option consommateurs

How Free is “Free”?
Setting limits on the collection of personal information for online behavioural advertising

RESEARCH REPORT

Produced by Option consommateurs
and presented to Industry Canada’s Office of Consumer Affairs

June 2015

Option consommateurs received funding for this report under Industry Canada’s Program for Non-Profit Consumer and Voluntary Organizations. The opinions expressed in the report are not necessarily those of Industry Canada or of the Government of Canada.

By Alexandre Plourde

Legal Deposit
Bibliothèque nationale du Québec
National Library of Canada
ISBN 978-2-89716-024-1

Option consommateurs
50, Ste-Catherine Street West, Suite 440
Montreal (Quebec)
H2X 3V4
Phone: 514 598-7288
Fax: 514 598-8511

Email: info@option-consommateurs.org
Website: www.option-consommateurs.org

Table of Contents

Option consommateurs

MISSION

Option consommateurs is a not-for-profit organization whose mission is to promote and defend the rights and interests of consumers and ensure that they are respected.

HISTORY

Option consommateurs has been in existence since 1983, when it arose from the Associations coopératives d’économie familiale movement, more specifically, the Montreal ACEF. In 1999 it joined forces with the Association des consommateurs du Québec (ACQ), which had already pursued a similar mission for over 50 years.

PRINCIPAL ACTIVITIES

Option consommateurs helps consumers experiencing difficulties, provides budget consultation and conducts sessions on budgeting, indebtedness, consumer law and the protection of privacy. We also make free visits to low-income households in order to improve energy efficiency in their homes.

Each year we produce research reports on important consumer issues. We also work with policy makers and the media to denounce unacceptable situations. When necessary, we institute class action suits against merchants.

MEMBERSHIP

In its quest to bring about change, Option consommateurs is active on many fronts: conducting research, organizing class action suits, and applying pressure on companies and government authorities. You can help us do more for you by becoming a member of Option consommateurs www.option-consommateurs.org

Acknowledgments

The research was conducted by Mtre. Alexandre Plourde, who also drafted this report, under the supervision of Ms. Maryse Guenette, head of Research and Representation at Option consommateurs, with the financial support of Industry Canada’s Office of Consumer Affairs.

The author wishes to acknowledge the work of all the employees, interns and volunteers at Option consommateurs who, in one way or another, collaborated in this research. He would especially like to thank Mivania Henry and Joanie Provost Brisebois, paralegal trainees at Ahuntsic College, and Amadou Barry, Boillat François-Madfouny and Linh Nguyen, law students at Université de Montréal.

The author also wishes to thank all those who agreed to grant him an interview in the context of this research: Manon Arcand, marketing professor at UQÀM, Stéphane Gauvin, marketing professor at Université Laval, Éloïse Gratton, partner, national co-leader, Privacy Practice Group at Borden Ladner Gervais LLP, Jacques Nantel, marketing professor at HEC Montreal, Pierrot Péladeau, expert in the social assessment of information systems, Alexandre Sagala, Vice President, Publipage, Jacques St Amant, lecturer in consumer law at UQÀM and Nicolas Vermeys, professor in the Faculty of Law at Université de Montréal.

Finally, the authors wish to thank Professor Jean-Pierre Beaud, Dean of the Faculty of Political Science and Law at UQÀM and Bruno Marien, sociologist and lecturer in the Department of Political Science and Law at the same university for their methodological support.

Summary

Google, Facebook, Yahoo!, YouTube ... most of the websites we visit every day don’t charge us a single penny for the use of their services. One of the major ways in which free Internet service providers finance their activities is through online behavioural advertising (OBA). This marketing strategy tracks the Web user’s browsing activities in order to create a virtual profile that will permit the companies to insert “tailored” ads into the pages the user visits.

An analysis of the privacy protection policies of the major free internet service providers in Canada reveals that these companies collect a stupefying quantity of data on their users, and can attach a considerable number of tags to each user profile. These policies impose very few limits on the companies concerning the use of users’ personal information for advertising purposes.

The Canadian consumers in our focus groups stated that they were surprised at the extent of the collection and use of their personal information for the purposes of OBA. In general, they said that the closer the information gets to their sphere of privacy, the less want it to be used for OBA purposes. They also expressed a desire to be better informed about OBA and to be able give or withhold their consent to it.

Contrary to what the providers suggest in certain of the policies analyzed, most of the data collected on Internet users for OBA purposes would in fact be considered personal information in the eyes of the law. Although this personal information constitutes a medium of exchange that allows consumers to access services online without charge, there is a marked discrepancy between the companies’ legal obligation to collect only as much personal information as they need for the purposes they state and the almost unlimited amount of data they actually do collect. Also, given the insufficiency of the information disclosed and the shortcomings of the available opting-out mechanisms, it is doubtful that the consent obtained from consumers could ever be truly informed.

Although the law does not define fixed categories of personal information whose collection or use is prohibited for the purposes of OBA, it does stipulate higher requirements of consent for what it considers to be sensitive personal information. While the law adopts a contextual definition of sensitivity of information, the companies, which operate in a virtual context, have themselves decided which categories of personal information they consider sensitive. Consequently, interpretations may vary substantially from one company to another. In addition, many companies do not seem to consider certain types of information, such as geolocation and the contents of personal correspondence, to be sensitive at all.

In order to provide companies with better guidance, Option consommateurs recommends in particular that guidelines be adopted that explicitly designate certain categories of personal information as sensitive, without limiting the scope and flexibility of the law. To ensure that consumers are able to consent to OBA in an informed manner, Option consommateurs also recommends that simple, effective and harmonized mechanisms be set in place to allow consumers to give informed, active consent to the collection of their personal information for the purposes of OBA.

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... most of the sites that Web surfers visit every day don’t charge their users a single penny. Yet this apparent freebee comes at a cost for consumers.

In exchange for a Facebook account or a query on Google, users have to agree to disclose a considerable amount of personal information: browsing history, search entries, online shopping, IP address[2], etc. This information, once amassed, is used to set up a profile of the consumer in order to guess their habits, their areas of interest... and to display advertisements on the websites they visit.

This practice, called online behavioural advertising (hereinafter “OBA”), helps fund the online content that is offered free of charge. Since this type of advertising is reportedly twice as effective as non-targeted online advertising[3], it seems likely that the more online companies learn about their users, and the more they can use the information they have about them to determine their specific characteristics, the more advertising revenue they will be able to generate.

It is of course legitimate for companies to try to maximize their profits. However, the amount and type of personal information collected for this purpose and the use that is made of it are cause for concern.

[1] Alan M. Turing, “Computing Machinery and Intelligence” (1950) 59-236, *Mind*, 433, p. 446

[2] An IP (Internet Protocol) is an identification number assigned to each device using the Internet that makes it possible to communicate information over the network.

[3] Howard Beales, *The Value of Behavioral Targeting*, a study presented to the Network Advertising Initiative, 2010

Research Questions

Studies conducted in Canada have pinpointed several difficulties raised by OBA with regard to the protection of privacy, such as gaps in the information disclosed to the consumer concerning the information they collect or in obtaining their consent[4].

However, despite the wide range of information that companies are able to collect on Internet users, little is known about the types of information that consumers are willing or unwilling to disclose in the context of OBA, or more generally, about the issues raised by the collection of each type of personal information. Studies abroad, however, suggest that the social acceptability of this practice varies depending on the type of information collected: one study in the United States, for example, indicates that Internet users feel less inclined to disclose certain types of information, such as their contact information or their geographical location, for OBA purposes[5].

What are the practices of Canada’s leading free Internet service providers? What personal information are consumers willing to disclose to get a “free” service on the Internet and what other information are they unwilling to share? Is there some information that should not be collected for the purposes of OBA? Which types of collection and uses of personal information are legitimate for the purposes of providing a free service? Is current Canadian law up to these challenges?

Methodology

To answer these questions, we first sketched out a portrait of how OBA operates (section 1). We then analyzed the privacy policies of the major free Internet service providers (section 2). In order to obtain the views of consumers, we held focus groups (two in Toronto and two in Montreal) with Canadians of all ages who use the Internet regularly (section 3). Finally, we conducted legal research in Canada, the United States and European Union on the standards governing information that may be collected for the purposes of OBA (section 4).

To aid us in our analysis, we also conducted interviews with experts in marketing, new technologies and privacy protection. We interviewed Manon Arcand, a marketing professor at UQÀM, Stéphane Gauvin, a marketing professor at Université Laval, Éloïse Gratton, a partner and national co-leader, Privacy Practice Group, at Borden Ladner Gervais LLP, Jacques Nantel, a marketing professor at HEC Montreal, Pierrot Péladeau, an expert in the social assessment of information systems, Alexandre Sagala, Vice President of Publipage, Jacques St-Amant, lecturer in Consumer Law at UQÀM and Nicolas Vermeys, a professor in the Faculty of Law at Université de Montréal.

[4] See especially: Janet Lo, *A “Do Not Track List” for Canada?*, report presented to Industry Canada’s Office of Consumer Affairs by PIAC, 2009; Mary Foster, Tina West, Avner Levin, *The Next Frontier: Targeted Online Advertising and Privacy,* Report to the Office of the Privacy Protection Commissioner of Canada, Ryerson University, 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. A few notes on how OBA operates

The deployment of banners, pop-ups or other promotions on the Internet might appear very trivial. For most Internet users, advertising is usually an uninteresting blip on the virtual landscape. Yet behind many of these ads is a complex mechanism involving a multitude of actors that goes into operation in a fraction of a second every time a Web user navigates from one Web page to the next.

1.1. Definition

Basically, the way OBA works is simple: by tracking users on the sites they consult, companies compile lists of their browsing activities, such as the pages they visit, how long they spend there, the search queries and purchases they perform[6]. This data is then processed using algorithms that allow advertisers to guess their preferences, interests or tastes. The resulting profile will be used to send targeted advertisements to the user[7]. For instance, science fiction buffs will receive ads for the latest David Cronenberg boxed DVD set and physics enthusiasts will get ads on the works of Albert Einstein.

Profiles constructed on the basis of Web users’ activities do not necessarily include their name, contact information or any specific identifiers. The user may just be identified “pseudonymically,” that is, by using information such as the number of a cookie, an IP address, or a unique device identifier. Strictly speaking, it is usually the browser or device that the individual uses that is actually being monitored. The ultimate goal of advertising is not to identify the consumer *per se*, but simply to produce the most targeted advertising possible; in general, however, the amount of information collected would easily be sufficient to identify the person profiled by OBA practices[8].

In theory, there are other forms of online advertising besides OBA. These are referred to by a variety of names. For example, “contextual” ads are those that are displayed depending on the page the user is currently viewing: an ad for windshield washer on an automobile site, for example. “Socio-demographic” advertising targets users based on their age, gender, or some other demographic criterion. So-called “geographical location” advertising focuses on where the consumer is located.

In practice, the differences between the types of online advertising are far from clear. Companies routinely combine several kinds of data to better target consumers – not just data derived simply from tracking their activities on the Internet. For example, the privacy policies of

[6] Janet Lo, *A “Do Not Track List” for Canada?*, report to Industry Canada’s Office of Consumer Affairs by PIAC, 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; Zhao Qi, Zhang Yi, Lucian Vlad Lita, “Have Your Cake and Eat It Too! Preserving Privacy While Achieving 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] We will come back to this in Section 4.1

Google and Facebook allow them to combine behavioural data with other types of information, such as demographic or geographical location data[9].

Given this mix, this report will consider OBA to be any form of advertising involving the tracking of customer activity over a period of time, whether in combination with other information or not. This monitoring may be conducted directly by the site the user is viewing or by a third party in partnership with this site. Accordingly, our definition may include practices that are not always considered OBA in the literature, such as profiling for advertising purposes by social media[10].

1.2. An invisible industry

The OBA industry responds to market logic. Advertisers[11] need space to display their ads; Websitewebsites[12] offer it, for a fee. In theory, nothing prevents advertisers from making direct contact with a site in order to negotiate the terms for displaying their ads, and vice versa. However, this approach is inefficient in a universe as diffuse as the Web, where negotiating advertising agreements one at a time with thousands of sites would be a mammoth proposition that none but the biggest players could hope to carry off.

The advertisers and the sites therefore need assistance to match the supply with the demand. To do this, there are two types of companies, "ad networks"[13] and "ad exchanges," that act as intermediaries[14]. Ad networks compile an inventory of advertising space offered by websites and put it up for sale, earning a commission on each space sold[15]. Ad exchanges offer a similar service, but by auctioning advertising slots, in real time, in just a few milliseconds.

It is mainly these intermediaries between websites and advertisers that are responsible for tracking and profiling Internet users. In fact, whenever an advertisement is displayed on a site through an ad network or an ad exchange, they use this opportunity to gather information on

[9] We will deal with the content of these policies in more detail in Section 2

[10] Our definition is actually broader than, for example the one used by Janet Lo in: Janet Lo, *A "Do Not Track List" for Canada?*, report to the Industry Canada's Office of Consumer Affairs by PIAC, 2009 pp. 20-21. In this report, the author refers to the definition used by the FTC in the U.S., explaining that the definition only includes collection by third parties. In contrast, the definition of OBA found on Wikipedia is broad and inclusive, and is closer to our own interpretation. See: http://en.wikipedia.org/wiki/Behavioral_targeting. The Office of the Privacy Protection Commissioner of Canada (hereinafter "OPC") also remains quite broad in its definition of OBA. See: *Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing, 2011*, pp. 14-15

[11] Also called "buyers"

[12] Also called "publishers" or "sellers"

[13] Also called "advertising brokers"

[14] There are actually many typologies and names used to describe these various stakeholders, which vary from one author to another. See: Mary Foster, Tina West, Avner Levin, *The Next Frontier: Targeted Online Advertising and Privacy,* report presented to the Office of the Privacy Protection Commissioner of Canada by Ryerson University, 2011, pp. 8-11

[15] Readers wishing to better understand the distinctions between these two types of intermediaries will find this article by Nitin Narang interesting: http://www.mediaentertainmentinfo.com/2014/02/5-concept-series-what-is-the-difference-between-ad-exchange-and-ad-network.html/

the user who is viewing the advertisement. They record this information and use it to set up the user’s profile, on the basis of which they select which ads are the best ones to display. In some cases, certain players can combine these roles, offering advertising space for sale and acting as ad publishing sites. For example, Facebook collects information on its own users in order to target the ads of the companies who want to promote their products on their platform.

Since most major sites have partnerships with several intermediaries at once[16], a user’s browsing data can be sent to multiple third parties every time they navigate from one Web page to another[17]. Similarly, since these intermediaries also have partnerships with many sites, they will be able to track the user at numerous Web locations. This will also allow them to post targeted ads on sites that are not necessarily linked to the products advertised.

To this already complex body of sites, advertisers and third parties transplant myriad other companies that specialize in specific roles within OBA such as retargeting[18], data mining[19] or targeting optimization. Others offer related services, such as media placement assessment, in order to assure advertisers that their money is well spent[20]. Others offer interfaces to the sites or advertisers that allow them to sell or buy advertising space across multiple ad networks or ad exchanges at the same time[21].

Given the high number of players and activities involved, it is difficult to define the boundaries or describe all the intricacies of the OBA industry[22]. On the one hand, scores of players may handle data from one user or provide services through OBA[23]. On the other, many of these companies perform several roles at the same time; Google, for example, provides services to users and also operates as an ad network.

[16] For example, in 2009, PIAC reported that Yahoo! Canada has a relationship with almost 50 ad networks. See Janet Lo, *A “Do Not Track List” for Canada?*, report to Industry Canada’s Office of Consumer Affairs by PIAC, 2009, pp. 26-27. In the U.S. , the report KnowPrivacy, published in 2009, eloquently reveals the extent of the collection of information on users by the largest U.S. sites. See: Joshua Gomez, Travis Pinnick, Ashkan Soltani, KnowPrivacy, UC Berkeley School of Information, 2009

[17] A simple browsing session with the Ghostery extension, which identifies cookies stored on a user's browser, reveals an impressive number of advertising cookies from *third parties*. Among these are names such as AdGear, AppNexus, ADTECH, Datalogix or DoubleClick.

[18] The aim of “retargeting” or “remarketing” is to reach consumers who were interested in buying a product, for example, by navigating to the purchase page of this product, but ultimately did not purchase the product in question.

[19] OPC, *Report on the 2010 Office of the Privacy Commissioner of Canada’s Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing,* 2011, p. 30

[20] For example, AdExpose, a company owned by ComScore, is a player that offers this service.

[21] To make things easier for everyone involved, these companies allow advertisers and websites to access the offer or demand of several platforms at once. We call these companies “demand-side platforms” (DSP) when they provide services to advertisers and “supply-side platform” (SSP) when they address sites.

[22] Even the OPC, in its 2011 consultations on OBA, claimed not to have been able to get a complete picture of the OBA environment in Canada. OPC, *Report on the 2010 Office of the Privacy Commissioner of Canada’s Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing*, 2011, p. 34

[23] To give an idea of the complexity of this advertising system, IAB Canada has sketched out a portrait of it in a diagram: http://iabcanada.com/files/IABCanada-TheCanadianProgrammaticLandscape.pdf. The diagram, which is apparently incomplete and limited to the Canadian context, is inspired by the one produced by LUMA Partners in the U.S., which provides a more detailed overview of the interactions and complexity of this industry: http://www.lumapartners.com/resource-center/lumascapes-2/

This multiplicity of actors and roles, however, should not obscure the fact that this is an industry which in recent years has experienced both a high degree of concentration and a phenomenal increase in revenues. A very few intermediaries have succeeded in capturing a significant share of the online advertising market; in the absence of competition, their ads may now appear on even more sites, thereby allowing them to monitor vast portions of the Internet[24]. At the same time, from 2003 to 2013, online advertising revenues in Canada increased from $364 million to over $3.5 billion. According to the Interactive Advertising Bureau of Canada, the Internet has become the medium with the largest advertising revenues in the country[25]. The online advertising industry is admittedly complex and invisible; but that doesn’t alter the fact that huge sums of money are concentrated into the hands of just a few privileged players.

1.3. Ineradicable bugs

Several technologies have been developed to permit companies to track users on the Web. Most often, they rely on “cookies[26]”: small files stored on the computers of users who visit Web pages. A cookie generally contains a unique identifier that allows the ad network or ad exchange to recognize Web surfers on the various sites they visit. So-called “persistent” cookies are programmed to remain inside the user's computer indefinitely without self-destructing. They enable companies to permanently identify the virtual profiles of users and update them using the data they are constantly collecting about their online activities.

Since online tracking is based on the use of cookies, an instinctive strategy to avoid it would simply be to configure the browser so that it refuses to install cookies, or at least removes them automatically at the end of each browsing session. However, this method does not always produce the desired results. On the one hand, cookies are used not only to regulate advertising systems, they provide numerous services to users, and refusing them can greatly disrupt the browsing experience[27]. On the other hand, the cookie is not the only technology used by companies to track Internet users, far from it. Merely blocking or deleting cookies will not put an end to online tracking.

[24] Figures from the Interactive Advertising Bureau of Canada show that in 2013 the 20 most important players in Canada’s online advertising market monopolized 89% of revenues. See: Interactive Advertising Bureau of Canada, *Canadian Internet Advertising Revenue Survey*, 2014, p. 10. The highlight of this concentration phenomenon was probably the purchase of the DoubleClick ad network by Google in 2007. In Canada, as a result of this transaction, the Canadian Internet Policy and Public Interest Clinic (CIPPIC) made a complaint to the Competition Bureau alleging that this purchase would hamper competition in the online advertising market. However, its arguments were rejected by the Bureau, See Janet Lo, *A “Do Not Track List” for Canada?*” report to Industry Canada’s Office of Consumer Affairs by PIAC, 2009, pp. 28-31

[25] These revenues represent 28% of advertising spending in the country. In comparison, advertising revenues from print newspapers dropped, in the same interval, from $2.6 billion to $1.7 billion; the revenue generated by television and radio, meanwhile, remained substantially stable. See: Interactive Advertising Bureau of Canada, *Canadian Internet Advertising Revenue Survey*, 2014, p. 16

[26] Variously called “Web cookies” “browser cookies” or “tracking cookies.”

[27] Cookies make it possible to retain information about a user from one Web page to another, thereby enabling all kinds of functions such as online shopping.

In fact, alongside the usual cookies, companies deploy an arsenal of technology to ensure they are able to track Internet users regardless of how their browsers or devices are configured[28]. One of these is the “flash cookie” which is installed on the user's computer via the extension module developed by the Adobe company for playing multimedia files. “Super cookies” utilize new storage locations built into browsers to record information about users. “Beacons[29]” are small image files which, once downloaded by the browser, are used to track users. Users can also be traced using their unit’s IP address or unique identifier. Some authors even talk of the possibility of using the browser’s “fingerprint”[30] or “deep packet inspection[31].”

In short, considering that there are so many companies monitoring the Internet, and that each one may be deploying a considerable number of technologies concurrently to do so, it is in practice very difficult to avoid being tracked online.

Admittedly, some of these companies, on their respective websites, offer users the option of requesting that they no longer be tracked, or that certain categories of interests be removed from their virtual profile (see section 2). However, attempting to use these various mismatched mechanisms to evade online tracking can be a perplexing experience. Among other difficulties, users will be first asked to identify the many companies that are tracking them online, most of which they will not know. They are also asked to subscribe, one at a time, to each of the withdrawal mechanisms offered to them – a tedious task for the lay user, not to mention that there is no guarantee of the effectiveness of such mechanisms or that this exercise will cover all the companies tracking the user online.

In response to these difficulties, the Digital Advertising Alliance of Canada (DAAC) has developed a more realistic solution for users. The Canadian Self-Regulatory Program for Online Behavioural Advertising is a voluntary code that requires that behavioural advertising by participating companies be accompanied by an *AdChoices* icon (see Figure 1). By clicking on this icon or by visiting the DAAC website, users can access a page containing the promise that they will be able to opt out of being tracked by the participating companies for advertising purposes[32].

[28] For a portrait of these technologies, see, for example: OPC, *Cookies – Following the Crumbs*, 2011, online at: https://www.priv.gc.ca/resource/fs-fi/02_05_d_49_01_e.asp; Janet Lo, *A “Do Not Track List” for Canada?*, report to Industry Canada’s Office of Consumer Affairs by PIAC, 2009, pp. 20-47

[29] This technology may be referred to by different names, such as a “Web bug” or a “Web tab.” More information can be found on its operation on the Electronic Frontier Foundation page, *The Web Bug FAQ*, online at: https://w2.eff.org/Privacy/Marketing/Web_bug.html

[30] The fingerprint of a browser or device consists of an identification method (complete or partial) based on the configuration of a device. It can therefore be used even when cookies are disabled. In 2010, a study by the Electronic Frontier Foundation stated that this identification method can achieve a high degree of accuracy. See: Peter Eckersley, *How Unique Is Your Web Browser?*, Electronic Frontier Foundation, 2010

[31] Deep packet inspection allows telecommunications service providers to read the communications that pass through their network. View: OPC, *What is deep packet inspection?*, online at: https://www.priv.gc.ca/information/research-recherche/dpi_intro_e.asp. To our knowledge, deep packet inspection is not currently used for advertising purposes in Canada. However, Bell Canada's recent changes to its privacy policy, which authorizes it to use a lot of data on the activity of its customers for OBA purposes, may raise doubts in this regard. See Philippe Mercure, “Renseignements personnels: Bell s’attire les critiques,” L*a Presse,* Montréal, October 22, 2013

[32] http://youradchoices.ca/choices

Figure 1: AdChoices Icon

Although convenient, this option offered by the industry is still not perfect[33]. It should be remembered from the outset that this is a voluntary standard that depends solely on the goodwill of the participants in the program[34]. Added to that is the fact that participating companies are still permitted, for various reasons, to continue tracking consumers subscribing to the mechanism, in order, for example, to count the number of times an ad is displayed by a particular browser[35]. Similarly, they are still authorized to use certain types of information for advertising purposes, such as “demographic” or “localization” data[36]. Finally, the technological basis for this mechanism, which depends on a cookie downloaded onto the user’s machine, raises questions as to the sustainability of the choice made by the consumer[37].

In short, even if users equipped themselves with every opting-out mechanism offered by the industry, some gaps in their online anonymity would still survive. To address these, there are yet other tricks that the more experienced user can try. One of these is to activate the “Do Not Track” setting on their browser, which sends a message to the advertisers’ servers that the user does not wish to be tracked[38]. However, as we shall see, many companies neglect to comply with such messages[39]. Users can install software such as AdBlock Plus or Ghostery in their

[33] As we will see in Section 3, this opt-out mechanism is little known among consumers, who in many cases, continue to suffer from online tracking because they are unaware of their right to withdraw their consent.

[34] In the U.S., for example, the study *Tracking the Trackers* by the Center for Internet and Society at Stanford Law School revealed in 2011 that some companies did not stop tracking users even after they used the opting-out formula provided by an industry association: http://cyberlaw.stanford.edu/blog/2011/07/tracking-trackers-early-results. See also: Giovanni, Pedro 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

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

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

[37] In fact, the withdrawal mechanism is based on the installation of a persistent cookie, which could easily be erased when the browser is reconfigured.

[38] This signal is an initiative of the World Wide Web Consortium, a non-profit Web standards body: http://www.w3.org/2011/tracking-protection/drafts/tracking-dnt.html. The Do Not Track option should not be confused with the private browsing mode offered by some browsers, which, as the developers of Firefox admit, does not guarantee anonymity online: https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history. The signal should also not be confused with the “Do Not Track List,” i.e. an opting-out mechanism based on a centralized list of persons not wishing to be tracked, similar to National Do Not Call list of numbers, whose implementation was supported by several consumer organizations in the United States.

[39] In this regard, see also: 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

browsers, which allow or blocks “pop-up” ads or block certain cookies; nevertheless, even these programs do not necessarily put a stop to the underlying online tracking.

Consumers therefore have various means available to them designed to evade online tracking, but in general these may be only partially effective. Moreover, these methods remain very little known by the general public, are inactive by default (they require positive action on the part of users who want to use them) and sometimes require advanced technical knowledge to install and use.

2. Analysis of privacy protection policies

To obtain more information on the practices of online companies in Canada, on the information they collect and what they do with it, we analyzed the privacy policies of the most important free Internet service providers in the country.

We defined “free Internet services” as services offered to Internet users with access to essential features at no monetary charge to the user, and at least part of whose business model is based on OBA as defined in this report[40]. These include search engines such as Google, and social media applications such as Facebook. They may also include any site offering free content to users, such as a news sites or sites offering online videos. Sites based on a “freemium” formula, i.e. ones that combine paid and free access (e.g. LinkedIn) may be included under this definition, insofar as they also practice OBA.

In setting up our sample, we selected, from among the websites most visited by Canadians, the ones that best fit this definition of free service provider[41]. We quickly found that, except in a very few cases[42], the most popular sites in Canada have adopted a business model that uses OBA. In addition, several of these sites belong to the same company and direct consumers to the same privacy policy. For example, YouTube, owned by Google, refers users to the same policy as the Google search engine and Gmail email service. To avoid duplication, we considered the policy used by several companies as a single component in our sample.

[40] This definition is inspired by the one found in Kent Sebastian’s report, *No Such Thing as a Free Lunch: Consumer Contracts and “Free” Services* submitted to Industry Canada’s Office of Consumer Affairs by PIAC, 2014, which defines a free service as “a free online service that monetizes user-provided value.”

[41] To do this, we used eMarketer data and those of the Alexa Rank, which get similar results. See: eMarketer, *Top 10 Websites Among Internet Users in Canada Ranked by Market Share of Visits*, June 2014; http://www.alexa.com/topsites/countries/CA. Some might argue that, since it is most often third parties that collect and use information from visitors for OBA purposes, it would have been better to study the practices of these companies directly. However, we considered that our approach truly allowed us to put ourselves in the position of consumers seeking to get information, who are not immediately aware of the existence of third parties. Nevertheless, the companies that were included in our sample generally combine several roles and state that they track users’ behaviour.

[42] One notable exception, Wikipedia, is ranked fifth in the standings, but does no online advertising. Its business model is based primarily on a participatory funding.

Finally, we analyzed the policies of the following ten companies: Google[43], Facebook[44], Microsoft[45], Yahoo![46], LinkedIn[47], Twitter[48], Kijiji[49], Amazon[50], Pinterest[51], and Imgur[52].

Due to the concentrated nature of the industry, we limited our sample to ten policies. According to the Interactive Advertising Bureau of Canada (IAB Canada), the top ten players in Internet advertising generated 82% of all revenue from Internet advertising in Canada in 2013[53]. Although the Bureau’s report does not state which companies these are, we would guess that Google and Facebook share top spots in this ranking. A look at the U.S. market should serve to convince: according to eMarketer, Google sits on top with 38.1% of Internet advertising in the

[43] Google's policy covers both the activities of the search engine and the company’s other services, such as YouTube and Gmail. We consulted Google's policy dated December 19, 2014, available online at: https://www.google.ca/intl/en/policies/. This section of the Google site contains many explanatory pages on the company’s practices; the largest of these is entitled “Privacy Policy.” There are also other relevant pages, including “Technologies and Principles,” “FAQ” and “Terms of Service.”

[44] We studied two versions of the Facebook policy. We essentially based our analysis on the most recent, dated January 30, 2015, found at: https://www.facebook.com/about/privacy/. We also consulted related pages such as “Facebook Ads Controls,” “Cookies Policy” and “Terms.” The earlier version was dated November 15, 2013.

[45] Several services are attached to the Microsoft banner, including Windows Live Mail, live.com, Bing and MSN Canada, which refer users to the “Microsoft Privacy Statement” dated January 2015, found at: http://www.microsoft.com/privacystatement/en-us/core/default.aspx. However, Bing and MSN also refer users to a separate policy: “Privacy Statement Bing and MSN,” dated January 2015 and available at: http://www.microsoft.com/privacystatement/en-us/BingandMSN/default.aspx. Both documents contain a great amount of detail and occasionally link to other pages, including the general Microsoft OBA opting-out page and the privacy protection policy of Microsoft Advertising, the advertising network operated by Microsoft. Despite these distinctions, we analyzed all Microsoft services concurrently, making adjustments as required.

[46] Yahoo! Canada has a policy for all its services. Its very brief policy, dated July 12, 2010, is available at: http://info.yahoo.com/privacy/ca/yahoo/. Yahoo! Mail also has a short separate policy, which refers to the general Yahoo! policy; for more details: http://info.yahoo.com/privacy/ca/yahoo/mail/ymail/details.html. There are some additional pages that define certain terms used, and a link to the Yahoo! OBA opting-out page. The terms of use are published at: https://info.yahoo.com/legal/ca/yahoo/utos/utos-ca01.html.

[47] We consulted the LinkedIn policy, dated October 23, 2014, available at: https://www.linkedin.com/legal/privacy-policy. We also reviewed the terms of use for this service at: https://www.linkedin.com/legal/user-agreement.

[48] We consulted the Twitter policy, dated September 8, 2014, at: https://twitter.com/privacy. Twitter also provides its users with additional pages on related topics such as “Twitter’s use of cookies and similar technologies” or “Your Privacy controls for tailored ads The “Twitter Terms of Service,” dated September 8, 2014, are available at: https://twitter.com/tos.

[49] We consulted the Kijiji policy, dated July 25, 2014, available at: http://help.kijiji.ca/helpdesk/policies/kijiji-privacy-policy The terms of use are available at: http://aide.kijiji.ca/centredaide/politiques/conditions-d-utilisation.

[50] We consulted the Amazon policy, dated March 3. 2014, available at: http://www.amazon.ca/gp/help/customer/display.html/180-9291331-5703514?nodeId=918814. A specific page is devoted to Amazon’s OBA practices: https://www.amazon.ca/gp/BIT/InternetBasedAds. The Conditions of Use, dated February 17, 2015, are available at: https://www.amazon.ca/gp/help/customer/display.html?nodeId=918816.

[51] We consulted the Pinterest policy, dated October 19, 2014, available at: https://about.pinterest.com/en/privacy-policy. There are also additional pages, including “Personalization and data” and “Third-party analytics or advertising providers Pinterest uses or allows.” The Terms of Service are available at: https://about.pinterest.com/en/terms-service. Our last visit to this page dates from January 9, 2015.

[52] We consulted very short Imgur policy dated January 14, 2014, at: http://imgur.com/privacy. The Terms of Use, dated October 22, 2014 are available at: http://imgur.com/tos.

[53] Interactive Advertising Bureau of Canada, *2013 Actual+2014 Estimated Canadian Internet Advertising Revenue Survey*, conducted by Ernst & Young and commissioned by the Interactive Advertising Bureau of Canada, September 17, 2014, p. 10

U.S. in 2014, followed by Facebook with 9.8%[54]. This means that Google and Facebook account for almost half of the online advertising market in the United States. Since the Canadian market has similar characteristics to the U.S. market, one can realistically assume that we will find similar ratios of revenue sharing here. In addition, these are also the companies most visited by Internet users in Canada.

2.1. Sparse documentation

We generally found the links to the privacy policies of selected services in discrete mentions in footnotes. Although some policies are couched in heavy, hard-to-understand verbiage, others are presented in a more accessible language and format: Google and Facebook noticeably make an attempt to explain their practices to users in clear, accessible language. Facebook, for example, makes sure to include an icon pointing to shortcuts on privacy protection in its navigation bar and presents the information in a generally user-friendly form.

Most often, the company publishes two main documents: one explaining the terms of service[55] and the other its policy regarding the management of users’ personal information[56]. Relevant information is sometimes included under different headings and is spread over several pages. For example, in addition to its privacy protection policy, Amazon posts a separate page explaining what interest-based advertising specifically entails[57]. In several cases, the policies studied state that they also apply when the user accesses the service via a mobile application.

Since determining what each service’s privacy policy involves exactly is sometimes unclear, we also, where necessary, studied other related documents, including these services’ conditions of use, additional explanatory pages accessible online, and even ads for advertising space aimed at advertisers.

2.2. Unlimited collection

Reading these policies should be enough to convince anyone: in targeted advertising, the companies studied gather every last scrap of information they can find on the Internet. Nothing escapes scrutiny, whether it be data obtained through tracking Internet activities, or data obtained at the time a user opens an account.

First, they collect information on the users’ activities. This naturally includes the pages they visit and the time spent on each[58]. They may also log, for example, the videos they watch on

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

[55] These terms may be presented under different names, such as “Terms of Use,” “Service Contract,” “Terms and Conditions” or “Terms of Service”

[56] Again, such documents may take various names, such as “Privacy Policy,” “Data Use Policy” or “Privacy Statement”

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

[58] The collection of users’ browsing activities is often explained in very broad terms. For example, Google adopts a very wide definition of the concept of “data we collect when you use our services” by including “information about the services that you use and how you use them, like when you watch a video on YouTube, visit a website that uses

YouTube, the purchases they make online or the ads that catch their attention. In short, every mouse-click is tracked.

Each service also collects data specific to the functionalities it offers. The Google and Bing search engines retain the keywords used in searches. Social media is interested in the “Likes” (or “+1” in Google), and in the comments and content the user shares. Online shopping platforms are no exception: for example, Amazon’s policy mentions that a consumer’s “shopping list” could be used for advertising purposes.

They are also interested in the relationships between the users of their service by trying to guess what type of relationship users have with each of their contacts. Facebook, the universally popular platform for online socializing, explains this practice as follows:

> We collect information about the people and groups you are connected to and how you interact with them, such as the people you communicate with the most or the groups you like to share with[59].

Even the emails a user sends or receives can be used for targeting purposes, through the use of algorithms designed to detect certain words or other items. Yahoo! explains this practice as follows:

> 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]

The consumer location is also a popular information item[61]. Companies can deploy an arsenal of means to find this information. Google, for example, gives a non-exhaustive list:

> When you use Google services, we may collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that may, for example, provide Google with information on nearby devices, Wi-Fi access points and cell towers[62].

---

our advertising services, or view and interact with our ads and content.” At Twitter, more generally it is stated interest in “how you interact with links across our Services.”

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

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

[61] We found explicit mentions of collecting information related to location in seven of the ten policies analyzed: Amazon, Facebook, Google, LinkedIn, Microsoft, Pinterest, Twitter. Three policies (Yahoo!, Kijiji, Imgur) do not specifically exclude, due to the general terms in which they are expressed, the location of the consumer; some of them also state that they collect the IP address. Google suggests that it may also compile a history of the places a consumer has visited for advertising purposes: “Your location info can also be used by any Google app. or service, including the ads you see.” See: https://support.google.com/gmm/answer/3118687?hl=enr&ref_topic=3137371

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

Several companies state that they collect, among other things, data from the GPS of mobile devices or from Wi-Fi networks, “information about wireless networks[63]” or “cell towers near your mobile device[64].” In other cases, they may use the user’s IP address to work out where they are located[65].

Companies can also seek to figure out the location of consumers by analyzing their online activities. For example, they might assume that a user who searches for information on the Eiffel Tower is in Paris[66]. This is what Google calls “implicit location information”:

> *Implicit location information* is information that does not actually tell us where your device is located, but allows us to infer that you are either interested in the place or that you might be at the place. An example of implicit location information would be a manually typed search query for a particular place.[67]

To all of this information is attached a multitude of other technical data. For example, most of the above data collections also provide an opportunity to gather metadata, i.e. data that provides information on other data[68]. For example, in addition to the key words in a query from a browser, the time and date it was issued may also be recorded[69].

More generally, it is possible to collect various digital or technological information about the user’s device: the device model, its unique identifier[70], the operating system, the network address or even the telephone number assigned to the device. Google also says it collects “telephony log information like your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls[71]”. To this Facebook adds that it collects “battery level and signal strength[72]”. Amazon adds:

> 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

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

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

[65] The IP address, the number assigned to each computer connected to the Internet, can certainly provide valuable geographical indicators, but a service provider can sometimes assign IP addresses from other geographical sectors to certain clients. In addition, a unit’s IP address station may vary during the same period. For these and for various technical reasons, geographical location based on IP address generally remains a more approximate localization method than those using data originating from a mobile device. A report by IAB Canada gives this targeting method an 88% accuracy level within a radius of 40 kilometers. See: IAB CANADA, *GeoTargeting Online* at: http://iabcanada.com/files/IABCanada_Geo-TargetingOnline.pdf

[66] This example is taken from Google's policy.

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

[68] OPC, *Metadata and Privacy, A Technical and Legal Overview*, October 2014, p. 1

[69] It is also possible to record a large amount of other contextual information. Google gives as examples IP address, browser configuration, location and any unique identifier contained in cookies. Bing lists similar information.

[70] The unique identifier of a device is a string of characters that identifies a device such as a mobile phone. A device may have several of these identifiers for various purposes, including advertising.

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

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

> certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page.[73]

This means that even areas the user's cursor wanders over, or pages he scrolls through, can be recorded.

On the face of it, one would think that such a wide collection of information could only be carried out while someone is actually using the company's services, i.e. when users are on the company’s platform or visiting its website. However, some companies also have the opportunity of following their activities outside their immediate territory. For example, companies operating ad networks, including Google[74], state that they are able to track consumers at many other locations on the Web, whenever they visit any one of the many pages that use their services to displays ads.

Social media are no exception. Facebook, for example, suggests that it is able to keep track of “activity on websites and applications outside of Facebook[75]” when these sites embed their “Like button or Facebook Login[76]” – what are known in the virtual jargon as “social plugins” – or when they use their advertising services. Twitter, for its part, says it may use tracking data from third parties to improve its ad targeting:

> Third-party ad partners may share information with us, like a browser cookie ID, website URL visited, mobile device ID, or cryptographic hash of a common account identifier (such as an email address), to help us measure and tailor ads. For example, this allows us to display ads about things you may have already shown interest in off of our Services.[77]

Some companies also reserve the option to buy information from other sources. This is the case with Microsoft, which states: “We may get additional information about you, such as demographic data we purchase from other companies[78].”

In short, most of the companies studied have tentacles that extend far beyond the sphere of the services they delivery. They utilize various means to monitor the activity of their users, and even those who do not use their services.

2.3. Consumer labelling

The policies we went through allow companies to process the data they collect in every possible way in their quest to optimize ad targeting. None of the policies directly linked each type of information collected to the precise use to be made of it. They instead chose to give a long list of

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

[74] Google also operates the DoubleClick and Google Adworks networks.

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

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

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

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

the kinds of information that may be collected, followed by a general statement that any of this data could be used for advertising purposes. The Facebook policy bluntly states:

> We want our advertising to be as relevant and interesting as the other information you find on our Services. With this in mind, we use all of the information we have about you to show you relevant ads.[79]

This not only includes data about consumers’ online activity, but also other information that the company already has, such as information that they disclosed when subscribing to the service (gender, age, employment). In short, anything that can be learned from a user’s account can be used to attribute fields of interest to their virtual double.

That said, despite the generality of such statements, we should note that many companies take the trouble to give their users additional explanations or concrete examples in order to demystify their advertising practices. Several supply multiple explanatory pages[80] or dot their policies with concrete examples, which can be refreshing in the midst of what is often dry reading. This is an illustration that Facebook gives of its advertising practices:

> For example, if a person “likes” the “Star Trek” Page and mentions “Star Wars” when they check into a movie theater, we may conclude that this person is likely to be a sci-fi fan. Advertisers of sci-fi movies, for example, could ask us to target “sci-fi fans” and we would target that group, which may include you. [81]

Companies also provide illustrations of certain more specific practices. For example, Google explains retargeting as follows:

> You may see ads for products you previously viewed through what's known as remarketing. Let’s suppose you visit a website that sells golf clubs, but you don’t buy those clubs on your first visit. The website owner might want to encourage you to return and complete your purchase. Google offers services that let website operators target their ads to people who visited their pages.[82]

Data from third parties may also be combined with data held by the company to target a certain group of people. Twitter explains:

> Here’s one way it would work. Let’s say a flower shop wants to advertise a Valentine’s Day special on Twitter. They’d prefer to show their ad to floral enthusiasts who subscribe to their newsletter. To get the special offer to those people, who are also on Twitter, the shop may share with us hashed emails from their mailing list. We can then

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

[80] Yahoo! for example, explains its advertising practices with regard to email service on its “FAQ” page: http://info.yahoo.com/privacy/ca/yahoo/mail/ymailfaq/

[81] This excerpt is from the Facebook privacy policy dated 15 November 2013. https://www.facebook-com-data-use-policy-tos

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

> match that to a hash of emails that our users have associated with their accounts in order to show them a Promoted Tweet for the Valentine's Day deal on Twitter.[83]

However, despite these few scattered examples, it is clear that the emphasis is on generalities. While we know that consumer data will be collected and used to flesh out their interests profile, the exact data used for this is difficult to understand, and even less is known about the algorithms that will be used to categorize a consumer within a given niche.

While they do not make their algorithms public, some companies do let users see what kinds of interest categories they can assign to a profile[84]. This is true of Google and Yahoo!, which allow consumers to consult such lists. On Facebook, we were also able to have a look at the profiling attributes used by consulting the representations made to advertisers[85]. These lists, which differ from one company to the next, are organized into broad categories, which are further divided into very specific subcategories[86].

The initial categories relate to very wide, diverse themes that cover vast fields of interest. Google lists over twenty of these, such as "Food & Drink," "Animals & Pets," "Autos and Vehicles," "Beauty & Fitness" or "Jobs & Education"[87]. Facebook proposes ten or so similar themes, including "Entertainment," "Hobbies and activities," "Sports and outdoors" or "Technology"[88]. The company also offers the opportunity to target consumers based on their alleged behaviour, such as playing games online or frequently making the same journey. Yahoo! also offers about fifteen of the same types of themes designated under names such as "Consumer Packaged Goods," "International Interest," "Life Stages," etc.[89]

While most of these targeting criteria are fairly obvious, others seem more obscure. For instance, the category "Business and Industry" on Facebook, covers interests that could include credit and personal finances; the category "Family and relations" covers interests such as

---

[83] https://support.twitter.com/articles/20170405-your-privacy-controls-for-tailored-ads#

[84] We found Google's "ad interest categories" here: https://support.google.com/ads/answer/2842480?hl=en. The Yahoo! Categories are available at: https://info.yahoo.com/privacy/ca/yahoo/opt_out/targeting/asc/details.html

[85] We found Facebook's targeting criteria at: https://www.facebook.com/ads/create/. The pages aimed at potential advertisers provide a clear overall explanation of how consumers' personal information can be used to target them. See: https://www.facebook.com/business/a/online-sales/ad-targeting-details

[86] Note that the typologies we looked at correspond fairly well to the Network & Exchanges Quality Assurance Guidelines developed by the American branch of the IAB, which propose a standardized typology aimed at making the industry more efficient. This typology has more than twenty major themes, each of which includes a number of second-level subcategories. Companies that wish to adhere to this standard do not have to fully respect the suggested categories "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." See: *IAB Network & Exchanges Quality Assurance Guidelines*, 2010, pp. 10-12

[87] The 25 categories listed by Google are: Arts & Entertainment, Autos & Vehicles, Beauty & Fitness, Books & Literature, Business & Industrial, Computers & Electronics, Finance, Food & Drink, Games, Hobbies & Leisure, Home & Garden, Internet & Telecom, Jobs & Education, Law & Government, News, Online Communities, People & Society, Pets & Animals, Real Estate, Reference, Science, Shopping, Sports, Travel, and World Locations.

[88] The nine categories listed by Facebook are: Business and industry, Entertainment, Family and relationships, Fitness and wellness, Food and drink, Hobbies and activities, Shopping and fashion, Sports and outdoors, and Technology.

[89] The 16 categories listed by Yahoo! are: 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, and Travel.

marriage; “Health” covers interests in dieting, fitness or bodybuilding. The Google category “People & Society” includes child education, social problems and militancy, while the category “Law & Government” covers interests as diverse as military affairs and law in general.

Under these initial categories, are hundreds, even thousands, of specific niches grouped into subcategories identifying a myriad of interests, ranging from “Insects & Entomology” to “Oil & Gas” through “Yoga & Pilates.” For example, the “Outdoors” subcategory of “Hobbies & Leisure,” lists interests as varied as “Hunting & Shooting,” “Fishing,” “Hiking & Camping” or “Riding.” The theme “Arts and Entertainment” contains the subcategory “Music & Audio” which in turn contains “Rock,” which is further sub-divided into interests such as “Metal,” “Punk” and “Classic Rock & Oldies.”

From among all these specific niches, advertisers will choose the ones that correspond best to the public targeted by their campaign. While the exact processes by which consumers get to be labeled in a certain way remain unclear, we can understand that such a massive collection of information on users of free online services affords advertisers an almost surgically precise means of targeting consumers.

2.4. Everything is permitted ... or almost

But is there a limit? Are there some types of information that companies refuse to collect or use? Labels that they refuse to assign to a profile? Although admittedly few and far between, we did find some commitment to limiting the processing of consumers’ personal information for advertising purposes.

At the outset, most of the policies studied define “personal data[90]” or “personally identifiable” data[91] as information they consider likely to identify the user “personally and directly[92].” A very narrow interpretation seems to be given of what may identify a person, by including under such data only “information such as your name or email address, that can be used to contact or identify you[93].” Google, for example, defines “personal data” in these terms:

> This is information that you provide to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google, such as information we associate with your Google Account.

Microsoft’s policy provides another illustration of this interpretation:

> Our advertising systems do not receive or use any information that would identify you personally and directly (such as your name, email address or phone number).

[90] We found this expression at Google, LinkedIn, Yahoo and Twitter

[91] We found this expression at Imgur and Pinterest

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

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

Such statements give the impression that companies consider that all the data they amass, apart from some specific identifiers, such as someone’s name or email address, to be impersonal – and therefore require less caution during processing. For this reason, many companies claim not to communicate any personal data to third parties of advertising purposes ... but do not preclude communicating any other kind of information for such purposes. Facebook, for example, states:

> We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission.

Such an approach rather too summarily patches over the dangers of data re-identification, which are increasingly well documented in the literature – without mentioning, of course, that its characterization of “personal information” falls short of what the law defines as such (we will come back to this in section 4.1).

There is little hope, therefore, of finding within these loose definitions any real limits to the collection of personal information for the purposes of OBA. Another, more promising approach, is suggested in Google’s privacy policy, which explicitly restricts the collection and use of sensitive information: “When showing you tailored ads, we will not associate an identifier from cookies or similar technologies with sensitive categories[94]”. Google defines , “sensitive categories” as those “based on race, religion, sexual orientation or health[95].” The company also cites the same restrictions with regard to what it calls “sensitive categories” of advertisements:

> When showing you tailored ads, we may associate a cookie or anonymous identifier with interests such as “Cooking & Recipes” or “Air Travel,” but not with sensitive categories. We impose a similar policy on our advertisers[96].

Our search turned up similar restrictions in Facebook, whose policy refers to the company’s “advertising rules” that are intended to regulate the practices of its advertisers. These rules contain the proviso that advertisers “must not assert or imply, directly or indirectly, in the advertising content or targeting[97]” any of a user’s personal characteristics, which include “a person’s race, ethnic origin, religion, beliefs, age, sexual orientation or practices, gender identity, disability, medical condition (including physical or mental health), financial status, membership in a trade union, criminal record, or name[98].”

---

[94] http://www.google.com/intl/en/policies/privacy/

[95] http://www.google.com/intl/en/policies/privacy/

[96] http://www.google.com/intl/en/policies/privacy/key-terms/; These terms are consistent with the OPC’s recommendations presented in a 2014 conclusion regarding the use of sensitive personal information in the context of retargeting advertising performed by Google. See: *Report of Findings: Use of sensitive health information for targeting of Google ads raises privacy concerns,* PIPEDA # 2014-001, January 14, 2014 (OPC). Google is careful to specify that the same restrictions apply to remarketing using sensitive data, in accordance with the recommendations of this conclusion. See: https://www.google.ca/intl/en/policies/technologies/ads/

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

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

LinkedIn also draws attention to so-called sensitive information, but not so as to limit its use. Rather, it informs subscribers that it is they who choose to disclose such information and that they apparently do so at their own risk:

> Supplying to us any information deemed “sensitive” by applicable law is entirely voluntary on your part. You can withdraw or modify your consent to our collection and processing of the information you provide at any time, in accordance with the terms of this Privacy Policy and the User Agreement, by changing your account settings or your profile on LinkedIn or SlideShare, or by closing your LinkedIn, SlideShare and Pulse accounts.

In addition to these rare pronouncements regarding sensitive information, several companies claim that they have restrictions regarding children. Some require their users to be at least 13 years old[99] or at least to have obtained the consent of a parent to use their services[100]. Yahoo does not exclude children under 13, but does state that it will not contact them for advertising purposes without the permission of a parent. The company adds: “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].” If we are to understand that a minor’s not being exposed to advertisements depends on such permission or prohibition, we might justifiably wonder whether such a declaration constitutes mere wishful thinking in a virtual environment where the control and verification of a person’s age and other personal details are too often illusory.

2.5. Consent and withdrawal

“By using our Services, you agree that Google can use such data in accordance with our privacy policies[102].” This is how Google, and most of the other services studied, obtain the consumer’s consent. In essence, the consumers are agreeing that their personal information can be used to target them with OBA when they choose to use an online service[103].

Some companies are careful to justify their methods. Some, such as Microsoft, explain that advertising is essential for the free supply of the service[104]. On Pinterest, the collection of information is presented as inevitable or simply obvious: “These days, whenever you use a website, mobile application, or other Internet service, there’s certain information that almost always gets created and recorded automatically[105].”

---

[99] We found these requirements in Twitter and Pinterest. LinkedIn, in its Terms of Use, specifies that the user must be at least 14 years of age.

[100] This approach is recommended by Microsoft and the Bing search engine.

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

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

[103] As we will see in Section 4.4.1, this is clearly constitutes implicit consent

[104] For example, we find this in Microsoft's policy: “Microsoft provides many of our sites and services free of charge because they are supported by advertising. To make these services widely available, the information we collect may be used to help improve the advertisements you see by making them more relevant to you”

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

While they do not provide consumers with an explicit choice, most of the policies we studied do list a number of ways to limit being tracked for advertising purposes. Although most admitted they ignored the “Do Not Track” signal from browsers, Twitter and Pinterest did state that they stop tracking when this is activated. Some instruct consumers on how to block cookies in their browser, as well as on the consequences of blocking them[106]; however, we learned in the same document that they use Super cookies, Web beacons or other tracking methods that cannot be avoided by simply blocking cookies. Others added that consumers are still free to close their accounts or not use the service if they do not wish to be tracked.

In some cases, companies provide their users with mechanisms for disabling or limiting the use of specific types of information. For example, the “Google Settings” on mobile devices running the Android operating system offer an option for preventing applications from using the device’s unique identifier for advertising purposes, or to reset it. Various settings also allow users to block the use of localization data originating from GPS or Wi-Fi networks. These options may be scattered over several locations, whether in the mobile device’s general options section or as one of the parameters of the applications offered by some of the services[107]. The Twitter mobile application, for example, lets consumers check a box to disable the use of localization[108].

Many companies provide consumers with mechanisms for opting out of OBA, on their own websites[109]. However, this “piecemeal” approach, which consists in individually requesting each company that tracks a user to stop doing so, quickly hits a wall given the number of players who may be participating in OBA. For example, in addition to offering a page allowing users to unsubscribe from its advertising monitoring[110], LinkedIn invites them to visit the pages of eight other intermediaries who may be tracking them:

> Please read our partners' privacy policies (linked below) to ensure that you're comfortable with how they use cookies. We've also provided links to opt out of their services, if you'd like.[111]

As it turns out, among all the options offered by the companies, apparently the most simple and effective way of refusing OBA probably lies in the opting-out page provided by DAAC, which permits block unsubscription from many participating companies[112].

These opt-out mechanism from the industry promises to disable all “interest-based” ads. However, so-called “generic[113]” or “contextual” ads that use certain types of information obtained from the consumer, will continue to appear. Amazon explains as follows:

---

[106] For example, Google LinkedIn, Twitter, Kijiji, Amazon and Pinterest provide information about it.

[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] Such mechanisms exist in: Google, Microsoft (https://choice.microsoft.com/en-ca), Yahoo!, LinkedIn (“Manage preferences for ads”), 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

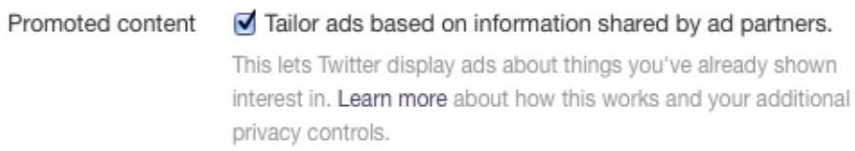
[112] We found that the following companies offer a link to the DAAC site: Google, Facebook, Microsoft, LinkedIn, Twitter, Kijiji, Amazon, Imgur, Yahoo!

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

> Even if you opt out of interest-based ads, you may still see ads based on factors such as your general location derived from your IP address, your browser type and recent, previous searches related to your current search[114].

What is more, the scope of these opting-out choices seem to be unequal from one service to another. On social media, especially, possibilities for opting-out of targeted advertising seem to be limited. In fact, if the explanations given in the Facebook, Twitter or LinkedIn are taken literally, it means that opting-out applies only to the user’s activities outside the platform. In other words, users will still be subjected to data tracking when they are using the service, but not while they are browsing on the rest of the Web.

Figure 2: Removing personalized Twitter ads



The company explains this feature as follows: “When you uncheck this box, Twitter will not match your account to information shared by ad partners to tailor ads for you. This means we would not match your account to information shared by ad partners, including browser-related information, mobile device identifiers, and email hashes, to tailor ads for you[115].” A careful reading of this text makes it clear that Twitter will continue to monitor consumers’ activity whenever they use their service; and there seems to be no way of escaping that.

In addition to the pure and simple OBA withdrawal option, Google and Yahoo! offer consumers a more nuanced choice: to purge their profiles of “interests” they do wish to be associated with. This option allows consumers a degree of control over ads on topics they dislike or attributions that in one way or another are invasive of their privacy. This is most exact level of control offered to consumers that we were able to find.

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

[115] https://support.twitter.com/articles/20170405-your-privacy-controls-for-tailored-ads#

Figure 3: Granular control offered by Google

This Google page allows users to delete interests attributed to their profile.

However, in the majority of companies studied, such granular control is not available. Facebook has mentioned such a possibility, but this feature was still not available in Canada at the time of writing[116].

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

3. Focus groups with consumers

Analysis of these policies reveals that free Internet service providers amass a stupefying amount of data on their users, and can assign a considerable number of labels to a single user profile. But what do consumers think? What personal information are they willing to divulge to get a “free” Internet service and what other information would they like to share?

In Canada and around the world, there are many studies documenting consumers’ views on OBA. From these studies, it generally appears that the majority of Internet users are worried or uncomfortable about online tracking[117]. They are often unaware of how extensive current practices that rely on their personal information actually are[118]. Despite this, a majority are not prepared to shell out money just to put an end to being tracked online for advertising purposes[119].

Studies on consumers’ perceptions of the types of information collected for OBA purposes are more scarce. In the United States, a 2013 study found that half of consumers surveyed simply not do want to share their data for purposes of OBA; the other half would be more willing to disclose their gender, their general (imprecise) location, the operating system on their device and their Web history than any other information[120]. Other studies indicate that consumers are strongly opposed to disclosing information related to their health[121]. In 2009, in the context of its GeoConnections program, Natural Resources Canada published a study on the collection of localization data. One of the main conclusions was that Canadians are uncomfortable about disclosing their real-time location for targeted marketing purposes[122].

To arrive at a better understanding of the views of Canadian consumers, we held four focus groups, two in Montreal and two in Toronto. In these groups, we sought to determine the level of acceptability among the participants with regard to the collection and use of their personal information for OBA purposes. The sessions were held with regular Internet users of all ages,

[117] PIAC in 2009 revealed that the majority of Canadians say they are uncomfortable with targeted behavioural advertising practices: Janet Lo, *A “Do Not Track List” for Canada?*, report to Industry Canada’s Office of Consumer Affairs PIAC, 2009, pp. 10-16. For similar results see also: Blase Ur et al, *Smart, Useful, Scary, Creepy. Perceptions of Online Behavioral Advertising*, Carnegie Mellon University, CMU-CyLab-12-007, 2012. The exact percentages of consumers obviously vary, depending on the studies and the methods used.

[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 Advertising and Privacy*, report presented Office of the Privacy Protection Commissioner of Canada by Ryerson University, 2011

[119] In this regard, we invite the reader to consult the literature review in Kent Sebastian, *No Such Thing as a Free Lunch: Consumer Contracts and “Free” Services,* a report submitted to Industry Canada’s Office of Consumer Affairs by PIAC, 2014, p. 14. See also: 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) 138 49-2 *Decision Support Systems* 138

[122] Phase 5 Consulting Group Inc., *Research on the confidentiality and use of geospatial data*, prepared for Natural Resources Canada, 2009

organizing two groups in each city, one composed of people 18 to 40 years of age and the other of people 40 and over[123]. Following are the results of these discussions.

3.1. A surprisingly extensive practice

Consumers are no dummies. Even without explaining to them how OBA operates, several mentioned that they had noticed that they were receiving ads for products or topics they had previously searched for, such as furniture or travel. For most, it was obvious that some ads are targeted on the basis of their online activity. “It's blatantly obvious,” one exclaimed. Many also understood that advertisers draw inferences based on their online transactions in order to assign categories of interest to them: “Google has a profile for us. They anticipate our gender, and they know what we search, what we like, our interests, and they focus advertisements towards that.”

But what degree of invasion of privacy are consumers willing to accept in exchange for free online content? Is there some information they would not want to disclose for OBA purposes? To find possible answers to these questions, we explained how OBA functions. We explained that information such as their browsing history, their activity on social media, the content of their emails or the information they give when opening an account can be collected for advertising purposes[124]. We then asked for their opinion about the collection of such information.

Although they were already aware that their online activities were being tracked, the consumers seemed surprised at how extensive the practice actually is. They declared that the online monitoring and collection of their personal information was on much larger scale than they imagined[125]. For example, many expressed surprise that the content of their emails was scanned for advertising purposes: “It’s exactly as if they took the time to open the envelope, read the contents, close the envelope and put it back in the mail.”

Such close monitoring was a cause for deep concern for many of them: “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.” They expressed concern, for example, that their privacy could be compromised by having their online advertising activities revealed: “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 it. This was supposed to be a surprise.” Many expressed fears about how far such uses of personal information could lead, evoking images of a dystopian society, of “Big Brother” or “1984.”

[123] We chose to divide the groups based on the age of the participants after consulting other studies that obtained different results from respondents of different ages. See, for example: Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley and Michael Hennessy, *Americans Reject Tailored Advertising and Three Activities That Enable It*, 2009, online at: http://ssrn.com/abstract=1478214

[124] The complete discussion guide is presented in Appendices 1 and 2

[125] This result is similar to that obtained by PIAC in Janet Lo, *A “Do Not Track List” for Canada?*, report presented to Industry Canada’s Office of Consumer Affairs by PIAC, 2009, 2009

Nevertheless, despite their concerns, consumers also seemed interested in the business model of online companies that are partially funded by OBA. “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’s good. But I think there's a certain ethical line, and if that’s crossed, then I think we need to re-evaluate.” Some added that this form of advertising might even be advantageous, enabling them to find interesting discounts, discover new ideas or compare products before purchasing. “If we have to see ads, it’s better to see ads for things we’re interested in.”

3.2. A draft typology

We continued the discussion by asking consumers for their opinions on the collection and use of eighteen types of information related to fields of interest that could be used to target them. Setting up a focussed list was no easy task, since, as our analysis of privacy policies shows, companies collect all kinds of information on the Internet. In addition, the fields of interest they use are very numerous, cover a broad spectrum, and vary significantly from one company to another[126].

We conducted a literature search to help us arrive at a representative synthesis of these various types of information. We first consulted other studies on consumers’ perceptions of the types of information used in OBA[127]. Subsequent to our legal research (Section 4), we also ensured that information categories generally considered to be sensitive in accordance with legal doctrine were included in our synthesis[128]. In addition, some of the experts we interviewed helped us identify the relevant types of information.

Finally, we asked the participants if they would accept online companies using the following types of information in order to send them targeted ads:

- The types of food you like and your favourite restaurants
- Your favourite entertainment (e.g. movies, music, video games, sports)
- Your shopping preferences (e.g. clothes, automobiles, electronics)
- The fact that you are looking for a new job
- The fact that you are getting married soon
- Your hobbies and pastimes (e.g. gardening, hiking, sports, crafts)
- The fact that you train or attend a fitness center
- Financial information such as your approximate salary, your retirement plans or the fact that you have made credit applications
- Places you have traveled to or plan to travel to

[126] See section 2.3

[127] The most important of these was 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] We mainly consulted two doctrinal sources consulted on this aspect: Éloïse Gratton, *Understanding Personal Information: Managing Privacy Risks*, Lexisnexis Canada, 2013; Paul Ohm, “Sensitive Information” (2015) 88 S. *Cal. L. Rev*. [Upcoming]

- The issues you are interested in, such as environmental protection, foreign affairs, politics, etc.
- Your medical condition or your health in general
- The fact that you are registered at a dating agency
- Your love life, your sexual orientation or your sexual preferences
- Your marital status and family status – for example, whether you are divorced or have children
- Your religious beliefs or political views
- Your ethnicity
- The content of your private messages, and whom you correspond with
- Your exact location

Although approximate, this list nevertheless covers most of the themes used by companies, while presenting concrete examples to consumers. For example, the item “favourite entertainment” subsumes many of the elements we identified in our analysis of privacy policies, such as film, literature, video games or sports. Note that the last two items on the list, concerning consumers’ correspondence and their geographical location, were added after consulting the legal doctrine, which emphasizes these two types of data[129].

Obviously, the discussion groups provided an opportunity to allow consumers to express themselves and get them to raise new points. The list was also intended as a discussion guide, to help participants think about other possible scenarios.

3.3. A matter of context

Most often, the participants identified little information whose use they considered acceptable for the purposes of online advertising. However, very few asserted from the start that they were against disclosing any information, under any circumstances. This finding contradicts previous studies that conclude that at least half of consumers have no wish to see their online activities tracked for advertising purposes[130]. This discrepancy can be explained by the methodologies employed: while many of these studies were based on surveys, we obtained the views of our consumers in focus groups. Accordingly, our collection method may have yielded more nuanced responses, as it was applied in a context where respondents were more aware of the online companies’ business model and the options available to them.

This is perhaps also a sign of a recent attitude shift towards Internet privacy; for instance, younger consumers, who are generally more open to new technologies, were demonstrably less apprehensive over the prospect of their personal information being collected and used online. Several declared that they had “nothing to hide,” “were blameless” or that they had no

[129] For details, see section 4.4.2

[130] See especially: 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 and Michael Hennessy, *Americans Reject Tailored Advertising and Three Activities That Enable It*, 2009, online at: http://ssrn.com/abstract=1478214

“immoral behaviour” – and consequently, being monitoring for advertising purposes was of little concern for them[131].

In any event, the use of certain categories of information for advertising purposes was acceptable to a large majority of consumers, regardless of age. For instance, most of the participants were willing to disclose their preferences as regards food, entertainment, shopping or hobbies. They felt such information to be relatively mundane, and could have few consequences for them.

Opinions over some categories, however, rapidly became more divided. For example, they were far more hesitant about revealing that they might be getting married soon, or were looking for a new job, or planning to make a trip or were interested in certain issues. “When I'm looking for a job, that's not something that I want out there, even if it’s just for an advertiser.” Even the fact that someone worked out or went to a health spa seemed less acceptable: “That's related to my health, to medical stuff, to things that are no one else’s business.”

Most of the participants also felt that OBA companies should not be permitted to use information such as marital status, family status, ethnicity, religious beliefs or being registered with a dating agency. “I think it's too personal ... it's not like the fact that I love roses.” Several stressed in particular that they would under no circumstances give out information about their children for advertising purposes. They were also concerned that younger Internet users do not sufficiently protect their privacy online, or are exposed to advertising that is inappropriate for their age.

Some types of information were almost unanimously rejected. For instance, consumers showed great reluctance towards the use of medical information or information about their romantic or sex lives. They stated that such information can be “embarrassing” and it is easy enough to understand why such a consensus emerged among participants. The same consensus was also observed with regard to information about their financial situation, such as their approximate salary, pension plans or whether they had made a credit application, “My credit application is nobody’s business but mine.” Using the content of private messages or the user’s exact location also aroused strong opposition, although some felt that the use of location could have benefits, such as finding the best stores.

It is easy to see that the information generally considered most sensitive is, of course, the type of information consumers are least likely to share. On the surface of it, then, the conclusion seems obvious: the closer a piece of information comes to touching a person’s sphere of intimacy the less that person will consider it acceptable to be used for OBA purposes. Accordingly, consumers find the use of information about their favourite entertainment to be acceptable, while they would prohibit the use of information relating to their medical condition or financial affairs.

[131] Researcher danah boyd has a few interesting thoughts to offer on this topic. She considers that, contrary to popular belief, young people are in fact very concerned about their online privacy, “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.” She explains that they have developed numerous tricks to protect their privacy online, even going so far as manipulating the companies’ algorithms to their advantage. See: http://knowledge.wharton.upenn.edu/article/teens-privacy-online/

However, such a conclusion might be hasty, since it does not take into account the fact that perceptions about what constitutes privacy vary from one person to the next: what is acceptable will also, and especially, depend on the context and the perception of the person concerned. In some cases, using what passes for innocuous information in the eyes of many can become distressing and harmful for others faced with a particular situation. For example, one participant claimed to have been upset by ads that appeared following a search he made: “My father-in-law died of prostate cancer, so I was looking up topics related to the prostate and after a while, I kept getting these ads about the prostate.” In another context, however, such a use may have not have been so upsetting.

What is privacy, exactly? While there are certain points of consensus on the acceptability of using certain categories of information, it is clear that privacy is a multifaceted concept. The participants did not fail to remark that “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.” While everyone has their own idea of privacy, it is difficult – if not impossible – to decide which categories of information enjoy the greatest social acceptability. Clearly, although broad outlines can be suggested, it all comes down to context and, ultimately, analysis should always be performed case by case, taking differing circumstances into account.

3.4. Choice, information, education

After questioning participants about the types of information that can be used in OBA, we asked them about how much control they believe they had over such use.

When we asked if they knew what to do to stop companies tracking their online activities for advertising purposes, participants gave various responses. From the outset, many doubted that they could completely escape online tacking. “There's nothing private anymore. Whatever you do, it's all recorded somewhere.” Others, more practically, pointed to the options on their Internet browsers, such as cookie deletion, private browsing mode or simply deleting the browser navigation history. Others raised the possibility of switching to online services that do not use tracking, such as DuckDuckGo[132].

The participants knew little about the options companies offer for opting out of OBA. For instance, although some participants had seen the AdChoices icon, few were able to explain what it was used for. In particular, it was clear that the participants generally did not know anything about the granular control option offered by Google: “I've seen it, but I thought it was just asking me questions about myself. I didn’t realize it had anything to do with what ads that they are going to use to cater to me.”

The participants were, however, enthusiastic to learn that such options were available to them: “This is a good choice to have.” This echoes the desire they expressed repeatedly during the focus groups: to have a choice about whether to accept or refuse to have their information

[132] https://duckduckgo.com/

collected for advertising purposes[133]. “I wish there was a system that gave me a choice. I could click it whenever I see an ad.”

More generally, the participants deplored not being sufficiently informed about the practices of online companies. As we know, the information on these practices is often found in abstract, mind-numbing privacy policies that the majority of consumers simply do not read. “I want to have access to appropriate information that I can easily understand.” Beyond mere disclosure by the companies, however, they also wanted to receive training: “They should not just inform us, but train us. There should be a course at school that everyone should take.”

Admittedly, some consumers said they were ready to pay to ensure that the online services they use do not track them for advertising purposes. Most, however, were also aware that advertising can finance online services, and found advantages in this business model: “If they removed advertising from YouTube, you’d end up paying more money every month for your Internet account, and that’s already expensive.” In this instance, their main source of reticence did not necessarily stem from the fact of being tracked on the Internet. What inspired their most heated reactions was their feeing that the practice is carried out surreptitiously, without their permission. “I think it should be a conscious choice you make. People don’t know about it and I think it's the fault of the governments, agencies and businesses that manage it.”

[133] Several other studies also indicate that consumers want more control over the tracking of their personal information for OBA purposes. For example: Lalit Agarwal et al, “Do Not Embarrass: Re-Examining User Concerns for Online Tracking and Advertising.” *Symposium on Usable Privacy and Security (SOUPS)*, Newcastle, UK, 2013

4. Legal analysis

4.1. Computer data and personal information

The goal is simple: to enable advertisers to not only make ads pop up on users’ screens, but to ensure that they are the kind of ads they are most likely to click on. To achieve this, they collect every conceivable kind of data: the addresses of the sites the users visit, the time spent on each, the purchases they make online, their geographical location, the publications they like, the social media they use. They also collect other data of a more technical nature, such as IP addresses or information about the device or the software they use. Basically, they collect everything they possibly can.

The collection and processing of such data do not take place in a legal vacuum. In Canada, any company that collects, uses or discloses personal information in the course of its commercial activities must comply with the requirements of the *Personal Information Protection and Electronic Documents Act*[134] (hereinafter the “Federal Act”) or of equivalent provincial legislation[135]. This applies equally to the physical world as to the virtual world.

These laws apply whenever an organization processes personal information, that is to say, in the words of the Federal Act, “information about an identifiable individual[136].” Case law gives a broad interpretation to this definition, considering that information relates to an identifiable individual “where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information[137].”

In light of this liberal interpretation, data collected on Internet users for the purposes of OBA will generally be considered to be personal information within the meaning of the law – with the result that companies that process the data must respect the privacy laws. Of course, data such

[134] *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 (hereinafter the “Federal Act”)

[135] Section 26 (2) b) of the Federal Act allows the federal government to exempt application of the Act within the limits of a province that has adopted a law it deems to be “substantially similar” to this one, except for “federal undertakings” and the collection, use or disclosure of personal information outside the province for which the Federal Act continues to be applied. Three Canadian provinces have adopted similar laws, that is to say, which include provisions and rights similar to those set forth in the Federal Act: Quebec, with the *Act respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1, RSQ, c. P-39.1; Alberta, with the *Personal Information Protection Act,* SA 2003, c. P-6.5; and British Columbia, with the *Personal Information Protection Act*, SBC 2003, c 63. Similarly, three other provinces have adopted substantially similar laws, but which apply only to the custodians of health information: Ontario, with the *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A; New Brunswick, with the *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05; and Newfoundland and Labrador, with the *Personal Health Information Act*, SNL 2008, c P-7.01. We will focus our legal analysis on the Federal Act for two reasons: First, since the provincial laws are equivalent, one might validly assume the state of the law to be similar in all Canadian provinces, even though the applicable laws may differ. Second, OBA, which is deployed on the Internet, necessarily involves the disclosure of information outside the physical limits of a province, raising doubts as to whether provincial laws are in fact applicable to these activities.

[136] Federal Act, s.2. Within the meaning of the Act, however, personal information does not include the name, title or business address or telephone number of an employee of an organization.

[137] OPC, *Legal information related to PIPEDA Interpretation Bulletin*, online at: https://www.priv.gc.ca/leg_c/interpretations_02_e.asp. The OPC gives many examples from jurisprudence of the liberal interpretation given by the courts to the concept of personal information, including *Gordon v. Canada* (Minister of Health), 2008 FC 258

as the serial number of a cookie or a user’s IP address do not in themselves necessarily identify a person. However, for the purposes of OBA, such data is combined with other data to set up a revealing profile of a consumer that would make that person easy to identify. As a result, the OPC has already concluded that an IP address[138], information stored in a cookie[139] or the unique identifier of a device[140] could constitute personal information within the meaning of the law. In 2013, the OPC concluded that the same was true of the information contained in a social media user's status message[141].

The same logic applies to information collected from a person in the context of OBA, such as the interests attributed to his profile. Even subjective material relating to a person, whether accurate or not, may qualify as personal information[142]. In a 2014 conclusion, for example, the OPC considered that Google had collected personal information on the health status of a user by collecting the user’s history of visiting sites offering devices for the treatment of sleep apnea[143].

This liberal interpretation was echoed by the OPC in its guidelines on online behavioural advertising published in 2012:

> the OPC will generally consider information collected for the purpose of OBA to be personal information, *given*: the fact that the purpose behind collecting information is to create profiles of individuals that in turn permit the serving of targeted ads; the powerful means available for gathering and analyzing disparate bits of data and the serious possibility of identifying affected individuals; and the potentially highly personalized nature of the resulting advertising.[144]

The state of the law thus easily convinces us of the inappropriateness of the distinction that most of the privacy policies we analyzed make between the data they call “personal,” which they restrict to only some of the consumer’s identifiers, and all the other types of data they collect. Clearly, personal information, within the meaning of the law, includes not only a person’s name and contact information, but also their browsing activities collected for the purposes of OBA. In this regard, companies that process information for OBA purposes may not

[138] *ISP's anti-spam measures questioned* PIPEDA Case Summary no2005-319, November3, 2005 (OPC); *Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection*, PIPEDA Case Summary #2009-010, September 2009 (OPC); see also: OPC: *What an IP Address Can Reveal About You*, a report prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada, 2013

[139] *Customer complains about airline's use of “cookies” on its Web site*, PIPEDA Case Summary #. 2003-162, April 16, 2003 (OPC)

[140] *Apple called upon to provide greater clarity on its use and disclosure of unique device identifiers for targeted advertising*, PIPEDA Report of Findings No. 2013-01720, November 2013 (OPC), para. 35

[141] *Survey of personal information handling practices of WhatsApp. Inc*. Report of findings under PIPEDA # 2013-001, January 15, 2013 (OPC), para. 61

[142] *Survey of personal information handling practices of WhatsApp. Inc*. Report of findings under PIPEDA # 2013-001, January 15, 2013 (OPC), para. 59

[143] *Use of sensitive health information for targeting of Google ads raises privacy concerns*, Report of findings under PIPEDA # 2014-001, January 14, 2014 (OPC), paras. 25-28

[144] *Policy Position on Online Behavioural Advertising*, (OPC) 2012, online at: https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp. These guidelines provide valuable insights into the legal framework applicable to OBA in Canada.

validly avoid the scope of the law by presuming the depersonalized nature of the data they collect.

4.2. Consumer data as currency

The accepted meaning of the word “free,” according to The Merriam-Webster Online Dictionary, is “not costing any money; not costing or charging anything[145].” However, several online companies nonetheless appear to restrict the meaning of “free” to a question of money, although “free” also implies that there is no cost whatsoever involved. Facebook's home page, for example, invites consumers to subscribe to the service by claiming, “It's free (and it always will be).”

But is it really free? Our analysis of privacy policies reveals that there is indeed a cost to users of “free” online services – even if this does not take the form of hard cash. In fact, consumers can only gain access to these services in exchange for the personal information they provide. In the opinion of several authors, including Chris Jay Hoofnagle[146] there is a reciprocal relation between the company and the consumer that strays very far from the notion of “free”:

> 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]

So, by agreeing to disclose their personal information, consumers are exposed a myriad of risks of which they may not be fully aware[148]. For example, they are exposed to the risk of having their vulnerabilities revealed and unduly exploited; think, for example, of the consumer with gambling problems who is confronted with online casino ads. Advanced knowledge of consumer preferences could also pave the way for discriminatory practices, such as giving merchants an opportunity to adjust their prices to the profiles of the consumers they aim their ads at.

Consumers also risk having their private lives exposed in various ways. For example, having one’s personal ads displayed in an Internet browser could lead to embarrassment if third parties chanced to see them and deduce harmful information from them. More worryingly, the large number of actors involved in OBA poses dangers to the security of the consumer data they

[145] We consulted the 2004 edition of this book.

[146] Mr. Hoofnagle is a professor at the University of California, Berkeley - School of Law

[147] Chris Jay Hoofnagle and Jan Whittington, “Free Accounting for the Costs of the Internet's Most Popular Price” (2014) 61 *UCLA L. Rev.* 606, p. 634

[148] For an exhaustive list of the harms and risks posed by the OBA, see: Janet Lo, *A “Do Not Track List” for Canada?*, report to Industry Canada’s Office of Consumer Affairs by PIAC, 2009, pp. 49-56

compile and exchange; even if the data is anonymized using state-of-the-art techniques, studies have vividly demonstrated the ease with which it can be re-identified[149].

In short, the exchange that takes place between the consumer and the merchant is above all contract of adhesion. In a context of information imbalance, consumers have little choice but to accept the company's terms in order to benefit from services that are often indispensable, such as the Google search engine. They must consent to an almost unrestricted collection of their personal information without knowing the scope or ramifications of the treatment reserved for them – and in so doing support the risks of damage to privacy, fraud or theft identity.

Canadian law, however, is slow to recognize this contractual imbalance. First of all, the courts have not yet confirmed the applicability of the laws on consumer protection – which could provide some remedies – to the relationship between consumers and free service providers. Moreover, as we shall see in the next section, the dominant interpretation of the privacy laws remains unclear as to the limits – if there are any – to the amount of personal information that may be collected through the supposedly free business model funded by OBA.

The consumer protection laws of Quebec and Ontario do not require the consideration offered in exchange for a service to be a sum of money in order for the contract be subject to the law. Ontario's *Consumer Protection Act, 2002* defines "a consumer agreement" as "an agreement between a supplier and a consumer in which the supplier agrees to supply goods or services for payment[150]." Such "payment," within the meaning of the Ontario legislation, does not necessarily imply a sum of money, but a "consideration of any kind." In Quebec, the definition of "consumer contract" given in the *Civil Code* opens the door to a similar interpretation; here again, "payment" is not limited to a sum of money, but may extend to other types of obligation[151].

However, the case law remains unclear as to the applicability of consumer protection laws to contracts in which the user receives a service in return for his personal information. Until now, it has mostly been in class action authorization decisions, where disputes are not settled on the merits, that the issue has been raised. In many cases, these class actions were authorized by the

[149] Several fascinating studies on the re-identification of anonymized data have been conducted in recent years, which suggest that it is fairly easy to identify a person on the basis of this data. Among these studies, researchers Alessandro Acquisti, Ralph Gross and Fred Stutzman, in 2011, demonstrated that it is possible to infer sensitive information about someone from a simple picture of their face, combining face recognition software, data mining algorithms and statistical identification techniques: http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/. See also: Latanya Sweeney, "*k-anonymity: a model for protecting privacy*," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 5570; John Bohannon, "Credit Card study blows holes in anonymity" (2015) 347-6221 *Science* 468

[150] *Consumer Protection Act, 2002*, SO 2002, c. 30, Sched A, s.1

[151] Civil Code of Québec, art. 1553. For further developments on these issues, see: Anthony Hémond, *Canadian Perspectives on Cloud Computing and Consumers,* Final Report of the Research Project Presented to Industry Canada's Office of Consumer Affairs, Consumers Union, 2011, pp. 22-28; Luc Thibaudeau, "Le I-consommateur à la recherche de la protection adéquate," *National Conference On Class Actions : Recent Developments in Quebec, in Canada and the United States* (2014), vol. 380, Quebec Bar – Continuing Education, Cowansville, Ed Yvon Blais, pp. 588-590; Kent Sebastian, *No Such Thing as a Free Lunch: Consumer Contracts and "Free" Services*, report to Industry Canada's Office of Consumer Affairs by PIAC, 2014 pp. 30-34

courts[152]. However, in 2011, the Quebec Superior Court dismissed an application for authorization to institute a class action against Facebook, on the grounds that the user's agreement with the company was not a "consumer contract," since, according to the Court, use of the service was "free[153]."

According to many commentators, this is a decision that ought to be appealed[154]. Nicolas Vermeys, professor at the Université de Montréal, remarks:

> Our personal information has a value. If it didn't, companies would not collect. It's false to say that it's free; it's not a gift from Facebook; it's is a swap, an exchange contract. On the one hand is the service, and on the other is your personal information. [TRANSLATION]

Despite these legal uncertainties we could only wish were ephemeral, it is clear that the economic logic remains implacable: personal information is a form of currency provided by consumers. It is their data that permits online services to generate income by selling their services to advertisers.

4.3. The price of "free"

Having established that personal information is a form of currency provided by the consumer, we can attempt to consider the problem from a quantitative standpoint. If the price of a service is defined in terms of data rather than dollars, how much personal information is it legitimate to require from consumers so that they can benefit from these services? In short: what is the right price?

The privacy laws, and in particular, the principle of limiting collection laid down within them[155], provide some clues. The law stipulates that the collection, use or disclosure of personal information should be carried out in a manner that any reasonable person would consider "appropriate to the purposes[156]." These purposes must not only be specified to the person who is the subject of the collection, but the company that provides the service may not require that person "to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes[157]."

In a 2009 conclusion, the OPC recognized the need to generate revenue through Facebook advertising, and felt it was reasonable "that users are required to consent to Facebook Ads as a

[152] See, for example: *Albilia v Apple Inc.*, 2013 QCCS 2805 (Free mobile applications). *Neale v. Groupe Aeroplan inc.,* 2012 QCCS 902 (loyalty program). In *Option Consommateurs v. Shoppers Drug Mart Corporation*, 2012 QCCS 1078, para. 44-45, the Superior Court authorized the class action, deferring its decision on the classification of the contract to a later stage of the proceedings.

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

[154] This case was the subject of a transaction before it could be appealed.

[155] Federal Act, Principle 4.4

[156] Federal Act, s. 5 (3)

[157] Federal Act, Principles 4.2.2 and 4.3.3

condition of service.[158]” In its guidelines on the OBA, the organization reiterates this interpretation, and to some degree, specifies its parameters:

> However, OBA should not be considered a term or condition for individuals to use the Internet generally. There are still other forms of advertising that websites can rely on. There must also be meaningful consent, and there should be limitations on the types of information collected and used for profiling. Safeguarding the information is also vital, as is limiting the retention of the data to the least amount of time possible.[159]

While these nuances offered by the OPC suggest setting limitations on the types of information collected and used, it should be noted that the criterion of necessity still remains practically unexplored. On the one hand, our analysis of privacy policies reveals that for all practical purposes, online services collect any scrap of information about their users that they can. On the other, however, the OPC’s conclusions with regard to OBA conducted in the context of the provision of a free service seem to obscure the fact that, even if the purposes of the information collection are acceptable, the information that the company collects “shall be limited to that which is necessary for the purposes identified by the organization[160].”

Here we can ask whether the criterion of necessity, however legitimate the purposes may be, has not been patched over too hastily. Is it really necessary to collect every scrap of information generated by a user to achieve commercial profitability? It rather seems that, under the guise of an acceptable purpose, consumers are required to pay a price for “free” online services that has no upper limit.

With this in mind, it is perhaps not unreasonable to hope that the principle of limiting data collection for the purposes of OBA can be revisited. The exercise would of course be an arduous one, and beyond the scope of this research. It would not only require access to the algorithms of the online companies, but also the deployment of considerable technological and legal resources to analyze them. However, the government authorities may have to seriously contemplate following such a course if they wish to assess the companies’ compliance with the law in a more than approximate way.

4.4. Categorizing personal information

Although the criterion of necessity sets no tangible limits on the collection of personal information for the purposes of OBA, we can hope to find some indications within the legal requirement of the consumer's consent, the form of which will vary according to the sensitivity of the personal information collected. While considering personal information as currency involved formulating the question in quantitative terms, the limits to be explored here are more qualitative in nature, since their scope varies depending on the nature of the information.

---

[158] *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act by Elizabeth Denham, Assistant Privacy Commissioner of Canada*, Case Summary under PIPEDA # 2009-008, July 16, 2009 (OPC), para. 134

[159] OPC Position Statement on online behavioural advertising, 2012, online at: https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_f.asp

[160] Federal Act, Principle 4.4

4.4.1. The pitfalls of implied consent

Under the law, consumers must be informed about the collection, use and disclosure of their personal information and must give their consent[161]. These principles of information and consent are the keystone of Canadian privacy law and, at least in theory, can serve as guideposts in determining what free service providers should be allowed to do with their data.

As we have seen, the major free Internet service providers fulfil these obligations by obtaining from the consumer a form of consent known as implicit (or negative) consent[162]. “Unless the individual takes action to “opt out” of the purpose — that is, says “no” to it — the organization assumes consent and proceeds with the purpose[163].” This is the formula of choice for companies offering free online services, who are most often content to inform consumers about the practices in their privacy policies; by using the service, the user agrees by default to everything these documents state.

Under the law, however, this form of consent for the OBA purposes is only valid if it meets certain requirements. The OPC guidelines state that negative consent to OBA is acceptable only if the individuals involved are notified of the purposes of the collection “in a clear and understandable manner” at or prior to the time of collection. This means that the purposes must be manifest and cannot be buried in a privacy policy. It also means that the information must be complete and detail the “various parties involved in the [OBA] process”, i.e. all those who deal with the consumer’s personal information in one way or another. In practice, the OPC suggests that companies meet these requirements “using a variety of communication methods, such as online banners, layered approaches, and interactive tools.”

One wonders how scrupulously the free service providers obey these requirements. Our analysis reveals that information on their advertising practices is most often found tucked away inside voluminous policies – difficult-to-understand documents that consumers simply do not read[164]. This is where vague and general statements are made about the advertisers’ use of consumer data, to the effect that any data can be used for advertising purposes. Moreover, there are relatively few indications at the time of collection directing the user to the relevant information, except in the form of links to privacy policies and terms in the footnotes or icons linked to the ads.

---

[161] These obligations are set forth in several places in Schedule 1 of the Federal Act, see: Principles 4.2, 4.3, 4.4

[162] Implied (or negative or opt-out) consent is contrasted with explicit (or active, or opt-in) consent, the latter offering consumers the opportunity of accepting the proposed use actively and unequivocally, otherwise the company will act as if consent had not been given. Explicit consent is therefore the highest form of consent. See: OPC, *Determining the appropriate form of consent under the Personal Information Protection and Electronic Documents Act,* online at: https://www.priv.gc.ca/resource/fs-fi/02_05_d_24_e.asp

[163] OPC, *Determining the appropriate form of consent under the Personal Information Protection and Electronic Documents Act,* online at: https://www.priv.gc.ca/resource/fs-fi/02_05_d_24_e.asp

[164] This is substantiated by a 2008 study that estimated it would take U.S. Internet users approximately 200 hours per year to read through all the privacy policies related to of the websites they use. A clearly unrealistic undertaking. Aleecia M. McDonald and Lorrie Faith Cranor, “The Cost of Reading Privacy Policies” (2008) 4 *ISJLP* 543

These findings are not new. In recent years, the paucity of information available to consumers regarding the online collection of their personal information is a point that has been raised in several OPC conclusions, which urged several companies to better inform consumers to ensure the validity of the consent they obtain[165].

Obviously, our analysis also revealed that some companies, such as Google and Facebook, do a better job than others of informing their users, in particular by publishing more accessible policies or by giving concrete examples of their practices. However, as we saw in the focus groups, this does not alter the fact that users remain unaware of the extent of the collection and use of their online information: one more sign that major information efforts are still needed.

Consent also implies the possibility of refusal. According to the OPC guidelines, in order for implied consent to be valid, OBA, users should easily be able to opt out “ideally at or before the time the information is collected.” In addition, the opt-out must take effect “immediately” and be “persistent.” But even here, there are problems.

First, some companies do not seem to permit consumers to remove themselves completely from OBA as defined in this report. In fact, the opting-out mechanisms offered by social media platforms such as Facebook and Twitter appear to be limited to information collected outside their platform, and are not applicable to all the information the companies collect on their own users.

Also, as our focus groups revealed, the mechanisms provided by the industry to give consumers a choice, such as the DAAC program, or the Google and Yahoo! granular opting-out mechanisms, remain largely unknown to the general public.

Nor does this not take into account, as mentioned earlier, the many technological difficulties or practices that undermine the effectiveness and sustainability of some of the options available to consumers. For example, some companies clearly offer unrealistic solutions for opting-out of OBA, such as deleting their cookies or stopping using their service – yet tell them in the same breath that they use “super cookies,” “ Web beacons,” or other user tracking methods which are almost impossible for the average user to remove without expert help. In another example, several companies reported that they do not respect the “Do Not Track” signal emitted by browsers, a mechanism that could offer users a simple option.

The unavoidable conclusion, then, is that despite some interesting innovations such as the DAAC opt-out mechanism, most of such options are mismatched, little known and sometimes even useless. In such a context, the whole issue of consumer consent, even when just implied, definitely stands in need of improvement.

[165] See especially: *Survey of personal information handling practices of WhatsApp. Inc* (PIPEDA *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act* by Elizabeth Denham, Assistant Privacy Commissioner of Canada, Case Summary under PIPEDA # 2009-008, July 16, 2009 (OPC) ; *Apple called upon to provide greater clarity on its use and disclosure of unique device identifiers for targeted advertising*, PIPEDA Report of Findings No. 2013-01720, November 2013 (OPC)

4.4.2. Tracking sensitive information

Although Canadian law does not specify categories of personal information the collection or use of which would be prohibited, it does provide tighter consent requirements for personal information it describes as “sensitive.” Accessing such information generally requires obtaining express consent from the consumer[166].

Determining what constitutes sensitive personal information is no easy matter. In fact, what is considered sensitive varies from one person to another and even from one situation to another for the same person. Principle 4.3.4 of the Federal Act acknowledges this difficulty:

> Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.[167]

At most, therefore, the Federal Act does little more than suggest that a person’s medical records and income may generally be considered to be of a sensitive nature.

Jurisprudence, for its part, has determined on a case-by-case basis that some information is sensitive, depending on the particular circumstances of each case – and without establishing a truly general theory of the concept[168]. The OPC has reached conclusions with regard to OBA in recent years that consider that some information used was of a sensitive nature. In 2014, it felt that Google had collected sensitive health information on a user that had been used for advertising purposes without the express consent required[169]. In 2013, it made a similar finding regarding the use of medical information obtained through an online dating site whose policies mentioned that it participated in OBA[170]. Also in 2013, the OPC considered that the unique identification number of an Apple telecommunications device used in the context of OBA constituted sensitive personal information given the permanent, persistent nature of this identifier[171]. However, we must be careful not to conclude from this that the unique identifier of

[166] Federal Act, Principles 4.3.4 and 4.3.6

[167] Federal Act, Principle 4.3.4

[168] For instance, prior drug use uncovered by screening was considered sensitive medical information: *Former employer discloses drug testing information,* PIPEDA Case Summary #2007-382No 27, July 2007 (OPC). Conversely, in an insurance case, implied consent for disclosure of medical information was considered acceptable: PIPEDA Case Summary #2009-003 : *Insurer discloses individual’s medical information to third-party consultant based on implied consent.* Images taken by video surveillance of children at a daycare centre were also considered “extremely” delicate information. Report of Findings under PIPEDA #2011-008: *Daycare Centre Modified Webcam Monitoring to Increase Privacy Protection*: Report of Findings under PIPEDA #2011-008, August 5, 2011, (OPC). Also retained as sensitive personal information was the information that a hairdresser wanted to open a salon in her own home: *Phone message left at client’s workplace disclosed personal information without consent,* Report of Findings under PIPEDA #2012-009, August 8, 2012 (OPC)

[169] *Use of sensitive health information for targeting of Google ads raises privacy concerns*, Report of Findings under PIPEDA # 2014-001, January 14, 2014 (OPC)

[170] *Profiles on PositiveSingles.com dating Website turn up on other affiliated dating Websites* Report of Findings under PIPEDA #2013-003, July 11, 2013 (OPC), para. 77

[171] *Apple called upon to provide greater clarity on its use and disclosure of unique device identifiers for targeted advertising*, PIPEDA Report of Findings No. 2013-01720, November 20, 2013 (OPC)

any device used for OBA purposes will automatically be classed as sensitive. In fact, at the end of the investigation, the OPC was satisfied that Apple had created a new device identifier for advertising purposes that could be reset by the user, thereby allowing the latter to limit tracking.

Some authors have proposed theoretical frameworks that might help determine the sensitivity of information items. According to Mtre. Éloïse Gratton, a partner and national co-leader, Privacy Practice Group at Borden Ladner Gervais LLP, sensitive information is data whose disclosure is likely to "create embarrassment for an individual" or cause "objective harm" such as exposing the individual to fraud or subjecting them to discrimination or physical harm. Mtre. Gratton believes that when gauging the sensitivity of information, one should take into account not only the private nature of the data, but also its identifiability and its availability to the 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], in a recent article on this issue, suggests four factors to consider in determining what constitutes sensitive information:

> 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]

For these authors, it is ultimately the risk of harm that is crucial in assessing the sensitivity of personal information. This theory, though certainly justified, at times seems like an attempt to illuminate the darkness by shining more darkness onto it. In fact, the scope of what exactly may constitute harm to someone with regard to personal information is highly subjective; similarly, assessing risk remains a highly tentative exercise that leaves room for a great deal of error[175]. Research clearly needs to be conducted to determine the conditions under which these intangibles can be reconciled with the general theory of privacy.

The work of Ohm and Gratton nevertheless makes it possible to establish a taxonomy of personal information that is generally regarded as sensitive, or at least "intimate" according to

[172] Éloïse Gratton, *Understanding Personal Information: Managing Privacy Risks*, LexisNexis Canada, 2013, p. 266

[173] Associate Professor at the Faculty of Law, University of Colorado

[174] Paul Ohm, "Sensitive Information" (2015) 88 *S. Cal. L. Rev.* [forthcoming], p. 5

[175] On pages 28 to 32 of his article, Paul Ohm lists several types of damage. By his own admission, the limits of what is harmful or otherwise when it comes to personal information are highly debatable and certain harms can seem very abstract and difficult to define.

the law, case law or self-regulatory principles in a large number of States[176]. Foremost among the types of information the authors classify as sensitive are those relating to an individual’s health, finances, love or sex life and their racial or ethnic origin[177]. Information about a person's family life, including their behaviour in the home also ranks very high[178]. Their religious, political or philosophical views are also classed as sensitive[179]. In addition, individual personal affiliations, such as membership in a union can also be included among this type of information[180]. Information regarding children also warrants a high degree of protection, sometimes going as far as a ban on collecting data for commercial purposes. In addition to the sensitivity of information related to minors, the question of the validity of their consent also deserves serious consideration[181]. Finally, according to Mtre. Gratton, two other types of information are generally considered sensitive: private communications between individuals, such as their correspondence[182], and a person’s precise location, which can be obtained by GPS.

Sex, money, health... Finally, what the law, case law or doctrine consider as sensitive information categories usually boils down to common sense. Instinctively, the average person could name most of the information categories listed above. It was therefore no surprise when we saw that the types of personal information deemed sensitive by law include most of the information categories that participants in the focus groups mentioned most often found objectionable when used for the purposes of OBA. In both cases, this came down to information most closely related to the person's sphere of intimacy.

For example, financial and medical information count among the topics that consumers are least willing to share, which accords with prevailing interpretations of what constitutes sensitive information within the meaning of the law. Consumers also expressed objections to information about their love, sex, or family life or their personal beliefs being used for the purposes of OBA, which again concurs with the legal interpretations mentioned above. We also noted that they

[176] These authors base their taxonomy on the applicable laws in various jurisdictions, including the European Union and the United States, case law, and voluntary regulatory instruments. Note that we omitted the categories Ohm mentions that seem more anecdotal and relate mainly to the American context: these include criminal records, school transcripts and information held by public institutions. At the end of his taxonomy, Ohm also mentions three types of personal information that should, in his view, be considered sensitive: geolocation, metadata communications and biometric data. We could not accept the result of his analysis, however, both because these types of information are subsumed by the other types we mentioned above, and because not all of the problems he cites in regard to such information relate, in our view, to a sensitivity issue, but rather to issues such as the principle of limiting collection that we mentioned earlier.

[177] Éloïse Gratton, *Understanding Personal Information; Managing Privacy Risks*, LexisNexis, 2013, pp. 293-294; Paul Ohm, “Sensitive Information” (2015) 88 S. *Cal. L. Rev*. [forthcoming], pp. 19-22, 23-24

[178] Éloïse Gratton, *Understanding Personal Information: Managing Privacy Risks*, LexisNexis, 2013, pp. 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*. [forthcoming], 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*. [forthcoming], p. 26. See also: *Report on the 2010 Office of the Privacy Commissioner* forthcoming], p. 27

[181] Paul Ohm, “Sensitive Information” (2015) 88 S. *Cal. L. Rev*. [forthcoming], p. 26. See also: OPC, *Report on the 2010 Office of the Privacy Commissioner of Canada’s Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing,* 2011, pp. 23-24. Remember also that advertising to children is subject to bans or limitations. For example, in Quebec, section 248 of the *Consumer Protection Act* is opposed to commercial advertising directed at children.

[182] Éloïse Gratton, *Understanding Personal Information; Managing Privacy Risks*, LexisNexis, 2013, p. 296

expressed the same reservations with regard to their location and the content of their correspondence.

Of course, it is important not to conclude that consumer opinion polls are the only valid means of determining the sensitivity of certain information. Consumers sometimes do not immediately realize that a piece of information they are willing to disclose might mean a significant intrusion into their privacy[183]. A recent conclusion by the OPC[184], which considered a device’s unique identifier to be sensitive information, provides a telling example; in fact, this is a kind of information that most consumers would not intuitively judge to be potentially sensitive. In general, however, an almost complete match emerges between what consumers say they do not want to share in the context of OBA and what lawyers tend to describe in the abstract as sensitive personal information.

Unfortunately, despite this correlation between consumer perceptions and theory, the problem of implementing the law in a virtual environment remains. While the law may be able to evaluate the sensitivity of personal information on a case-by-case basis, in the online world, where consumer data is processed instantly by algorithms, distinguishing which information is sensitive is a far more difficult proposition. The OPC also stressed this difficulty in 2011, in a consultation report on OBA:

> In considering the appropriate type of consent, there is also the question of sensitivity. There are some grey areas with respect to sensitive personal information. What is sensitive for some may not be for others, and what could be considered sensitive in one context may not be in another. The problem with trying to assess sensitivity online is that the environment lacks context.[185]

How could an algorithm, however powerful, guess that an interest attributed to a profile constitutes sensitive information for one person, even though it would not be for another, in other circumstances? How could it know that a certain piece of information it has collected raises a privacy issue? There are numerous examples of situations in which merely following the instructions emitted by an algorithm produced crass results; among these is the example of the “Year in Review” automatically generated by Facebook in 2014, in which a grieving father was presented with images of his recently deceased daughter[186]. Basically, this brings us back to the Turing test[187]: a machine may perhaps be able to understand words – it may even be able to scrutinize data and give consistent responses to instructions – but this does not mean it will be able to exercise the same judgment as a human being. And, anyway, determining what happens to be sensitive for one person would entail very, very long prior acquaintance with them, which

[183] Authors in the United States make a similar observation: that the role of privacy protection experts is essential in determining whether a seemingly innocuous item of information poses risks: 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 called upon to provide greater clarity on its use and disclosure of unique device identifiers for targeted advertising*, PIPEDA Report of Findings No. 2013-01720, November 2013 (OPC)

[185] *Report on the 2010 Office of the Privacy Commissioner of Canada’s Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing,* 2011, p. 31

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

[187] Alan M. Turing, “Computing Machinery and Intelligence” (1950) 59-236, *Mind*, 433

paradoxically would require the collection of an unreasonable amount of their personal information.

In practice, in the absence of algorithms able to pass the Turing test, any company that wants to untie this Gordian knot will have to determine, without a context, whether or not the personal information it collects from a user for the purposes of OBA is of a sensitive nature. Since this is an almost impossible task, the company will have no other choice but to proceed with predefined categories of information: it will have to choose to program its algorithms so that they do not process certain objective information and will eliminate, from among the targeting categories available to advertisers, the ones that may be riskier[188]. After this exercise, it may choose to eliminate certain interests in such precise niches as “products for ‘full-figured’ women,” “false eyelashes,” “weapons,” “adult movies” or “constipation products[189].”

Even though such an approach appears unavoidable if there is ever to be compliance with the law, our analysis of the policies of free service providers reveal that few of them refer to their practices on categorizing sensitive information – except for data relating to children, which is mentioned frequently[190]. One notable exception is Google, which explicitly states that it does not attribute any interest to a user’s profile that is centered on sensitive data, which it defines as “personal information relating to confidential medical facts, racial or ethnic origins, political or religious beliefs or sexuality[191].” Facebook, for its part, says it imposes restrictions on advertisers not only with regard to the sensitive data mentioned above (health, personal beliefs, sexuality or ethnicity), but also on data referring to age, name, criminal record, financial situation or even union membership.

Obviously, the lack of transparency shown by the other companies studied does not mean that they are totally remiss in their obligations regarding personal information of a sensitive nature. In fact, several mentioned that they subscribe to Principle V of the *Canadian Self-Regulatory Principles for Online Behavioural Advertising*, which states that members should not collect and use “sensitive” personal information for OBA purposes “without consent, as required and otherwise in accordance with Canadian privacy legislation[192].” In short, while these companies proffer very little on the categories they consider sensitive, and while there are few references to the issue in their policies, we can perhaps find comfort in their commitment to respecting the law.

In any event, despite good intentions, the category approach has its shortcomings. First, one can simply ask whether the types of information that businesses identify as sensitive are always consistent with the ones that consumers regard as such. We also note that the policies of

[188] This method is discussed in: OPC, *Report on the 2010 Office of the Privacy Commissioner of Canada’s Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing*, 2011, p. 32

[189] These examples were provided in an interview with Mtre. Éloïse Gratton.

[190] See also DAAC Principle V (a) CHILDREN: Entities should not collect Personal Information for Online Behavioural Advertising purposes from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioural Advertising, or otherwise engage in Online Behavioural Advertising directed to children they have actual knowledge are under the age of 13, unless such collection and other treatment of Personal Information is in accordance with Canadian privacy legislation.

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

[192] DAAC, *Canadian Self-Regulatory Principles for Online Behavioural Advertising*, p. 6

Facebook and Google, although both careful to name the categories of sensitive information, do not list exactly the same types of information. Paul Ohm makes the same observation about the United States: the lists pre-established by companies, both as regards the voluntary codes and their privacy policies, contain different types of information, whose scope does not seem the same from one document to another[193]. The mismatched nature of these categories may be an indicator of the confusion that reigns as to what constitutes sensitive information; it is also a sign that companies might benefit from more guidance in establishing these categories.

Moreover, while we do not know the precise uses that most of the companies studied make of sensitive information, we do know that they widely collect and use certain information that could generally be regarded as sensitive. This is primarily true of the contents of consumers’ correspondence, which several services (such as Yahoo! Mail) openly admit that they analyze, with apparently no more formal consent as for the remainder of their users’ information. The same applies to consumers’ geographical location, which could often be considered sensitive information; again, we have seen that companies like Google are not shy to inquire where consumers are located, including accessing their GPS data[194].

Categorizing is therefore a relatively unconvincing exercise which will not, at least by itself, make it possible to impose effective limits on the collection of personal information in the context of OBA. However, based on the results we have obtained, it appears possible to provide companies with better guidance concerning which types of information are problematic. Without excluding the flexibility of the law, benchmarks could be proposed for better harmonizing business practices and classifying certain types of information as sensitive. These types of information should obviously include the topics that are usually considered to be sensitive, such as health, finances, sexuality, opinions and affiliations, ethnicity, family, and information pertaining to children. Also, other categories of information should be explicitly added to the list, and in particular should include consumers’ precise geographical location and the content of their private correspondence. Such benchmarks, however, will not be a panacea and will have to continue to be applied in tandem with other means of control for the benefit of consumers.

4.5. A look at foreign law

In other countries, the collection of personal information for the purposes of OBA poses similar challenges to those faced in Canada. The United States and the European Union have chosen two different approaches to regulate this practice: the U.S. has opted for self-regulation, whereas Europe has chosen to develop general, binding standards.

[193] Paul Ohm, “Sensitive Information” (2015) 88 S. *Cal. L. Rev*. [forthcoming], pp. 11-12

[194] In the American context, author Blase Ur also regrets that none of the self-regulatory programs in the industry include location and correspondence under “sensitive” data: Giovanni, Pedro 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

4.5.1. The United States

The United States has not adopted a general legislative framework on the protection of personal information, whether online or offline. Although some provisions of various laws may incidentally be applied for the purposes of OBA – for example, in matters of fraud[195], electronic surveillance[196] or information about children[197] – there is no federal law that specifically regulates OBA[198].

In the absence of binding norms, the Federal Trade Commission (FTC) has issued guidelines that set forth principles that companies can follow to regulate OBA[199]. These principles more or less reiterate those found in many self-regulatory instruments created by business associations, including the *Self-Regulatory Principles for Online Behavioural Advertising* of the Digital Advertising Alliance (DAA)[200] and the *Code of Conduct* issued by the Network Advertising Initiative (NAI)[201].

The FTC and the voluntary codes promote the principles of transparency and control, which stress that consumers should be informed about the sites they visit and the data that is collected from them[202]. The information should not be buried inside a complex privacy policy; to ensure that consumers are fully informed, the agency encourages companies to develop innovative methods and clear information for their benefit[203].

According to the FTC, consumers should also be able to choose whether or not to participate in OBA, and have a simple mechanism for doing so[204]. The OBA industry in the U.S. has responded to this request by offering the public the same opt-out mechanism as that provided via the

[195] *Computer Fraud and Abuse Act*, 18 USC § 1030 (2006)

[196] *Electronic Communications Privacy Act of 1986*, 18 USC §§ 2510-2522

[197] *Children's Online Privacy Protection Act of 1998*, 5 USC 6501-6505

[198] Paul Ohm, "Sensitive Information" (2015) 88 S. *Cal. L. Rev*. [forthcoming], pp. 8-9. In 2011, draft laws aimed at regulating the practice were introduced, but died on the order paper: HR 654, Rep. Jackie Speier (D-CA), *Do Not Track Me Online Act of 2011*; Sen. John Kerry (D-MA), co-sponsor Sen. John McCain (R-AZ), *Commercial Privacy Bill of Rights Act of 2011* (April 12, 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, pp. 289-290

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

[201] The NAI is a member organization of the DAA, which currently oversees actually a large number of organizations, including the IAB. The scope of the NAI code is slightly narrower than that of the DAA because the NAI is composed of third parties only, whereas the DAA code generally applies to anyone participating in OBA. In any event, the two codes provide very similar provisions with some variations. See: Network Advertising Initiative, *NAI Code of Conduct*, 2013, pp. 2-3

[202] This analysis will omit certain principles which, although relevant, are beyond the scope of this study. This is the case with Principle 2 in the FTC guidelines, which specifies that adequate security measures must be taken to protect data, depending on the sensitivity of the information. 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, pp. 35-37, 46. It could, for example, be a phrase like "Why am I seeing this ad?" next to an ad.

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

AdChoices icon found in Canada[205]. The FTC also supports the inclusion of a "Do Not Track" mechanism within users' browsers, as it considers this to be a more effective solution for consumers[206].

However, the level of consumer consent to OBA is modulated according to the type of information collected. The NAI code, for example, defines three types of information, each carrying specific obligations. First, the data used to identify a particular individual directly is called "personally identifiable" ("Personally Identifiable Information (PII)"); this relates to a very limited amount of information, such as the person's name, address or telephone number. "Non-Personally Identifiable Information" is information that can be linked not to a person but to a specific computing device: unique ID, IP address, etc. Finally, "De-Identified Data," is the term the code uses for data that cannot reasonably be linked to a person or to a particular device. While opt-in consent is required for the use of PII, opt-out consent is sufficient for "Non-PII" data. It seems that no consent is required for "de-identified" data.

This typology of data collected for OBA purposes differs significantly from that in the state of law in Canada, in which the notion of "personal information" seems far more encompassing. These American standards are helpful, however, in explaining certain distinctions observed when analyzing the privacy policies of online services offered to Canadians, in which several companies seem to avoid their responsibilities when it comes to data that they do not consider to be "personally identifiable."

There are nonetheless similarities to be found between the American and Canadian situations. For instance, just like in Canada, the U.S. framework sets tighter restrictions in the case of more sensitive information. In fact, the FTC states that companies must obtain express consent from the consumer when the company intends to collect such information for OBA purposes[207]. The agency does not specify exclusive categories or give a precise definition of sensitive information, as it considers this to depend on context:

> 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

[205] This mechanism can be found at: 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*, presented to the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce, United States House of Representatives, December 2, 2010

[207] The FTC specifies a second situation in which such consent must be obtained: when the representations made to consumers about the processing of their information undergoes a "material" (i.e . significant) change. This requirement of explicit consent only applies, however, when the change affects previously collected data; if this applied only to information collected after the change in policy, we can understand why we might be satisfied with implied consent. FTC, 2009, p. 41; FTC, *Self-Regulatory Principles for Online Behavioral Advertising*, FTC Staff Report, 2009, p. 47

> whether there may be certain categories of data that are so sensitive that they should never be used for behavioural advertising.[208]

In their implementation of the FTC guidelines, the voluntary codes were nonetheless rather clear-cut as to what the notion of “sensitive data” covers. In addition to certain information concerning children[209], they set forth lists of specific information that companies should not collect or use without the consent of the user[210]. For the AAD, this information is: financial account numbers, social insurance numbers, and pharmaceutical prescriptions or medical records relating to a specific person[211]. The NAI code is a little wider, listing, in addition to social insurance numbers and financial account numbers, insurance policy numbers, sexual orientation, and “precise information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history[212].”

Faced with these well-defined lists, business associations at least admit that it might prove necessary to add other fields[213]. And for good reason: these lists contain some noteworthy omissions with regard to information usually considered sensitive, including political opinion, ethnicity, the individual’s family life, private correspondence or geographical location. In the latter case, the 2013 NAI code smacks of fence-sitting:

> 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].

This means that in the absence of a binding framework to this effect, there will be very few cases in which express consent sets limits on the collection of personal information for the purposes of OBA in the United States.

4.5.2. European Union

Inside the European Union, two Directives are applied in the context of OBA[215]. The first, Directive 95/46/EC known as The Data Protection Directive[216], oversees the processing of

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

[209] The voluntary codes we consulted state that members must undertake to respect to the *Children's Online Privacy Protection Act*, which stipulates that parental consent has to be obtained to collect certain information on children under 13 years of age1. See: DAA *Self-Regulatory Principles for Online Behavioral Advertising*, 2009, pp. 16-17

[210] According to the NAI Code, this consent should be by opt-in.

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

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

[213] According to the 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,” See: DAA *Self-Regulatory Principles for Online Behavioral Advertising*, 2009, p. 40; Network Advertising Initiative (NAI), NAI Code of Conduct, 2013, pp. 4 and 11

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

[215] European Union directives must be transposed into the national law of each Member State.

[216] *Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23.11

personal data in general. The second, Directive 2002/58/EC, known as the "E-Privacy Directive[217]," applies more specifically to the personal information protection issues raised by new technologies.

These directives create a framework for the processing of consumers' "personal data." They set forth principles similar to those of Canadian laws, such as limiting collection, right of access and, of course, the consent of the person concerned. Just as with the definition of "personal information" in Canada, the definition of "personal data" used is broad and inclusive, and may include for example an IP address[218] or, in all likelihood, the unique identifier of a cookie.

The legal requirements related to the type of consent obtained in the context of OBA, however, appear to be tighter in the EU than in Canada, where, as we have seen, the law is generally satisfied with implied consent to collect personal information with the aid of a cookie. In fact, in 2009, article 5 (3) of the E-Privacy Directive was amended in order to tighten requirements in this regard:

> Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia about the purposes of the processing. [Emphasis added][219]

Such language suggests that, generally, only explicit consent is acceptable for installing a cookie on a consumer's computer. In fact, according to the Article 29 Working Party on Data Protection[220], this consent must not only be express; it must also have been obtained "before the personal data are collected, as a necessary measure to ensure that data subjects can fully appreciate that they are consenting and what they are consenting to[221]." According to the working party, once consent is obtained, it will not be necessary to obtain it again every time the advertising network gains access to it; however, consent should be requested again periodically[222] and be revocable at any time.

.1995. Proposals for reforming the Directive have been discussed within the European Union since 2012. However, at the time of writing, the Council of the European Union has not yet adopted a proposal in this regard in the European Parliament. See *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, COM (2012) 11 final - E 7055

[217] *Directive 2002/58 / EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications*), OJ L 201, 31.7.2002

[218] See, for example: *Productores de Música de España (Promusicae) v Telefónica de España* SAU, ECLI: EU: C: 2008: 54

[219] *Directive 2002/58 / EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications*), OJ L 201, 31.7.2002, s. 5 (3)

[220] Working Group "Article 29" is an independent European advisory body on data protection and privacy.

[221] Working Group "Article 29" on the Protection Of Data*, 2/2010 Reviews behavioural advertising*, June 22, 2010, p. 15

[222] In France, for example, the CNIL stipulates that a cookie installed on a device may have a shelf life of 13 months, beyond which, new consent should be requested. See: CNIL « Cookies & traceurs : que dit la loi ? » online at: http://www.cnil.fr/vos-obligations/sites- Web-cookies-et-autres-traceurs/que-dit-la-loi/

In practice, however, this process is not as strict as the Directive suggests. In France, for example, where the EU Directive was incorporated into the *Data Protection Act of 6 January 1978,* the CNIL[223] asserts that the consent of the user to install a cookie on their computer can be obtained by displaying a banner on the site being consulted[224]. This banner will notify the user of the specific purposes for which the cookies are used, of the opportunity to refuse installation by clicking on a link in the banner, and above all, of the fact that the user consents to the installation of the cookie if the latter continues navigating on the site, that is to say, by accessing other pages.

We see that the implementation of this so-called “express” consent nonetheless has some features in common with the implied consent we are familiar with in Canada. Even if the consumer is informed in advance of the intrusion of cookies for advertising purposes, those who choose to ignore the information and continue browsing the site thereby implicitly consent to their installation. In addition, the opting-out mechanism is not directly accessible to the user, who to avoid being tracked, must follow a potentially “piecemeal” opting-out procedure that is located on another page.

Like Canada and the United States, European law sets additional restrictions on categories of sensitive information. These are set forth in Article 8 of Directive 95/46 / EC:

> Member states shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.[225]

We can see that the European Union chose to adopt a less flexible approach than Canadian law to determine what constitutes sensitive information, by providing an exhaustive list. While reading this article, one gets the impression that any processing of these data types will be prohibited, the CNIL admits it will be possible to collect such data for OBA purposes, but only provided that very high consent requirements are respected and that the purpose and the public interest justify it:

> To lawfully collect and process this type of information, ad network providers would have to set up mechanisms to obtain explicit prior consent, separate from other consent obtained for processing in general[226].

Similarly, under Article 9 of the E-Privacy Directive, special protective measures are provided for localization data, which is defined as “any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly

[223] La Commission Nationale de l’Informatique et des Libertés (CNIL) is a French public body that is mandated to protect the rights of citizens with regard to Information Technology.

[224] The exact form of this may vary: an overlay zone, a checkbox or other ads that appear on the site the user is visiting.

[225] *Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23.11.1995, s. 8

[226] *Working Group “Article 29” On The Protection Of Data, 2/2010 Reviews behavioral advertising*, 22 June 2010, p. 23

available electronic communications service[227].” This attests that European law recognizes the sensitive nature of such data.

[227] *Directive 2002/58 / EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications),* OJ L 201, 31.7.2002

Conclusion and recommendations

Should there limits be set on the collection of personal information for the purposes of online behavioural advertising? Certainly, but there are many pitfalls involved.

First of all, the law already imposes limits on the collection of information for the purposes of OBA, limits that companies often ignore. For example, there is a marked disparity between the legal obligation of businesses to collect only the personal information necessary for the purposes that they claim, and the almost unlimited amount of data they actually do collect. Moreover, many do not even seem to consider all this data as personal information at all, in contradiction to the definition given by law.

Also, the online environment and the very concept of privacy makes it difficult to set in place universal benchmarks based on the types of personal information collected. In the focus groups, consumers told us that the closer a piece of information approaches their sphere of privacy, the less they are willing for it to be used for the purposes of OBA. This aligns almost perfectly with the concept of sensitive personal information as defined by law, case law or doctrine. Based on these results, it is possible to designate certain categories of information that companies should consider sensitive in the context of OBA: health, personal finances, sexuality, beliefs and affiliations, ethnicity, family life, precise geographical location, private correspondence, and information about children.

While the Federal Act adopts a contextual approach to the sensitivity of information, practice teaches us that the companies themselves have determined rigid categories based on what they believe constitutes sensitive information – with the collateral effect that some have a more restrictive interpretation than others. In addition, many companies do not seem to consider certain information, such as geographical location and the content of private correspondence, to be necessarily sensitive. In this regard, it might be possible to provide companies with better guidance, or even oblige them to explicitly recognize certain information as sensitive in nature.

But there are no magical solutions. The major shortcoming of the category approach resides in the fact that by clearly defining certain types of information, some other types of harmful situations will be allowed to slip between the cracks. The sensitive nature of an information item is a highly contextual issue – something that predefined lists or algorithms are clearly not able to appreciate. While the approach espoused by the Federal Act provides the flexibility to deal with individual situations, this same flexibility threatens to usher in even more confusion and uncertainty. In such a context, it can be argued that a hybrid approach that retains the flexibility of the Act while defining certain rigid categories, would perhaps serve consumers better.

However, even with such arrangements, other mechanisms would still be needed to adapt to the context of each situation. Since algorithms can not universally determine what information is sensitive for everyone, nor even decide what information a person wants or does not want for advertising purposes, we will have to rely for the rest on the will of the parties involved. In the light of such considerations, the principle of consent and the wider issue of consumer control over personal information assumes even more relevance.

But for consent to be valid, it still needs to be informed. Our analysis has highlighted the work that remains to be done in this area, particularly as regards the information given to consumers, and the lack of transparency and effectiveness of the opt-out mechanisms available to them. Yet, simple and effective methods for validly consenting to behavioural advertising are quite feasible: think for example of the “Do Not Track” option incorporated within the browser, a solution that the FTC has also promoted. In the case of sensitive information processing, express consent as required by law could be obtained through separate, explicit and specific reference to each proposed use.

Implementing effective mechanisms to inform and obtain the consent of consumers certainly seems imperative for ensuring true compliance with the law. But the technological context also raises another problem: consumers have a very limited understanding of the invisible processes that go into action as they are browsing the Web, or more generally of the new technologies that are constantly entering their daily lives. Here we can question whether the development of digital literacy among consumers – including the operation of computer devices, programming languages and, ultimately, new advertising systems – would allow them to better understand the choices available to them, and ideally, to give truly informed consent. For these reasons, improving digital literacy among Canadians is a field that perhaps deserves to be further explored[228].

Categorization, transparency, consent, education: setting limits on the collection of personal information for the purposes of OBA is an ambitious undertaking. Successful implementation would result, among other things, in people having a conscious, meaningful opportunity to reject online tracking for advertising purposes. Given what we have learned in the focus groups, it could mean that large numbers of consumers could suddenly choose to refuse or severely limit the tracking they are subjected to. To this, some would object that such a move would significantly deprive many business of the benefits of online profiling, resulting in a sharp decline in advertising revenues.

There are other threats that darken the economic outlook for free online service providers. For example, the AdBlock Plus software, which allows Internet users to remove all the ads that normally appear in their browsers, gradually attained a critical mass of users; on Chrome, by June 2014, this extension had been downloaded over 40 million times. We also began to see alternatives to the services of large technology companies, which do not depend on the collecting personal information from users in order to generate revenue. Among these are France’s *Dégooglisons Internet*[229] (let’s de-Google the Internet) associated with the free software movement that provides Internet users an alternative to Facebook: the Framasphere network[230].

Does this sound the death knell of a business model? Will the law and consumer resistance see the “free” Web economy gradually shrink away to nothing? Such a prognosis probably underestimates the ingenuity of the “technological wizards.” For instance, according the Information and Protection of Privacy Commissioner of Ontario, who promotes the principles of

[228] Readers may find the initiatives of the MediaSmarts digital literacy group to be of interest: http://habilomedias.ca

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

[230] https://framasphere.org/

"Privacy by Design"[231], fully respecting the laws in force is not incompatible with economic development; on the contrary, it is actually an opportunity to innovate in order to benefit everyone[232]. When it comes to OBA, there is no shortage of avenues to explore: whether by developing algorithms that are less greedy for personal information, by recognizing its monetary value, or by exploiting the profit potential of truly anonymous information. Although such approaches may entail rethinking the economic foundations of their business models, legal compliance is not synonymous with a death knell for such companies, but an opportunity to find innovative solutions.

Option consommateurs therefore submits the following recommendations:

Recommendations to the federal government and the provinces:

- **Option consommateurs recommends that companies participating in OBA be compelled to implement simple, effective, harmonized mechanisms to permit consumers to properly and actively consent to the collection of their personal information for the purposes of OBA. In doing so, they should particularly explore the possibility of compulsorily integrating a "Do Not Track" type mechanism within the browser.**

- **Option consommateurs recommends increasing the funding and powers of Canadian privacy protection commissions and of the authorities responsible for enforcing the privacy laws, in order to more effectively address the challenges posed by the new technologies.**

- **Option consommateurs recommends developing and promoting digital literacy initiatives for Canadians, to assist them in learning the operation of computer devices, programming languages and new advertising systems.**

Recommendations to Canadian privacy commissions and the authorities responsible for the enforcement of laws respecting the protection of personal information:

- **Option consommateurs recommends that guidelines be established to designate which types of personal information are sensitive in nature. These types of information should include information relating to health, personal finances, sexuality, beliefs and affiliations, ethnicity, family life, precise geographical location, the content of private correspondence and information relating to children. However, the establishment of such a list should in no way limit the scope and flexibility of the law, in order that the sensitivity of any other information may continue to be evaluated in context.**

- **Option consommateurs recommends that compliance with the principle of the need to collect personal information be investigated as specified in the *Personal***

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

[232] Ann Cavoukian et al., *The Unintended Consequences of Privacy Paternalism, the Information Commissioner and the protection of privacy of Ontario*, 2014, p. 10

***Information Protection and Electronic Documents Act*, by obtaining accurate information from free Internet service providers on the treatment and use made of each item of personal information they collect from their users.**

Recommendations to free Internet service providers:

- **Option consommateurs recommends that free Internet service providers abandon the restrictive notion of “personal data” included in their privacy policies, and explicitly consider all the data they collect to be personal information within the meaning of Canadian privacy laws.**

- **Option consommateurs recommends that free Internet service providers disclose and expand the categories of information that they consider sensitive. In particular, they should consider precise geographical location and correspondence as sensitive information.**

- **Option consommateurs recommends that free Internet services develop better mechanisms to inform consumers of their advertising practices and obtain to their consent in accordance with the law, in particular by respecting the “Do Not Track” signal emitted from a browser.**

Recommendations to consumers:

- **Option consommateurs recommends that consumers inform themselves about the personal information that the companies whose online services they use collect on them, the use these providers make of it, as well as the means available to consumers to limit online tracking.**

- **Option consommateurs recommends that consumers lodge complaints with the competent authorities if they feel that their privacy is not being respected by the companies with which they contract online.**

Appendix 1 - Discussion Guide (English version)

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 you 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 that 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 you 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 email 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 device 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

What foods and restaurants you like
Your preferred entertainment activities (e.g. films, music, video games, attending sports etc…)
What preferences you have for consumer goods like clothes, cars, electronics etc…
The fact that you are looking for a new job
The fact you are soon getting married
Your hobbies and leisure activities (e.g. gardening, hiking, sports, crafts etc…)
That you work out and or belong to a gym
Financial information like your approximate income level, retirement plans, credit applications
Where you have travelled to or plan to travel to
Issues you are interested in like environmental protection, foreign policy, politics etc…
Your personal health and medical conditions you may have
That you are online dating
Your love life, sexual orientation or sexual preferences
Your marital and familial status – whether you are divorced, whether you have kids etc…
Your religious beliefs or political opinions

Your ethnic origin
The content of your private messages and who you correspond with
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 actually do 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 you worth something?

Thanks for your participation!

Appendix 2 – Discussion Guide (French version)

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