier offrant au consommateur la possibilité d'accepter l'utilisation proposée de manière active et non équivoque, sans quoi l'entreprise agira comme si le consentement n'avait pas été donné. Le consentement explicite est donc la forme de consentement la plus haute. Voir : CPVP, *Détermination de la forme de consentement appropriée aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques*, en ligne : https://www.priv.gc.ca/resource/fs-fi/02_05_d_24_f.asp

négatif à l'égard de l'utilisation prévue – c'est-à-dire, à moins qu'elle ne la refuse – l'organisation présume que le consentement a été donné et met à exécution l'utilisation prévue[163] ». Il s'agit de la formule de choix des entreprises offrant des services sans frais en ligne, qui se contentent le plus souvent d'informer les consommateurs sur leurs pratiques dans leurs politiques de confidentialité; lorsqu'il utilise le service, l'internaute consent, par défaut, à tout ce que ce document stipule.

Au regard du droit, cette forme de consentement, dans le cadre de la PCL, ne sera toutefois valide que si elle respecte certaines exigences. Les lignes directrices du CPVP énoncent ainsi qu'un consentement négatif à la PCL ne pourra être acceptable que si les personnes concernées sont avisées « des objectifs de la pratique de façon claire et compréhensible » au moment de la collecte ou avant celle-ci. Cela implique que « ces objectifs doivent être manifestes et ne peuvent être enfouis dans une politique de protection de la vie privée ». Cela implique aussi que l'information doit être complète, et porter sur les « diverses parties qui participent au processus » de la PCL, c'est-à-dire tous les acteurs qui traiteront d'une façon ou d'une autre les renseignements personnels du consommateur. En pratique, le CPVP suggère aux entreprises de remplir ces exigences « à l'aide de divers moyens de communication, comme l'utilisation de bannières en ligne, de technologies multicouches et d'outils interactifs ».

On peut se demander jusqu'à quel point les fournisseurs de services sans frais obéissent scrupuleusement à ces exigences. Notre analyse révèle que l'information sur leurs pratiques publicitaires se trouve le plus souvent au milieu de politiques fort volumineuses – des documents pour la plupart difficiles à comprendre, que les consommateurs ne lisent tout simplement pas[164]. On y énonce de manière vague et générale l'utilisation publicitaire des données du consommateur, de façon à ce que toute donnée puisse être utilisée à des fins publicitaires. De surcroît, on trouve relativement peu d'indications pointant, au moment de la collecte, vers l'information pertinente, si ce n'est que des liens vers les politiques de confidentialité et les modalités en bas de page ou des icônes adjointes aux annonces.

Ces constats ne sont pas inédits. Au cours des dernières années, le déficit dans l'information donnée aux consommateurs dans le cadre de la collecte en ligne de leurs renseignements personnels a été un lieu commun de plusieurs conclusions du CPVP, qui a invité nombre d'entreprises à mieux informer les consommateurs afin que le consentement obtenu puisse être valable[165].

---

[163] CPVP, *Détermination de la forme de consentement appropriée aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques*, en ligne : https://www.priv.gc.ca/resource/fs-fi/02_05_d_24_f.asp

[164] Pour s'en convaincre, mentionnons qu'une étude de 2008 estimait qu'il faudrait aux internautes américains environ 200 heures de lecture par année pour lire toutes les politiques de confidentialité des sites Web qu'ils utilisent. Une tâche manifestement irréaliste : Aleecia M. McDONALD et Lorrie FAITH CRANOR, « The Cost of Reading Privacy Policies », (2008) 4 *ISJLP* 543

[165] Voir notamment : *Enquête sur les pratiques de traitement des renseignements personnels de WhatsApp Inc.*, Rapport des conclusions en vertu de la LPRPDE no 2013-001, 15 janvier 2013 (CPVP); *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques par Elizabeth Denham Commissaire adjointe à la protection de la vie privée du Canada*, Résumé de conclusions d'enquête en vertu de la LPRPDE no 2009-008, 16 juillet 2009 (CPVP); *Apple est sommée de fournir davantage de précisions sur l'utilisation et la communication des identifiants uniques d'appareils aux fins de la publicité ciblée*, Rapport de conclusions en vertu de la LPRPDE no 2013-017, 20 novembre 2013 (CPVP)

Évidemment, notre analyse a aussi révélé que certaines entreprises, telles que Google et Facebook, font davantage d'efforts pour informer leurs utilisateurs, notamment en publiant des politiques plus accessibles ou en donnant quelques illustrations concrètes de leurs pratiques. Cependant, comme nous l'avons constaté dans les groupes de discussion, cela n'empêche pas que les internautes ignorent toujours l'ampleur de la collecte et de l'utilisation de leurs renseignements en ligne; il s'agit peut-être d'un signe que d'importants efforts d'information restent encore à faire.

Qui dit consentement dit aussi possibilité de refuser. Selon les lignes directrices du CPVP, pour que le consentement implicite à la PCL soit valable, les internautes doivent facilement être en mesure d'y renoncer, « idéalement au moment de la collecte ou avant ». De plus, cette renonciation doit être « immédiate et durable ». Or, encore là, on note des problèmes.

D'abord, certaines entreprises ne semblent pas permettre de se soustraire complètement de la PCL telle que définie dans le présent rapport. En effet, les médias sociaux tels que Facebook et Twitter offrent des mécanismes de retrait qui semblent se limiter aux renseignements recueillis à l'extérieur de leur plate-forme, et non pas à toutes les informations colligées par l'entreprise sur ses utilisateurs.

Ensuite, comme l'ont révélé nos groupes de discussion, les mécanismes mis en œuvre par l'industrie pour donner le choix aux consommateurs, tels que le programme de l'APNC ou les mécanismes de retrait granulaire de Google ou de Yahoo!, demeurent largement inconnus du public.

C'est sans compter, comme mentionné précédemment, que bien des difficultés technologiques ou tout simplement pratiques minent l'efficacité et la durabilité de certaines options offertes aux consommateurs. Par exemple, des entreprises leur proposent des solutions manifestement irréalistes pour échapper à la PCL, telles que supprimer leurs cookies ou cesser d'utiliser leur service – alors qu'elles affirment du même souffle user de supertémoins, de pixels invisibles ou d'autres méthodes de suivi des internautes dont il est presque impossible pour le profane d'échapper par ses propres moyens. Autre exemple : plusieurs entreprises affirment ne pas répondre au signal « *Do Not Track* » des navigateurs, alors que ce mécanisme pourrait offrir une option simple pour les internautes.

Force est donc de constater que, malgré quelques percées intéressantes telles que l'option de retrait de l'APNC, les mécanismes de retrait demeurent dépareillés, peu connus et parfois même inefficaces. Dans un tel contexte, le consentement donné par les consommateurs, même s'il se veut simplement implicite, est assurément perfectible.

4.4.2. Sur la piste des renseignements sensibles

Bien que la loi canadienne n'établisse pas de catégories fixes de renseignements personnels dont la collecte ou l'utilisation serait interdite, elle prévoit des exigences de consentement plus élevées quant aux renseignements personnels qualifiés de « sensibles ». Dans le cas de tels

renseignements, un consentement exprès devra généralement être obtenu du consommateur[166].

Déterminer ce qui constitue un renseignement personnel sensible n'est pas une mince affaire. En effet, ce qui est sensible varie d'une personne à l'autre, et d'une situation à l'autre pour cette même personne. Le principe 4.3.4 de la Loi fédérale reconnaît d'ailleurs cette difficulté :

> « Si certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. Par exemple, les nom et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les nom et adresse des abonnés de certains périodiques spécialisés pourront l'être.[167] »

Tout au plus, la Loi fédérale laisse donc pour seuls indices que le dossier médical et le revenu d'une personne pourront généralement être considérés de nature sensible.

De son côté, la jurisprudence a déterminé, au cas par cas, que certains renseignements étaient de nature sensible, selon les circonstances particulières de chaque affaire – et sans véritablement établir une théorie générale de ce concept[168]. Dans le cadre de la PCL, le CPVP a ainsi rendu quelques conclusions au cours des dernières années considérant que des renseignements utilisés étaient de nature sensible. En 2014, il a estimé que Google avait recueilli des renseignements sensibles sur la santé d'un internaute, lesquels avaient été utilisés à des fins publicitaires sans obtenir le consentement exprès requis[169]. En 2013, une conclusion similaire a été rendue à l'égard de l'utilisation d'informations médicales par un site de rencontres en ligne, dont la politique mentionnait qu'il pourrait s'adonner à la PCL[170]. Toujours en 2013, le CPVP a considéré que le numéro d'identification unique d'un appareil de télécommunications Apple utilisé dans le cadre de la PCL était un renseignement personnel

[166] *Loi fédérale*, principes 4.3.4 et 4.3.6

[167] *Loi fédérale*, principe 4.3.4

[168] Par exemple, on a considéré des antécédents en matière de tests de dépistage de drogue comme des renseignements médicaux sensibles : *Un employeur dévoile des renseignements sur les tests de dépistage des drogues subis par un ancien employé*, Résumé de conclusions d'enquête en vertu de la LPRPDE no 2007-382, 27 juillet 2007 (CPVP). *A contrario*, dans une affaire d'assurances, le consentement implicite pour la divulgation de renseignements médicaux a été jugé acceptable : *Un assureur communique les renseignements médicaux d'un particulier à un expert-conseil indépendant en fonction d'un consentement implicite*, Résumé de conclusions d'enquête en vertu de la LPRPDE no 2009-003, 23 février 2009 (CPVP). On a aussi considéré comme des renseignements « extrêmement » délicats des images prises par vidéosurveillance d'enfants dans une garderie : *Une garderie modifie son système de surveillance par cybercaméra pour améliorer la protection de la vie privée*, Rapport des conclusions en vertu de la LPRPDE no 2011-008, 5 août 2011 (CPVP). On a aussi retenu à titre de renseignement personnel sensible une information comme quoi une coiffeuse souhaitait ouvrir son propre salon de coiffure chez elle : *Des renseignements personnels sont communiqués sans consentement dans un message téléphonique laissé sur le lieu de travail d'une cliente*, Rapport des conclusions en vertu de la LPRPDE no 2012-009, 8 août 2012 (CPVP)

[169] *L'utilisation par Google de renseignements sensibles sur l'état de santé aux fins de l'affichage de publicités ciblées soulève des préoccupations en matière de vie privée*, Rapport des conclusions en vertu de la LPRPDE no 2014-001, 14 janvier 2014 (CPVP)

[170] *Des profils affichés sur le site de rencontres PositiveSingles.com se retrouvent sur d'autres sites Web de rencontres affiliés*, Rapport des conclusions en vertu de la LPRPDE no 2013-003, 11 juillet 2013 (CPVP), par. 77

sensible, compte tenu du caractère permanent et persistant de cet identifiant[171]. Toutefois, il faut ici se garder de conclure que tout identifiant unique d'appareil utilisé dans le cadre de la PCL sera automatiquement retenu comme sensible. En effet, au terme de son enquête, le CPVP s'est satisfait qu'Apple ait créé un nouvel identifiant d'appareil pour des fins publicitaires qui pouvait être réinitialisé par l'utilisateur, permettant du coup de limiter le suivi.

Certains auteurs ont proposé des cadres théoriques pouvant aider à définir la nature sensible d'un renseignement. Selon M[e] Éloïse Gratton, associée et Cochef National, groupe de pratique Respect de la vie privée chez Borden Ladner Gervais LLP, un renseignement sensible est un renseignement dont la divulgation risquerait de « créer de l'embarras pour un individu » ou encore causer un « dommage objectif », tel que subir une fraude ou encore faire l'objet de discrimination ou d'un préjudice physique. M[e] Gratton estime que, pour jauger le caractère sensible d'une information, il faut tenir compte non seulement de son caractère intime, mais aussi de son identifiabilité et de sa disponibilité au public :

> « *The sensitivity of the data can be determined by the sum of the risk of harm resulting from the identifying aspect of the data (the more identifiable to a unique individual, the greater the risk of harm), the intimate nature of the data (the more intimate, the greater the risk of harm), and the availability of the data (the less available it was pre-disclosure, and the more available it will be post-disclosure, the greater the risk of harm) upon this data being disclosed*.[172] »

Paul Ohm[173], dans un article récent sur la question, ébauche quant à lui quatre facteurs pour déterminer ce qu'est une information sensible :

> « *First, sensitive information can lead to significant forms of harm. Second, sensitive information is the kind that exposes the data subject to a high probability of such harm. Third, sensitive information often is information transmitted in a confidential setting. Fourth, sensitive information tends to involve harms that apply to the majority of data subjects while information leading to harms affecting only a minority less readily secure the label*.[174] »

Pour ces auteurs, c'est ultimement le risque de préjudice qui sera déterminant dans l'évaluation de la sensibilité d'un renseignement personnel. Cette théorie, certes fondée, semble toutefois par moments éclairer l'obscur par le plus obscur. En effet, la portée de ce qui peut constituer exactement un préjudice pour une personne en matière de renseignements personnels est fort discutable; de même, en évaluer les risques demeure un exercice prospectiviste qui laisse place à bien des errements[175]. Manifestement, des recherches devront encore être conduites pour

[171] *Apple est sommée de fournir davantage de précisions sur l'utilisation et la communication des identifiants uniques d'appareils aux fins de la publicité ciblée*, Rapport de conclusions en vertu de la LPRPDE no 2013-017, 20 novembre 2013 (CPVP)

[172] Éloïse GRATTON, *Understanding personal information : managing privacy risks*, LexisNexis Canada, 2013, p. 266

[173] Professeur associé à la faculté de droit, University of Colorado

[174] Paul OHM, « Sensitive Information », (2015) 88 *S. Cal. L. Rev.* [à venir], p. 5

[175] Dans son article, aux pages 28 à 32, Paul Ohm mentionne ainsi plusieurs types de préjudices. De son aveu même, les limites de ce qui est préjudiciable ou non en matière de renseignements personnels est hautement sujet à débat et certains préjudices apparaissent parfois comme fort abstraits et difficiles à cerner.

déterminer sous quelles conditions cet éther est réconciliable avec la théorie générale de la protection des renseignements personnels.

Quoi qu'il en soit, les travaux de Ohm et Gratton permettent d'établir une taxinomie de renseignements personnels qui tendent généralement à être considérés comme sensibles, ou du moins « intimes », selon la loi, la jurisprudence ou les principes d'autoréglementation dans un grand nombre d'États[176]. En premier lieu, ces auteurs retiennent les informations concernant la santé, les finances, la vie amoureuse ou sexuelle d'une personne et son origine raciale ou ethnique[177]. Des informations concernant la vie familiale d'une personne, incluant son comportement à la maison, sont aussi soulignées[178]. Les opinions religieuses, politiques ou philosophiques pourront aussi être qualifiées de nature sensible[179]; on peut greffer à ce type d'information les affiliations personnelles de l'individu, telles que son appartenance à un syndicat[180]. L'information concernant les enfants fera également l'objet d'une plus grande protection, voire d'une interdiction de collecte pour des fins commerciales; au-delà de la sensibilité de ces renseignements, la question de la validité du consentement des mineurs peut aussi être soulevée[181]. Finalement, selon M[e] Gratton, deux autres types de renseignements pourront généralement être considérés comme intimes : les communications privées des personnes, telles que leur correspondance[182], et la localisation précise de la personne, qui peut notamment être obtenue *via* un GPS.

Sexe, argent, santé… Finalement, ce que la loi, la jurisprudence ou la doctrine considèrent comme des catégories de renseignements sensibles tombe généralement sous le sens. D'instinct, le commun des mortels pourrait nommer la plupart des catégories de renseignements ci-haut énumérées. C'est donc sans grande surprise que nous constatons que les types de renseignements personnels qualifiés de sensibles par le droit subsument l'essentiel des catégories de renseignements pour lesquelles les consommateurs ont majoritairement

[176] Ces auteurs basent leur taxinomie sur les lois applicables dans diverses juridictions, dont l'Union européenne et les États-Unis, la jurisprudence et des instruments normatifs volontaires. À noter que nous avons omis des catégories mentionnées par Ohm qui semblaient plus anecdotiques et qui référaient essentiellement au contexte américain : il s'agit notamment du dossier criminel, des relevés de notes scolaires et de l'information détenue par des institutions publiques. Ohm, au terme de sa taxonomie, mentionne aussi trois types de renseignements personnels qui devraient, selon lui, être considérés comme sensibles : la géolocalisation, les métadonnées des communications et des données biométriques. Nous n'avons toutefois pas retenu le résultat de son analyse, à la fois parce que ces types d'information sont subsumés par d'autres types que nous avons mentionnés précédemment, et parce que certaines problématiques soulignées par l'auteur à l'égard de ces renseignements ne relèvent pas toutes, selon nous, d'une question de sensibilité, mais plutôt d'enjeux tels que le principe de limitation de la collecte que nous avons évoqué précédemment.

[177] Éloïse GRATTON, *Understanding personal information : managing privacy risks*, LexisNexis, 2013, p. 293-294; Paul OHM, « Sensitive Information », (2015) 88 *S. Cal. L. Rev.* [à venir], p. 19-22, 23-24

[178] Éloïse GRATTON, *Understanding personal information : managing privacy risks*, LexisNexis, 2013, p. 292-293

[179] Éloïse GRATTON, *Understanding personal information : managing privacy risks*, LexisNexis, 2013, p. 294; Paul OHM, « Sensitive Information », (2015) 88 *S. Cal. L. Rev.* [à venir], p. 26

[180] Éloïse GRATTON, *Understanding personal information : managing privacy risks*, LexisNexis, 2013, p. 295; Paul OHM, « Sensitive Information », (2015) 88 *S. Cal. L. Rev.* [à venir], p. 27

[181] Paul OHM, « Sensitive Information », (2015) 88 *S. Cal. L. Rev.* [à venir], p. 26. Voir aussi : CPVP, *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et l'infonuagique*, 2011, p. 23-24. Rappelons par ailleurs que la publicité destinée aux enfants peut faire l'objet d'interdictions ou de limitations. Par exemple, au Québec, l'article 248 de la Loi sur la protection du consommateur s'oppose à la publicité à caractère commercial destinée aux enfants.

[182] Éloïse GRATTON, *Understanding personal information : managing privacy risks*, LexisNexis, 2013, p. 296

mentionné, dans les groupes de discussion, s'objecter à l'utilisation pour des fins de PCL. Dans les deux cas, on parle de renseignements qui se rapprochent de la sphère d'intimité de la personne.

Par exemple, autant les informations médicales que financières font partie de ce que les consommateurs souhaitent le moins partager, conformément aux interprétations dominantes de ce qu'est un renseignement sensible au sens de la loi. Les consommateurs ont aussi manifesté des objections à ce que les informations sur leur vie amoureuse, sexuelle ou familiale, ou leurs croyances personnelles soient utilisées dans le cadre de la PCL, encore là en symétrie avec les interprétations de la loi exposées ci-haut. On note également que la localisation et le contenu de leur correspondance font l'objet de mêmes réticences.

Bien entendu, il faut se garder de conclure que seule l'opinion des consommateurs prévaut pour déterminer la sensibilité d'un renseignement. Parfois, les consommateurs ne devineront pas d'emblée qu'un renseignement qu'ils sont prêts à divulguer pourrait leur valoir une intrusion importante dans leur vie privée[183]. Une conclusion récente du CPVP[184], qui estimait qu'un identifiant unique d'appareil était un renseignement sensible, en donne un exemple éloquent; en effet, il s'agit là d'un renseignement qui n'apparaîtra pas intuitivement aux consommateurs comme potentiellement sensible. Cependant, règle générale, il se dégage une adéquation presque totale entre ce que les consommateurs mentionnent ne pas vouloir partager dans le cadre de la PCL et ce que les juristes tendent à désigner *in abstracto* comme des renseignements personnels sensibles.

Hélas, si la perception des consommateurs s'aligne avec la théorie, le problème de la mise en œuvre de la loi dans le contexte virtuel demeure entier. Alors que le degré de sensibilité d'un renseignement personnel s'évalue au cas par cas, l'univers en ligne, où des algorithmes traitent instantanément les données des consommateurs, permet difficilement de cerner quelles sont les informations sensibles. Le CPVP soulignait d'ailleurs cette difficulté en 2011, dans un rapport de consultations sur la PCL :

> « Pour déterminer le type de consentement approprié se pose également la question de la nature délicate des renseignements. Or celle-ci comporte des zones grises. Un renseignement de nature délicate pour certains peut ne pas l'être pour d'autres, et un renseignement peut être de nature délicate dans un contexte donné, mais pas dans un autre. Le problème lorsqu'on essaie de déterminer la sensibilité d'un renseignement en ligne, c'est que l'environnement ne fournit pas de contexte.[185] »

[183] Encore là, des auteurs font un constat similaire aux États-Unis, en mentionnant que le rôle d'experts en protection de la vie privée demeure essentiel pour déterminer si une information apparemment anodine pose des risques : Pedro GIOVANNI LEON, Blase UR, Yang WANG, Manya SLEEPER, et al., « What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers », *Proceedings of the Ninth Symposium on Usable Privacy and Security*, article No. 7, 2013, p. 11

[184] *Apple est sommée de fournir davantage de précisions sur l'utilisation et la communication des identifiants uniques d'appareils aux fins de la publicité ciblée*, Rapport de conclusions en vertu de la LPRPDE no 2013-017, 20 novembre 2013 (CPVP)

[185] CPVP, *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et l'infonuagique*, 2011, p. 31

Comment un algorithme, aussi performant soit-il, pourra deviner qu'un attribut affublé à un profil constitue un renseignement sensible pour une personne, alors que ce ne le serait pas pour une autre, dans d'autres circonstances? Comment peut-il deviner qu'une information qu'il recueille relève de l'intimité d'une personne? Nombre d'exemples pointent vers des situations où la mise en œuvre des instructions d'un algorithme a donné des résultats grossiers; parmi ceux-ci, rappelons la « revue de l'année » générée automatiquement par Facebook en 2014, dans laquelle un père en deuil s'était vu présenter des images de sa fille récemment décédée[186]. Fondamentalement, ceci nous ramène au test de Turing[187] : une machine comprendra peut-être des mots – elle s'avèrera peut-être en mesure de scruter des données et de donner des réponses conformes à ses instructions – toutefois, cela ne signifie pas qu'elle sera en mesure d'exercer le même jugement qu'un humain. Et, de toute façon, déterminer ce qui s'avère sensible pour une personne exigerait probablement d'en savoir *a priori* long, très long, sur cette personne – ce qui nécessiterait paradoxalement une collecte déraisonnée de ses renseignements personnels.

En pratique, en l'absence d'algorithmes qui gagnent au test de Turing, l'entreprise qui voudra dénouer ce nœud gordien devra déterminer, sans contexte, si les informations qu'elle recueille ou qu'elle devine sur un internaute dans le cadre de la PCL constituent ou non des renseignements personnels de nature sensible. Puisque c'est là une tâche quasi-insurmontable, l'entreprise n'aura d'autre choix que de se rallier à des catégories de renseignements prédéfinies : elle choisira de programmer ses algorithmes de façon à ce qu'ils ne traitent pas certaines informations objectives et elle éliminera, parmi les catégories de ciblage publicitaire offertes aux annonceurs, celles qui pourraient s'avérer les plus risquées[188]. Au terme de cet exercice, elle pourra choisir d'éliminer certains centres d'intérêts dans des niches aussi précises que « produits pour les personnes "taille forte" », « faux cils », « armes », « films pour adultes » ou « produits pour la constipation »[189].

Malgré qu'une telle approche apparaisse comme inévitable pour espérer se conformer à la loi, notre analyse des politiques de fournisseurs de services sans frais a révélé que peu d'entre eux détaillent leurs pratiques à l'égard de catégories de renseignements sensibles – exception faite des données concernant les enfants, qui sont fréquemment mentionnées[190]. Figure d'exception, Google affirme explicitement ne pas associer au profil d'un internaute des centres d'intérêts portant sur ce qu'elle définit comme des données sensibles, soit des « informations confidentielles relatives à la santé, à une origine raciale ou ethnique, à des opinions politiques, à des croyances religieuses ou à la sexualité d'une personne.[191] » De son côté, Facebook affirme imposer des restrictions à ses annonceurs non seulement à l'égard données sensibles vues ci-

[186] http://meyerweb.com/eric/thoughts/2014/12/24/inadvertent-algorithmic-cruelty/

[187] Alan M. TURING, « Computing Machinery and Intelligence », (1950) 59-236, *Mind*, 433

[188] Cette méthode est évoquée dans : CPVP, *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et l'infonuagique*, 2011, p. 32

[189] Ces quelques exemples ont été fournis par Me Éloïse Gratton, en entrevue.

[190] Voir aussi APNC, *Principes canadiens d'autoréglementation de la publicité comportementale en ligne*, principe V : « ENFANTS Les entités ne doivent pas recueillir des renseignements permettant d'identifier une personne à des fins de PCL auprès d'enfants dont ils savent qu'ils ont moins de 13 ans ou sur des sites destinés aux enfants âgés de moins de 13 ans ni autrement se livrer à de la PCL destinée à des enfants lorsqu'ils savent que ces derniers ont moins de 13 ans, à moins que cette collecte ou que cet autre traitement des renseignements personnels soit en conformité avec la législation canadienne sur la protection de la vie privée. »

[191] http://www.google.com/intl/fr/policies/privacy/key-terms/

haut – c'est-à-dire la santé, les croyances personnelles, la sexualité ou l'origine ethnique –, mais aussi quant à des données sur l'âge, le nom, le casier judiciaire, la situation financière ou même l'appartenance à un syndicat.

Évidemment, ce déficit de transparence chez les autres entreprises étudiées ne signifie pas irrémissiblement qu'elles ne se conforment pas pour autant à leurs obligations à l'égard des renseignements personnels de nature sensible. D'ailleurs, plusieurs mentionnent adhérer aux Principes canadiens d'autoréglementation de la publicité comportementale en ligne, dont le principe V indique que les adhérents ne doivent pas recueillir et utiliser des renseignements personnels « de nature délicate » à des fins de PCL « sans consentement, selon les exigences de la législation canadienne sur la protection de la vie privée applicable[192] ». Bref, si on n'est guère avancés quant aux catégories que ces entreprises considèrent sensibles, et si on trouve peu de mentions sur la question dans leurs politiques, on pourra peut-être trouver réconfort dans leur engagement de respecter la loi.

Quoi qu'il en soit, malgré ses bonnes intentions, l'approche par catégories a bien des lacunes. D'abord, on peut simplement se demander si les types de renseignements que les entreprises identifient comme sensibles concordent toujours avec ceux que le droit ou les consommateurs considèrent comme tels. On notera ainsi que les politiques de Facebook et Google, bien qu'elles prennent soin d'énoncer des catégories de renseignements sensibles, n'énoncent pas exactement les mêmes types de renseignements de l'une à l'autre. Aux États-Unis, Paul Ohm fait également le même constat : les listes préétablies par les entreprises, autant dans les codes volontaires que dans les politiques de confidentialité des entreprises, énumèrent des types de renseignements différents, dont la portée ne paraît pas la même d'un document à l'autre[193]. Le caractère dépareillé de ces catégories peut constituer un indicateur de la confusion pouvant régner quant à ce qui constitue un renseignement sensible; il est également signe que les entreprises gagneraient peut-être à être davantage guidées dans l'établissement de ces catégories.

Par ailleurs, si on ne connaît pas les usages précis de la plupart des entreprises étudiées quant aux renseignements de nature sensible, on sait néanmoins que certains renseignements qui pourraient généralement être considérés comme sensibles sont largement recueillis et utilisés par celles-ci. C'est d'abord le cas du contenu de la correspondance des consommateurs, que plusieurs services (tels que Yahoo! Mail) mentionnent ouvertement analyser, sans apparemment obtenir de consentement plus formel que pour le reste des informations de leurs utilisateurs. Il en va de même de la géolocalisation du consommateur, qui pourtant pourrait s'avérer bien souvent une information sensible; encore là, nous avons vu que des entreprises telles que Google ne se gênent pas pour s'enquérir d'où se situe le consommateur, notamment en accédant aux données de son GPS[194].

[192] ACPN, *Principes canadiens d'autoréglementation de la publicité comportementale en ligne*, p. 7

[193] Paul OHM, « Sensitive Information », (2015) 88 *S. Cal. L. Rev.* [à venir], p. 11-12

[194] Dans le contexte américain, l'auteur Blase Ur déplore également qu'on n'énonce pas dans les programmes d'autoréglementation de l'industrie que la localisation et la correspondance sont des données « sensibles » : Pedro GIOVANNI LEON, Blase UR, Yang WANG, Manya SLEEPER, et al., « What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers », *Proceedings of the Ninth Symposium on Usable Privacy and Security*, article No. 7, 2013, p. 10

Catégoriser est donc un exercice relativement peu convaincant et qui ne pourra pas, à lui seul du moins, permettre d'imposer des limites efficaces à la collecte de renseignements personnels dans le cadre de la PCL. Cependant, sur la base des résultats que nous avons obtenus, il paraît envisageable de chercher à mieux guider les entreprises quant aux types de renseignements qui posent problème. Sans exclure la flexibilité de la loi, des balises pourraient ainsi être établies de façon à mieux harmoniser les pratiques des entreprises et pour déterminer certains types de renseignements comme étant sensibles. Ces types de renseignements devraient évidemment inclure ce que l'on a pour coutume de considérer comme sensible : santé, finances, sexualité, opinions et affiliations, origine ethnique, vie familiale et informations concernant des enfants. Également, d'autres catégories de renseignements devraient explicitement s'ajouter à la liste : c'est le cas, notamment, de la géolocalisation précise d'un consommateur et du contenu de ses correspondances privées. De telles balises, toutefois, ne constitueront pas une panacée et devront continuer à s'appliquer en complémentarité avec d'autres moyens de contrôle pour les consommateurs.

4.5. Regard sur le droit étranger

À l'étranger, la collecte de renseignements personnels dans le cadre de la PCL pose des défis similaires à ceux qui se présentent au Canada. Les États-Unis et l'Union européenne ont choisi deux avenues différentes pour encadrer cette pratique : alors que l'Amérique opte pour l'autoréglementation, l'Europe a choisi de développer des normes générales et contraignantes.

4.5.1. États-Unis

Les États-Unis n'ont pas adopté de cadre législatif général sur la protection des renseignements personnels, en ligne comme hors ligne. Bien que certaines dispositions légales, dans diverses lois, peuvent accessoirement trouver application dans le contexte de la PCL – par exemple, en matière de fraude[195], de surveillance électronique[196] ou de renseignements concernant des enfants[197] – aucune loi fédérale n'encadre spécifiquement la PCL[198].

En l'absence de normes contraignantes, la Federal Trade Commission (FTC) a émis des lignes directrices, qui proposent des principes aux entreprises pour encadrer la PCL[199]. Ces principes sont repris *grosso modo* dans de nombreux instruments d'autoréglementation créés par des associations d'entreprises, dont les *Self-Regulatory Principles for Online Behavioral Advertising*

[195] *Computer Fraud and Abuse Act*, 18 U.S.C. § 1030 (2006)

[196] *Electronic Communications Privacy Act of 1986*, 18 U.S.C. §§ 2510-2522

[197] *Children's Online Privacy Protection Act of 1998*, 5 U.S.C. 6501–6505

[198] Paul OHM, « Sensitive Information », (2015) 88 *S. Cal. L. Rev.* [à venir], p. 8-9. En 2011, des projets de loi visant à encadrer la pratique ont été introduits, mais ceux-ci sont morts au feuilleton : H.R. 654, Rep. Jackie Speier (D-CA), *Do Not Track Me Online Act of 2011*; Sen. John Kerry (D-MA), cosponsor Sen. John McCain (R-AZ), *Commercial Privacy Bill of Rights Act of 2011* (12 avril 2011)

[199] FTC, *Self-Regulatory Principles for Online Behavioral Advertising*, FTC Staff Report, 2009; Julia ZUKINA, « Accountability in a Smoke-Filled Room: The Inadequacy of Self Regulation Within the Internet Behavioral Advertising Industry », (2012) 7 *Brook. J. Corp. Fin. & Com. L.* 277, p. 289-290

de la Digital Advertising Alliance (DAA)[200], et le *Code of Conduct* du Network Advertising Initiative (NAI)[201].

La FTC et ces codes volontaires promeuvent notamment le principe de la transparence et du contrôle, qui veut que le consommateur soit informé, sur les sites qu'il visite, de la collecte de ses données[202]. L'information ne devrait pas être enfouie dans une politique de confidentialité complexe; pour bien informer les consommateurs, l'agence encourage les entreprises à développer des méthodes d'information innovantes et claires pour les consommateurs[203].

Selon la FTC, les consommateurs devraient également pouvoir choisir ou non de participer à la PCL, à l'aide d'un mécanisme simple pour ce faire[204]. L'industrie de la PCL américaine a répondu à cette invitation en offrant au public le même mécanisme d'*opt-out* annoncé par l'icône *AdChoices* qu'on trouve au Canada[205]. La FTC supporte aussi la mise en œuvre d'un signal « *Do Not Track* » dans les fureteurs des internautes, estimant que c'est là une solution plus efficace pour les consommateurs[206].

Cependant, le niveau de consentement du consommateur à la PCL est modulé selon le type de renseignement recueilli. Le code de la NAI, par exemple, définit trois grands types de renseignements, chacun emportant des obligations spécifiques. D'abord, les données permettant d'identifier directement un individu particulier sont dites « personnellement identifiables » (« *Personally Identifiable Information* (PII) »); cela recoupe un nombre très restreint d'informations, tels que le nom, l'adresse ou le numéro de téléphone d'une personne. Ensuite, les données « non-personnellement identifiables » sont celles qui peuvent être liées non pas à une personne, mais à un appareil informatique précis : identifiant unique, adresse IP, etc. Finalement, les données « dé-identifiées » sont, aux termes du code, des données qui ne peuvent raisonnablement être liées à une personne ou à un appareil particulier. Alors qu'on exigera un consentement par *opt-in* pour l'utilisation des données « personnellement identifiables », on se contentera d'un consentement par *opt-out* pour les données « non personnellement identifiables »; quant aux données « dé-identifiées », il semble qu'aucun consentement ne soit requis à leur égard.

---

[200] DAA, *Self-Regulatory Principles for Online Behavioral Advertising*, 2009

[201] La NAI est une organisation membre de la DAA. Cette dernière chapeaute en fait un grand nombre d'organisations, dont l'IAB. Le champ d'application du code de la NAI est légèrement plus restreint que celui de la DAA, car la NAI est une association de tiers-parties seulement, alors que le code du DAA s'applique généralement à tous les participants de la PCL. Quoi qu'il en soit, les deux codes prévoient des dispositions très similaires, même si on y trouve quelques variantes. Voir : Network Advertising Initiative (NAI), *NAI Code of Conduct*, 2013, p. 2-3

[202] Notre analyse omettra certains principes qui, bien que pertinents, dépassent le cadre de la présente étude. C'est le cas du principe 2 des lignes directrices du FTC, qui prévoit que des mesures de sécurité adéquates pour protéger les données doivent être prises, considérant la sensibilité des informations. FTC, *Self-Regulatory Principles for Online Behavioral Advertising*, FTC Staff Report, 2009, p. 47

[203] FTC, *Self-Regulatory Principles for Online Behavioral Advertising*, FTC Staff Report, 2009, p. 35-37, 46. Il pourra s'agir, par exemple, d'une phrase de type « Pourquoi vois-je cette annonce? » près d'une annonce.

[204] FTC, *Self-Regulatory Principles for Online Behavioral Advertising*, FTC Staff Report, 2009, p. 46

[205] On trouvera ce mécanisme à cette adresse : http://www.aboutads.info/choices/. DAA, *Self-Regulatory Principles for Online Behavioral Advertising*, 2009, p. 14

[206] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FTC Report, 2012, p. VIII; David VLADECK, *Prepared Statement of the Federal Trade Commission on Do Not Track*, Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on the Energy and Commerce, United States House of Representatives, 2 décembre 2010

Cette typologie des données recueillies dans le cadre de la PCL s'éloigne significativement de l'état du droit canadien, où la notion de « renseignement personnel » paraît bien plus englobante. Ces standards américains permettent toutefois d'expliquer certaines distinctions que nous avons observées dans l'analyse des politiques de confidentialité des services en ligne offerts aux Canadiens, dans lesquelles plusieurs entreprises semblent éluder leurs responsabilités à l'égard de données qu'elles ne considèrent pas comme « personnellement identifiables ».

On trouve tout de même des similitudes entre la situation américaine et canadienne. Ainsi, à l'instar de ce qu'on trouve au Canada, le cadre américain prévoit des exigences plus élevées dans le cas de renseignements dont le degré de sensibilité est plus élevé. En effet, la FTC mentionne que les entreprises devraient obtenir du consommateur un consentement exprès lorsque l'entreprise se propose de recueillir de telles informations pour des fins de PCL[207]. L'agence n'énonce pas de catégories exclusives ou de définition précise de ce qu'est une information sensible, considérant que c'est là une affaire de contexte :

> « *With respect to defining what constitutes sensitive data, staff agrees with the commenters that such a task is complex and may often depend on the context. Although financial data, data about children, health information, precise geographic location information, and Social Security numbers are the clearest examples, staff encourages industry, consumer and privacy advocates, and other stakeholders to develop more specific standards to address this issue. Staff also encourages stakeholders to consider whether there may be certain categories of data that are so sensitive that they should never be used for behavioral advertising*.[208] »

Dans leur mise en œuvre des lignes directrices de la FTC, les codes volontaires se montrent toutefois pointus quant à ce qu'englobe la notion de « données sensibles ». Outre certains renseignements concernant les enfants[209], ils énoncent des listes spécifiques d'informations que les entreprises ne devraient pas recueillir ou utiliser sans le consentement de l'internaute[210]. Pour la DAA, ces renseignements sont : les numéros de comptes financiers, les numéros d'assurance sociale, les prescriptions pharmaceutiques ou les dossiers médicaux concernant une personne spécifique[211]. Le code de la NAI ratisse un peu plus large, énonçant, en plus des numéros d'assurance sociale et des numéros de comptes financiers, les numéros de police d'assurances, l'orientation sexuelle, et « *precise information about past, present, or potential*

[207] La FTC prévoit une seconde situation où un tel consentement doit être obtenu : lorsque les représentations faites aux consommateurs sur le traitement de leurs informations subissent un changement « matériel », c'est-à-dire un changement important. Cette exigence de consentement explicite ne s'applique toutefois que lorsque le changement affecte des données préalablement recueillies; si cela s'applique seulement aux données recueillies après le changement de la politique, on peut comprendre qu'on pourra se satisfaire d'un consentement implicite. FTC, 2009, p. 41 FTC, *Self-Regulatory Principles for Online Behavioral Advertising*, FTC Staff Report, 2009, p. 47

[208] FTC, *Self-Regulatory Principles for Online Behavioral Advertising*, FTC Staff Report, 2009, p. 44

[209] Le codes volontaires que nous avons consultés stipulent que les adhérents doivent s'engager à respecter le *Children's Online Privacy Protection Act*, selon lequel il faut obtenir le consentement des parents lors de la collecte de certains renseignements au sujet d'un enfant de moins de 13 ans. Voir : DAA, *Self-Regulatory Principles for Online Behavioral Advertising*, 2009, p. 16-17

[210] Selon le code la NAI, ce consentement devrait être par *opt-in*.

[211] DAA, *Self-Regulatory Principles for Online Behavioral Advertising*, 2009, p. 17

future health or medical conditions or treatments, including genetic, genomic, and family medical history »[212].

Face à ces listes bien délimitées, les associations d'entreprises admettent du moins qu'il pourrait s'avérer nécessaire d'y ajouter, éventuellement, d'autres champs[213]. Et pour cause : ces listes comptent nombre de grands absents parmi les renseignements généralement considérés comme sensibles, dont les opinions politiques, l'origine ethnique, la vie familiale de la personne, la correspondance privée ou encore la géolocalisation. Dans ce dernier cas, le Code de 2013 de la NAI ménage la chèvre et le chou :

> « *While the NAI has removed "Precise Geolocation Data" from the definition of "Sensitive Data" for purposes of this Code update, the NAI believes that a user's precise location is often sensitive, particularly when such data can be used to build detailed profiles of user movements over time*.[214] »

C'est dire qu'en l'absence d'un cadre contraignant à cet effet, les cas où le consentement exprès balisera des limites à la collecte de renseignements personnels dans la cadre de la PCL aux États-Unis demeurent fort restreints.

4.5.2. Union européenne

Au sein de l'Union européenne, deux directives trouvent application dans le cadre de la PCL[215]. D'abord, la directive 95/46/CE sur la protection des données personnelles[216] encadre le traitement de données à caractère personnel de manière générale. Ensuite, la directive 2002/58/CE, appelée « Vie privée et communications électroniques »[217], s'applique plus particulièrement aux enjeux de protection des renseignements personnels soulevés par les nouvelles technologies.

Ces directives créent un cadre général concernant le traitement des « données à caractère personnel » des consommateurs. Elles prévoient des principes similaires à ceux des lois

[212] Network Advertising Initiative (NAI), *NAI Code of Conduct*, 2013, p. 4

[213] Selon la DAA, « *This is a complex area and there may need to be additional areas that should fall into the sensitive data category. The entities participating in the development of these Principles intend to evaluate such areas if and when they may arise in the marketplace*. » Voir : DAA, *Self-Regulatory Principles for Online Behavioral Advertising*, 2009, p. 40; Network Advertising Initiative (NAI), *NAI Code of Conduct*, 2013, p. 4 et 11

[214] Network Advertising Initiative (NAI), *NAI Code of Conduct*, 2013, p. 11

[215] Les directives de l'Union européennes doivent être transposées dans le droit national de chaque État membre.

[216] *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*, JO L 281 du 23.11.1995. Depuis 2012, des propositions de réforme de cette directive sont étudiées au sein de l'Union européenne. Cependant, au moment d'écrire ces lignes, le Conseil de l'Union européenne n'a toujours pas adopté une proposition dans ce sens du Parlement européen. Voir : *Proposition de règlement du Parlement européen et du Conseil 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*, COM(2012) 11 final – E 7055

[217] *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)*, JO L 201 du 31.7.2002

canadiennes, tels que la limitation de la collecte, le droit d'accès et, bien entendu, le consentement de la personne concernée. Tout comme la définition de « renseignement personnel » au Canada, la définition de « données à caractère personnel » est large et inclusive, pouvant notamment comprendre une adresse IP[218] ou, vraisemblablement, l'identifiant unique d'un cookie.

Les exigences légales quant au type de consentement obtenu dans le cadre de la PCL paraissent toutefois plus élevées dans l'Union européenne qu'au Canada où, on l'a vu, la loi se satisfait généralement d'un consentement implicite pour recueillir des renseignements personnels grâce à un cookie. En effet, en 2009, l'article 5(3) de la directive Vie privée et communications électroniques a été modifié de façon à resserrer les exigences à cet égard :

> « Les États membres garantissent que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement. [nous soulignons][219] »

Une telle formulation laisse entendre que seul un consentement explicite pourrait généralement être acceptable pour qu'un cookie soit installé sur l'ordinateur d'un consommateur. En fait, selon le Groupe de travail « Article 29 » sur la protection des données[220], ce consentement doit non seulement être exprès; il doit aussi avoir été obtenu « avant que les données à caractère personnel ne soient collectées, sans quoi les personnes concernées ne comprendraient pas pleinement qu'elles donnent leur consentement et à quoi elles consentent[221] ». Selon le Groupe, une fois le consentement obtenu, il ne sera pas nécessaire de l'obtenir de nouveau chaque fois que le réseau publicitaire y accèdera; cependant, le consentement devrait être redemandé périodiquement[222] et être révocable en tout temps.

En pratique, cependant, ce processus n'est pas aussi strict que la directive le laisse croire. En France, par exemple, où la directive européenne a été incorporée dans Loi du 6 janvier 1978 dite « Loi informatique et libertés », la CNIL[223] affirme ainsi que le consentement de l'internaute à l'installation d'un cookie sur son ordinateur peut être obtenu en affichant un bandeau sur le site qu'il consulte[224]. Ce bandeau l'informera des finalités précises des cookies utilisés, de la

---

[218] Voir, par exemple : *Productores de Música de España (Promusicae) v Telefónica de España SAU*, ECLI:EU:C:2008:54

[219] *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)*, JO L 201 du 31.7.2002, art. 5(3)

[220] Le Groupe de travail « Article 29 » est un organe consultatif européen indépendant sur la protection des données et la vie privée.

[221] GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES, *Avis 2/2010 sur la publicité comportementale*, 22 juin 2010, p. 15

[222] En France, à titre d'exemple, le CNIL énonce que le cookie installé sur un appareil ne peut avoir une durée de vie de 13 mois et qu'au-delà, un nouveau consentement devrait être demandé. Voir : CNIL, « Cookies et traceurs : que dit la loi », en ligne : http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/que-dit-la-loi/

[223] La Commission Nationale de l'Informatique et des Libertés (CNIL) est un organisme public français qui a pour mandat de protéger les droits des citoyens dans le contexte informatique.

[224] La forme exacte pour ce faire peut varier : une zone en surimpression, une case à cocher ou autre annonce qui figurera sur le site que l'internaute consulte.

possibilité de s'opposer à leur installation en cliquant sur un lien figurant dans le bandeau et, surtout, du fait qu'il consent à l'installation du cookie s'il poursuit sa navigation sur le site, c'est-à-dire s'il accède à d'autres pages.

On le voit, la mise en œuvre de ce consentement dit « exprès » garde tout de même des airs de famille avec le consentement implicite tel qu'on le connaît au Canada. En effet, même si le consommateur est préalablement informé de l'intrusion des cookies pour des fins publicitaires, celui qui choisit d'ignorer l'information et de poursuivre sa navigation sur le site consent alors implicitement à leur installation. De plus, le mécanisme de retrait n'est pas directement accessible pour l'internaute, qui devra suivre une procédure de retrait potentiellement « à la pièce » indiquée dans une autre page pour échapper au suivi.

À l'instar du Canada et des États-Unis, le droit européen prévoit des restrictions supplémentaires pour des catégories de renseignements sensibles. Celles-ci sont énoncées à l'article 8 de la directive 95/46/CE :

> « Les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances, l'appartenance syndicale, ainsi que le traitement des données génétiques ou des données concernant la santé ou la vie sexuelle.[225] »

On le constate, l'Union européenne a choisi d'adopter une approche moins flexible que la loi canadienne pour déterminer ce qui constitue un renseignement sensible, en les énumérant de manière exhaustive. Si la lecture de cet article laisse croire que tout traitement de ces types de données sera interdit, la CNIL admet qu'il sera possible de les recueillir dans le cadre de la PCL si on respecte des exigences de consentement très élevées et pourvu que la finalité et l'intérêt public le justifient :

> « Pour collecter et traiter licitement ce type d'information, les fournisseurs de réseaux publicitaires devraient mettre en place des mécanismes leur permettant d'obtenir un consentement préalable exprès, distinct du consentement recueilli pour le traitement des données en général.[226] »

De même, selon l'article 9 de la directive Vie privée et communications électroniques, des mesures spéciales de protection sont prévues pour les données de localisation, lesquelles se définissent comme « toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public[227] ». En ceci, le droit européen reconnaît donc un caractère délicat à ce type de données.

---

[225] *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*, JO L 281 du 23.11.1995, art. 8

[226] GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES, *Avis 2/2010 sur la publicité comportementale*, 22 juin 2010, p. 23

[227] *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)*, JO L 201 du 31.7.2002

Conclusion et recommandations

Doit-on imposer des limites à la collecte de renseignements personnels dans le cadre de la publicité comportementale en ligne? Certes, mais cela pose bien des écueils.

D'abord, la loi impose déjà des limites à la collecte des renseignements dans le cadre de la PCL, limites qui sont souvent éludées par les entreprises. Par exemple, on note une discordance entre l'obligation légale des entreprises de ne recueillir que les renseignements personnels nécessaires aux fins qu'elles énoncent et la quantité presque illimitée de données qu'elles affirment recueillir. D'ailleurs, plusieurs ne semblent pas même considérer toutes ces données comme des renseignements personnels, contrairement à la définition qu'en donne la loi.

Ensuite, l'environnement en ligne et la conception même de ce qui est intime rend difficile la mise en œuvre de balises universelles, basées sur les types de renseignements personnels recueillis. En groupes de discussion, les consommateurs nous ont dit que plus un renseignement se rapproche de leur sphère d'intimité, moins ils souhaitent qu'on l'utilise pour des fins de PCL. Cela s'aligne presque parfaitement avec la notion de renseignement personnel sensible telle que définie dans la loi, la jurisprudence et la doctrine. Sur la base de ces résultats, on peut désigner quelques catégories de renseignements qui devraient être considérées comme sensibles par les entreprises dans le cadre de PCL : la santé, les finances personnelles, la sexualité, les opinions et les affiliations, l'origine ethnique, la vie familiale, la géolocalisation précise, le contenu des correspondances privées et les informations concernant des enfants.

Alors que la Loi fédérale adopte une approche contextuelle de la sensibilité d'un renseignement, la pratique nous apprend que les entreprises déterminent elles-mêmes des catégories rigides sur la base de ce qu'elles croient constituer des informations sensibles – avec pour effet collatéral que certaines ont une interprétation plus restrictive que d'autres. De plus, plusieurs entreprises ne semblent pas considérer *a priori* comme sensibles certains renseignements pourtant délicats, tels que la géolocalisation et le contenu de la correspondance privée. À cet égard, il pourrait être envisageable de mieux guider les entreprises, quitte à les contraindre à reconnaître explicitement ces renseignements comme étant de nature sensible.

Mais il n'y a guère de solution magique. La principale lacune de l'approche par catégories tient dans le fait que fixer des types d'information comme étant sensibles, sans contexte, laissera manifestement passer des situations préjudiciables entre les mailles du filet. La nature sensible d'un renseignement est une question hautement contextuelle – ce que des listes préétablies ou des algorithmes ne sont manifestement pas en mesure d'apprécier. Si l'approche de la Loi fédérale donne la flexibilité nécessaire pour traiter les situations individuelles, cette flexibilité amène du coup plus de confusion et d'incertitude. Face à cette situation, on peut avancer qu'une approche hybride, dans laquelle on conserverait la flexibilité de la loi tout en prescrivant certaines catégories rigides, pourrait peut-être mieux servir les consommateurs.

Cependant, même avec de tels aménagements, d'autres mécanismes demeurent nécessaires pour tenir compte du contexte de chaque situation. Puisque les algorithmes ne peuvent universellement déterminer quelle information est sensible pour chacun, ou plus simplement distinguer quels renseignements une personne souhaite ou non partager pour des fins publicitaires, on devra s'en remettre pour le reste à la volonté de la personne concernée. Le

principe du consentement, et plus largement du contrôle du consommateur sur ses renseignements personnels, garde ainsi plus que jamais sa pertinence.

Mais pour qu'un consentement soit valable, encore faut-il qu'il soit éclairé. Or, notre analyse a mis en lumière les efforts qui restent à faire à ce chapitre, notamment quant à l'information donnée aux consommateurs, au manque de transparence et à l'efficacité des mécanismes de refus disponibles pour les consommateurs. Pourtant, des méthodes simples et efficaces pour consentir valablement à la publicité comportementale sont aisément envisageables : pensons notamment au signal « *Do Not Track* » intégré au fureteur, solution dont la FTC a d'ailleurs fait la promotion. Dans le cas du traitement de renseignements sensibles, le consentement exprès exigé par la loi pourra être obtenu comme il se doit par une mention distincte, explicite et spécifique à chaque utilisation proposée.

Mettre en œuvre des mécanismes efficaces pour informer et obtenir le consentement des consommateurs apparaît certes impératif pour atteindre une véritable conformité à la loi. Mais le contexte technologique soulève également un autre problème : la compréhension globale par les consommateurs des processus invisibles qui s'articulent lorsqu'ils naviguent sur la toile, ou plus généralement des nouvelles technologies qui entrent incessamment dans leur quotidien, demeure souvent approximative. On peut ici s'interroger à savoir si le développement des compétences numériques des consommateurs – incluant entre autres le fonctionnement des appareils informatiques, les langages de programmation et, ultimement, les nouveaux systèmes publicitaires – leur permettrait de mieux comprendre les choix qui s'offrent à eux; bref, de donner un consentement éclairé. À cet égard, la littératie numérique au Canada est un champ qui mériterait peut-être d'être exploré davantage[228].

Catégorisation, transparence, consentement, éducation : poser des limites à la collecte des renseignements personnels dans le cadre de la PCL est un large programme. Sa mise en œuvre signifierait, entre autres choses, que les internautes disposent, en toute connaissance de cause, de l'occasion valable refuser le suivi en ligne pour des fins publicitaires. Au regard de ce que nous avons appris lors des groupes de discussion, cela pourrait signifier, du coup, qu'une large proportion de consommateurs choisirait de refuser ou de limiter grandement le suivi dont ils font l'objet. Or, d'aucuns soulèveront que les entreprises, largement privées des bénéfices du profilage en ligne, verraient alors rapidement chuter leurs revenus publicitaires.

D'autres menaces obscurcissent les prospectives économiques des fournisseurs de services sans frais en ligne. Par exemple, le logiciel AdBlock Plus, qui permet de faire disparaître toutes les annonces apparaissant normalement dans le fureteur d'un internaute, atteint progressivement une masse critique d'utilisateurs; sur Chrome, en juin 2014, cette extension avait ainsi été téléchargée plus de 40 millions de fois. On voit également poindre des substituts aux services des grandes entreprises technologiques, lesquels ne reposent pas sur la collecte des renseignements personnels des utilisateurs pour générer des revenus. Entre autres exemples, l'initiative « Dégooglisons Internet[229] », associée au mouvement du logiciel libre, met ainsi à la disposition des internautes une alternative à Facebook : le réseau Framasphere[230].

[228] Notons que les initiatives en littératie numérique de l'organisme HabiloMédias pourront s'avérer intéressantes au lecteur curieux : http://habilomedias.ca

[229] http://degooglisons-internet.org/

[230] https://framasphere.org/

Est-ce là sonner le glas d'un modèle d'affaires? La loi et la résistance des consommateurs réduiront-t-elles l'économie « gratuite » du web à une peau de chagrin? Un tel pronostic sous-estime sans doute l'ingéniosité des artisans technologiques. Ainsi, pour le Commissaire à l'information et à la protection de la vie privée de l'Ontario, qui promeut les principes « *Privacy by Design* »[231], respecter intégralement les lois en vigueur n'est pas antinomique avec le développement économique; au contraire, c'est plutôt une occasion d'innover au bénéfice de tous[232]. À cet égard, dans le cadre de la PCL, les pistes à explorer ne manquent pas : développer des algorithmes moins gourmands en renseignements personnels, en reconnaître la valeur pécuniaire, parvenir à monétiser des renseignements véritablement dépersonnalisés. En ceci, bien qu'elle exige peut-être de repenser les assises économiques de leurs modèles d'affaires, la conformité aux lois n'est pas synonyme d'une mort annoncée, mais plutôt l'occasion pour les entreprises de trouver des solutions novatrices.

Dans ce contexte, nous formulons les recommandations suivantes :

Recommandations à l'État fédéral et aux provinces :

- **Option consommateurs recommande de contraindre les entreprises participantes à la PCL à mettre en œuvre des mécanismes simples, efficaces et harmonisés permettant aux consommateurs de consentir valablement et activement à la collecte de leurs renseignements personnels dans le cadre de la PCL. Pour ce faire, la possibilité de recourir à un mécanisme obligatoire « *Do Not Track* » intégré au fureteur devrait être plus particulièrement explorée.**

- **Option consommateurs recommande d'augmenter le financement et les pouvoirs des commissariats à la protection de la vie privée canadiens et des autorités chargées de l'application des lois en matière de protection des renseignements personnels pour tenir compte des défis que présentent les nouvelles technologies.**

- **Option consommateurs recommande de développer et d'encourager des initiatives en littératie numérique et de promouvoir chez les Canadiens l'apprentissage du fonctionnement des appareils informatiques, des langages de programmation et des nouveaux systèmes publicitaires.**

Recommandations aux commissariats à la protection de la vie privée canadiens et aux autorités chargées de l'application des lois en matière de protection des renseignements personnels :

- **Option consommateurs recommande d'établir des lignes directrices désignant des types de renseignements personnels comme étant de nature sensible. Ces types de renseignements devraient notamment inclure des renseignements portant sur la santé, les finances personnelles, la sexualité, les opinions et les affiliations, l'origine**

[231] https://www.privacybydesign.ca/

[232] Ann CAVOUKIAN et al., *The Unintended Consequences of Privacy Paternalism*, Commissaire à l'information et à la protection de la vie privée de l'Ontario, 2014, p. 10

ethnique, la vie familiale, la géolocalisation précise, le contenu des correspondances privées et les informations concernant des enfants. Toutefois, l'établissement d'une telle liste ne devrait, en aucun cas, limiter la portée et la flexibilité de la loi, de façon à ce que la sensibilité de tout autre renseignement puisse continuer d'être évaluée selon le contexte.

- **Option consommateurs recommande d'enquêter sur la conformité au principe de la nécessité de la collecte prévu à la Loi sur la protection des renseignements personnels et les documents électroniques, en obtenant des fournisseurs de services sans frais sur Internet des informations précises sur le traitement et l'utilisation qui sont faits de chaque renseignement personnel qu'ils recueillent de leurs utilisateurs.**

Recommandations aux fournisseurs de services sans frais sur Internet :

- **Option consommateurs recommande d'abandonner la notion restrictive de « données personnelles » qui figure dans leurs politiques de confidentialité, et de considérer explicitement toutes les données qu'ils recueillent comme des renseignements personnels au sens des lois canadiennes sur la protection de la vie privée.**

- **Option consommateurs recommande de divulguer et d'élargir les catégories de renseignements qu'ils considèrent sensibles. Les fournisseurs de services sans frais sur Internet devraient notamment considérer la géolocalisation précise et la correspondance comme des renseignements de nature sensible.**

- **Option consommateurs recommande aux fournisseurs de services sans frais de développer de meilleurs mécanismes pour informer les consommateurs sur leurs pratiques publicitaires et obtenir leur consentement conformément à la loi, notamment en reconnaissant le signal « *Do Not Track* » des fureteurs.**

Recommandations aux consommateurs :

- **Option consommateurs recommande aux consommateurs de s'informer sur les renseignements personnels que les entreprises dont ils utilisent les services en ligne recueillent sur eux, de l'utilisation qu'elles en font, ainsi que sur les moyens dont ils disposent pour limiter le suivi en ligne.**

- **Option consommateurs recommande aux consommateurs de porter plainte aux autorités compétentes s'ils estiment que leur vie privée n'est pas respectée par les entreprises avec lesquelles ils contractent en ligne.**

Annexe 1 – Guide de discussion (version française)

1.0 Présentation (5 minutes)

Bienvenue. Ce groupe de discussion est organisé dans le cadre d'une recherche menée par Option consommateurs, un organisme voué à la défense des droits des consommateurs. La durée de la discussion sera d'environ 1h45.

Nous voudrions connaître vos opinions. Je ne veux pas dire ce que vous pensez que les autres pensent, mais bien ce que vous, vous pensez.

Vous pouvez être d'accord, en désaccord ou sans opinion. Même si vous êtes la seule personne du groupe à être d'un certain avis, vous pouvez représenter des centaines de milliers de personnes du pays qui ont la même opinion que vous.

Vous n'êtes pas obligé de vous adresser directement à moi pour formuler vos commentaires. Vous pouvez aussi échanger des idées et des arguments entre vous.

Pour m'aider à préparer mon rapport, nous faisons un enregistrement de la discussion, les données resteront strictement confidentielles. Des observateurs assistent au déroulement de la discussion.

En plus de l'enregistrement, je vais prendre des notes pendant la discussion pour ne pas oublier de détails.

À la fin de la séance, nous vous remettrons la somme prévue pour votre participation.

Maintenant, nous allons faire un tour de table pour que chacun d'entre vous se présente et se décrive brièvement, en disant votre prénom, votre occupation professionnelle et votre lieu de résidence et comment vous utilisez l'Internet et vos sites web favoris.

2.0 Publicité en ligne – premier contact (15 minutes)

Vous êtes tous des utilisateurs réguliers d'Internet. J'imagine que la plupart d'entre vous visitez des sites web, faites des recherches, faites des achats en ligne et que vous interagissez sur les médias sociaux. Vous voyez probablement tous de la publicité en ligne aussi.

Quand vous voyez de la publicité en ligne, croyez-vous que tout le monde voit les mêmes publicités que vous et que les publicités que vous voyez sont affichées par pur hasard?

Pensez-vous que les publicités que vous voyez sont liées à votre comportement en ligne? **SI OUI :** Pouvez-vous donner un exemple de cela?

Avez-vous déjà eu l'expérience de voir apparaître une publicité en ligne qui était liée à ce que vous veniez de faire en ligne? (Par exemple, vous regardiez des horaires de films et peu après, des bannières de publicité faisant la promotion d'un film en particulier sont apparues, etc.)

Pensez-vous que les compagnies ont des façons de cibler leurs publicités en ligne? Comment le font-elles? **SONDER :** Est-ce seulement basé sur le type de visiteurs que les publicitaires croient qu'un site attire, ou est-ce que cela va plus loin?

3.0 Renseignements recueillis (15 minutes)

En fait, afin de vous cibler leur publicité, beaucoup de compagnies enregistrent vos activités en ligne, comme les sites que vous visitez et à quels médias sociaux vous participez. Ils ont des algorithmes qui analysent cette information pour prédire vos intérêts et ce, afin de vous montrer des publicités annonçant des choses qu'il y a plus de chances qui vous intéressent. Par exemple, en suivant vos activités en ligne, elles pourraient déterminer que vous aimez la science-fiction, et ainsi vous montrer des publicités sur le dernier film de «Star Wars».

Cette pratique est appelée «publicité comportementale en ligne» ou «publicité ciblée par centres d'intérêt». Ce type de publicité est de plus en plus répandu. Les médias sociaux tels que Facebook et Twitter génèrent beaucoup de revenus en vendant de l'espace publicitaire qui peut être ciblé de cette façon. Les moteurs de recherche tels que Google, Yahoo! et Bing (Microsoft) font également de même. Ils enregistrent vos activités lorsque vous utilisez leur service. Certains enregistrent également vos activités sur d'autres sites que vous visitez.

Des réseaux publicitaires ont des accords avec des sites web, des moteurs de recherche ainsi que des médias sociaux qui leur permettent de récolter des données à propos du comportement en ligne de leurs visiteurs. Google est au courant des sites que vous utilisez le plus, et génère beaucoup de revenus grâce à ces informations…

Cela veut dire que lorsque vous êtes en ligne, vous êtes exposé à des publicités qui sont personnalisées à ce que des entreprises croient être vos intérêts, en se basant sur vos comportements en ligne.

Avez-vous a déjà entendu parler de ce phénomène auparavant?

Que pensez-vous de cette «publicité comportementale en ligne»? Quels sont les pours et les contres?

En quoi est-ce une bonne chose?

SONDER SI NON MENTIONNÉ : Est-ce utile pour vous de voir des publicités pour lesquelles vous êtes susceptibles d'être intéressés? Aide à générer des revenus qui font en sorte que les contenus en ligne sont gratuits (ex : Facebook, Twitter sont gratuits)?

En quoi est-ce une mauvaise chose ou quelque chose qui vous préoccupe?

SONDER SI NON MENTIONNÉ : Est-ce une intrusion dans votre vie privée? Y a-t-il trop de publicités?

Selon vous, lorsque vous êtes en ligne, quelles informations enregistre-t-on?

Selon vous, quelles informations n'enregistre-t-on PAS? Celles de nature privée?

4.0 Renseignements recueillis (15 minutes)

Lorsque vous êtes en ligne ou que vous êtes sur un média social, il y a plusieurs types d'information qui sont enregistrés à propos de vos activités afin de vous présenter de la publicité ciblée. Ceci inclut :

- Informations sur vos activités en ligne – les sites vous visitez, le temps que vous passez sur chacun, les mots-clés que vous recherchez sur Google, les vidéos que vous regardez, les achats en ligne que vous faites et les publicités sur lesquelles vous avez cliqué
- Votre comportement sur les réseaux sociaux (Ex : Facebook, Twitter, etc.), ce que vous «aimez», vos commentaires, qui sont vos contacts et comment vous interagissez avec eux, quels groupes vous faites partie et ce que vous partagez
- Le contenu de vos courriels et le contenu de vos messages sur les médias sociaux
- L'endroit où vous vous situez selon le GPS qui se trouve sur votre téléphone cellulaire
- Des informations techniques, comme le modèle d'ordinateur ou le modèle de cellulaire vous avez, le système d'exploitation vous utilisez ou votre adresse IP
- Des informations personnelles que vous avez fournies pour vous créer un courriel ou pour vous créer un compte sur un média social, telles que votre âge, votre emploi, votre éducation, etc.

Ces informations ne sont pas nécessairement rattachées à votre nom. Dans la plupart des cas, elles sont recueillies grâce à des «cookies», qui sont des fichiers contenus dans votre ordinateur et qui permettent de suivre vos activités en ligne. Ces «cookies» aident à créer un profil qui servira à cibler la publicité qui vous est présentée.

Est-ce que chacun d'entre vous savait que toutes ces données et informations étaient recueillies à propos de vous? Êtes-vous surpris?

Saviez-vous que tous ces types de données et d'informations étaient recueillis afin de faire de la publicité ciblée?

J'aimerais que vous écriviez tous sur un papier une liste de toutes les informations que vous ne voudriez PAS qui soient enregistrées de cette façon.

Qu'avez-vous écrit, et pourquoi?

Cela ferait-il une différence pour vous si les entreprises gardaient ces informations sur vous seulement pour une très courte période de temps, seulement le temps de créer un profil vous, et effaceraient ensuite toutes les données?

5.0 Profilage en ligne (15 minutes)

L'information recueillie dont nous avons discuté sert à créer un «profil» de vous sur vos intérêts.

Par exemple :

- Quelqu'un qui «aime» la page de «Star Wars» sur Facebook et qui partage un article à propos de «Star Wars» pourrait être catégorisé comme étant une personne aimant la science-fiction
- Une personne qui visite des sites web sur la maternité pourrait être catégorisée comme étant «enceinte» et pourra être exposée à des publicités à propos de la grossesse et ce, sur n'importe quel site qu'elle visite, mêmes ceux qui n'ont aucun lien avec la grossesse

Y-a-t-il des types de catégorisations que vous ne voudriez PAS qui figurent à votre profil? (Par exemple, cela ne vous dérangerait pas d'être catégorisé comme une personne qui aime voyager au Mexique, mais cela vous dérangerait d'être catégorisé comme étant quelqu'un qui souffre de dépression).

Donnez des exemples de types d'intérêts ou de préférences que vous ne voudriez PAS que les publicitaires se servent pour vous cibler.

Voici une liste de types d'informations qui pourraient être déduites sur vous à partir de votre activité en ligne. Indiquez celles que vous trouveriez acceptables d'utiliser à des fins de ciblage publicitaire et celles pour lesquelles vous ne trouveriez pas cela acceptable.

DISTRIBUER LA LISTE

a. Le type de nourriture vous aimez et vos restaurants préférés
b. Vos divertissements préférés (ex : films, musique, jeux vidéo, sports)
c. Vos préférences d'achats (ex : Vêtements, automobiles, électronique etc.)
d. Le fait que vous cherchez un nouvel emploi
e. Le fait que vous vous mariez bientôt
f. Vos passe-temps et loisirs (ex : jardinage, randonnée, sports, bricolage, etc.)
g. Le fait que vous vous entrainez ou que vous allez à un centre de conditionnement physique
h. Des informations financières comme votre salaire approximatif, vos plans de retraite ou le fait que vous avez fait des demandes de crédit
i. Les endroits où vous avez voyagé ou les endroits où vous planifiez voyager
j. Les enjeux auxquels vous vous intéressez, tels que la protection de l'environnement, les affaires étrangères, la politique, etc.
k. Votre situation médicale ou votre état de santé en général
l. Le fait que vous êtes inscrit à une agence de rencontre
m. Votre vie amoureuse, votre orientation sexuelle ou vos préférences sexuelles
n. Votre état matrimonial et votre statut familial – par exemple, le fait que vous êtes divorcé ou que vous avez des enfants

o. Vos croyances religieuses ou vos opinions politiques
p. Votre origine ethnique
q. Le contenu de vos messages privés et avec qui vous correspondez
r. L'emplacement exact où vous vous trouvez

Qu'est-ce qui fait que vous seriez prêt à divulguer certaines de ces informations et d'autres non? Quels sont vos critères?

6.0 Consentement et retrait (10 minutes)

Selon vous, avons-nous le choix de partager ou de ne pas partager toutes ces informations en ligne? Quels choix avons-nous? Pouvons-nous refuser?

Avez-vous déjà lu les politiques de confidentialité sur les sites web que vous visitez? Pourquoi? Pourquoi pas?

Y-a-t-il une façon de forcer les compagnies d'arrêter de traquer nos activités en ligne ? Comment ferions-nous ?

Plusieurs entreprises rendent disponible un formulaire pour demander de mettre fin au suivi en ligne. Une des façons d'accéder à cette option est en cliquant sur l'icône « Ad Choices » qu'on trouve aux côtés de plusieurs annonces. Des publicités seront toujours affichées aux internautes qui se désabonnent, mais elles ne seront plus ciblées à partir de leur activité en ligne.

Saviez-vous que cela existait? Est-ce que cela fonctionne vraiment?

Quelques entreprises, dont Google, offrent de plus une autre possibilité. Elles permettent de retirer des centres d'intérêts qui ont été attribués au profil de l'internaute. Par exemple, si l'entreprise a catégorisé un internaute comme « amateur de science-fiction », celui-ci peut supprimer cet intérêt dans les options de Google. Par la suite, on ne lui présentera plus de publicités correspondantes à cet intérêt.

Saviez-vous que cela existait? Qu'en pensez-vous ?

7.0 Conclusion (5 minutes)

Quels sont vos conclusions sur tout ce dont nous avons parlé? Y a-t-il des choses qui vous ont surpris?

Pensez-vous que les compagnies en ligne en savent trop sur vous ou est-ce acceptable?

Quelles sont vos préoccupations?

Les médiaux sociaux tels que Facebook et Twitter sont gratuits en partie grâce aux revenus qu'il tirent des publicités ciblées. Qu'arriverait-il si pouviez demander à Facebook d'arrêter de suivre

votre comportement en ligne, mais qu'en échange, vous devriez payer pour utiliser Facebook? Combien seriez-vous prêt à payer pour utiliser ces services sans que votre comportement soit suivi?

Selon vous, les informations qu'on recueille sur vous valent-elles de l'argent?

Merci pour votre participation

Annexe 2 – Guide de discussion (version anglaise)

1.0 Introduction to Procedures (10 minutes)

Welcome to the group. We want to hear your opinions. Not what you think other people think – but what you think!

Feel free to agree or disagree. Even if you are just one person around the table that takes a certain point of view, you could represent many Canadians who feel the same way as you do.

You don't have to direct all your comments to me; you can exchange ideas and arguments with each other too.

You are being taped and observed to help me write my report.

I may take some notes during the group to remind myself of things also.

The host/hostess will pay you your incentives at the end of the session.

Let's go around the table so that each of you can tell us your name and a little bit about yourself, such as what kind of work you do if you work outside the home and also since we are going to be discussing some issues around use of the internet – how often do you go online and what are your favourite websites or what social media do you use?

2.0 Online advertising - initial attitudes (15 minutes)

You are all people who use the internet regularly. I assume most of you visit websites, research topics, make purchases and interact through social media. You probably all see online advertising as well.

When you see online advertising, do you think everyone sees the same ads and that whatever ads you see you are just seeing by random chance?

Do you think the ads you see online are linked at all to your personal online behaviour? **IF YES**: What would be an example of this?

Have any of you ever had the experience of having an ad appear to you online that were linked to what you had just been doing online? (For example, you look up movie listings and soon after banner ads appeared to you promoting a specific film etc…)

Do you think companies have ways of targeting their online advertising? How do they do that? PROBE: Is it just based on who they think are the kinds of people who visit the site they are advertising on or does it go further than that?)

3.0 Collected personal information (15 minutes)

In fact in order to target their advertising at you, many companies record your online activities such as what sites your visit and what social media you participate in. They have algorithms that analyse this information to predict what your interests are so that they can show you ads that are for things you are likely to be interested in buying. For example, by following your online activity they might determine that you like science fiction and so you might then be shown ads for the latest Star Wars etc…

This is known as "online behavioural or 'interest-based' advertising" and is more and more common. Social media sites like Facebook and Twitter get a lot of their revenue by selling this information about their users, as do companies with search engines like google, Yahoo! and Microsoft. They record your activities when you use their services and some also record your activities on sites you visit through them.

There are advertising networks which have agreements with many websites, search engines and social media sites whereby they can collect data about the online behaviour of their visitors. Google makes a lot of its money this way and knows what news sites you use the most etc…

This means that when you go online you will be exposed to ads that are customized to what they think you are interested in based on your online behaviour.

Had any of you heard of this phenomenon before?

What do you think of this "online behavioural advertising"? What are the pros and cons?

In what ways is it a good thing?

PROBE IF NOT MENTIONED: Useful to you to get ads that you are more likely to be interested in? Helps generate revenue that makes most of what we do online free (e.g. Facebook and twitter cost nothing)

In what ways is it a bad thing or something that concerns you?

PROBE IF NOT MENTIONED: Invasion of privacy? Means you get too many ads?

As far as you know, when you go online what information do you think gets recorded?

What information do you think does NOT get recorded? Is anything private?

4.0 Personal information from "cookies" (15 minutes)

When you go online or use social media there are all kinds of information that gets recorded about your activities and interests in order to target you with advertising. These include:

- Information about your online activities – what sites your visit, how long you are on each site, what key words you search on google, videos you watch, your online purchases and what ads you have clicked on.
- Your social media behaviour (e.g. Facebook, Twitter etc…), what you "like", your comments, who your contacts are and how you interact with them, what groups you belong to and what you share.
- The content of your e-mails and messages within social media.
- Where you work and where you are through the GPS on your cell phone.
- Technical information like what type of computer or phone you have, what operating system you have, your IP address etc…
- Personal information you may have provided to sign up for e-mail or social media services such as your age, employment, education etc…

Much of this information is not necessarily attached to your name. In most cases this is all collected though what are called "cookies" which are devices in your computer or devise that follow your online activities. These cookies help to create a profile of you that allows advertising to be aimed at you.

Did you each know that all of these kinds of data and information are being collected about you? Are you surprised by any of it?

Did you know this was all collected for the purpose of aiming advertising at you?

I would like you to each jot down on paper a list of kinds of information that you would NOT want recorded in this way?

What did you each come up with and why?

What if the ad agencies only kept this information about you for a very short time just to create a profile for you and then all the individual information about you was erased, what that make any difference to you?

5.0 Online profiling (15 minutes)

All of the information collected that we discussed goes into creating a "profile" for you based on your interests. For example:

- Someone who "likes" the page for "Star Wars" on Facebook and shares an article about Star Wars may be categorized as "science fiction fan".
- Someone who visits sites about maternity might be profiled as "pregnant" and may get exposed to ads about pregnancy related products and services all over the internet, even if you are visiting sites that have nothing to do with pregnancy.

Are there specific ways in which you would NOT want to be profiled? (For example, maybe it wouldn't bother you to be profiled as someone who likes to travel to Mexico, but it would bother you to be profiled as someone who suffers from depression)

What would be examples of kinds of interests you might have that you would NOT want known to advertisers who might target ads at you?

Here is a list of kinds of information that could be extracted about you. Could you check off which of these things you would be OK with know these things about you and target their ads at you accordingly or if you would NOT be OK with that?

HAND OUT LIST

a. What foods and restaurants you like
b. Your preferred entertainment activities (e.g. films, music, video games, attending sports etc…)
c. What preferences you have for consumer goods like clothes, cars, electronics etc…
d. The fact that you are looking for a new job
e. The fact you are soon getting married
f. Your hobbies and leisure activities (e.g. gardening, hiking, sports, crafts etc…)
g. That you work out and or belong to a gym
h. Financial information like your approximate income level, retirement plans, credit applications
i. Where you have travelled to or plan to travel to
j. Issues you are interested in like environmental protection, foreign policy, politics etc…
k. Your personal health and medical conditions you may have
l. That you are online dating
m. Your love life, sexual orientation or sexual preferences
n. Your marital and familial status – whether you are divorced, whether you have kids etc…
o. Your religious beliefs or political opinions
p. Your ethnic origin
q. The content of your private messages and who you correspond with
r. Where exactly you are located

What makes you willing to divulge some of this information and not the rest? What criteria do you apply?

6.0 Consent and opting out (10 minutes)

As far as you know, do any of us have any choice in whether or not to share all this information online? What choices do we have? Can we opt out?

Do any of you ever read the confidentiality terms and conditions on websites you visit? Why? Why not?

Is there a way to force companies to stop tracking your online activities? How would you do that?

Some companies do actually provide an online form you can fill out to forbid them from tracking your online activities. One way is to click on an icon called “Ad Choice” that you may see on many online ads. If you click on that – you will still see ads online, but they will no longer be targeted at you based on your preferences.

Did any of you know that existed? Does it actually work?

Other companies and providers such as Google have another service. You can go into your own profile and remove some interests they may have identified for you. For example, maybe they have “science-fiction” listed as an interest of yours. You can go in and “uncheck” that so that you no longer receive sci-fi related advertising.

Did any of you know that existed? What do you think of that?

7.0 Conclusions

What are your final thoughts based on everything we have discussed? What surprised you, if anything?

Do you think online companies know too much about you or is it acceptable?

What are your concerns?

Part of why social media like Facebook and Twitter are free is that they make money by selling information about you like what we have been discussing. What if you could tell Facebook to stop tracking any of your behaviour – but in exchange you had to start paying to use Facebook? How much would you be willing to pay to use these services and never have your behaviour tracked anymore?

Is this information that websites and social media collect about your worth something?

Thanks for your participation!