ARTICLE

OUR DIGITAL SELVES: PRIVACY ISSUES IN ONLINE BEHAVIOURAL ADVERTISING

By Christopher Scott*

CITED: (2012) 17 Appeal 63-82

INTRODUCTION

Canadians are spending more of their lives online than ever before.[1] This trend has profound ramifications across Canadian society, including within the field of privacy law. This paper will examine the privacy implications of two related technologies within the emerging field of online behavioural advertising. The first is the use of tracking cookies to track users' activity across websites, and the second is deep packet inspection ("DPI"). The use of these technologies in the field of targeted advertising has not yet been subject to a finding under the *Personal Information and Protection of Electronic Documents Act ("PIPEDA"* or the *"Act"),*[2] the federal private-sector privacy statute.

The goal of this paper is to survey the application of *PIPEDA* to this yet-nascent field and describe the shape that a *PIPEDA*-compliant use of these technologies is likely to take. For context, I will make reference to two prominent corporations at the forefront of this field: Google and Phorm. These corporations are intended to be viewed as case studies. The goal of this paper is not to catalogue the apparent failures of either organization in the style of a complaint to the Privacy Commissioner, but rather to illustrate the delicate interplay of – and tensions between – privacy rights and legitimate commercial interests.

I. THE TECHNOLOGIES AT ISSUE

Before exploring the legal issues arising from these technologies, it is necessary to have some familiarity with the technical manner in which they operate and an understanding of the kinds of personal information they enable organizations to obtain. Understanding the present and potential use of these technologies is essential to framing the privacy issues they raise.

---

* Christopher Scott is a J.D. candidate at the University of Victoria. He wrote this paper for the course "Information and Privacy Law", taught by David Loukidelis and Murray Rankin, Q.C. He is grateful for David and Murray's encouragement and depth of insight on this and related topics. Christopher is actually quite fond of Google, and finds some of this paper's conclusions to be bittersweet.

1. Statistics Canada, *Canadian Internet Use Survey* (Business Special Surveys and Technology Statistics Division, 2009), online: The Daily <http://www.statcan.gc.ca/daily-quotidien/100510/dq100510a-eng.htm>.
2. SC 2000, c 5.

A. Tracking Cookies

i. How Tracking Cookies Work

When a web browser visits a website, that site may instruct the browser to store a "cookie". A cookie is a small text file containing information provided by the website. If a browser has been given a cookie by a website, it will send the cookie back to the website on every subsequent visit. By placing a unique identifier in each cookie, the website can use cookies to keep track of a particular web browser's comings and goings.[3] This interaction is invisible to the user operating the browser, and typically occurs without his or her explicit consent.[4]

Tracking cookies do more than enable organizations to identify users within the confines of their own websites. Organizations also use them to track browsers across the websites of third parties with which they have partnered (and which have added a piece of code to their own websites to enable this). In this way, tracking organizations can keep track of browsers' activity across extensive networks of partnered sites. These cookies enable the organizations to record information including the time of the access, the IP address of the browser (which may reveal the approximate geographic location of the browser), the URL of the pages visited, the contents of the pages visited and the unique identifier stored in the browser's cookie.[5]

Up to this point, I have referred primarily to "browsers" and only rarely to "users". This is intended to highlight the fact that tracking cookies see only browsers, not people. Generally, a cookie is particular to a single browser on a single computer user account (usually on a single computer). Accordingly, one person may be associated with many tracking cookies, and a single tracking cookie can capture the personal information of multiple individuals. The most relevant example here is of a family computer with a single user account. To the extent that members of the family (as well as any guests) use a common browser on the computer, they will be tracked together, and all of their disclosed personal data will be lumped together under the cookie's common identifier.

Finally, the last relevant consideration regarding browser cookie technology is that cookies have expiry dates. When a cookie expires, it gets deleted, meaning the issuing organization must issue a new unique identifier the next time that the browser visits. Similarly, most browsers allow users to manually delete cookies before their expiry dates. This is an effective *tabula rasa*; having lost the key that ties your browser to your past browsing behaviour, the organization must now start from scratch with a new identifier.

ii. Case Study – Google AdSense

The most prominent system of tracking cookies is Google's AdSense.[6] Google serves advertisements on the websites of its vast network of partners – by some estimates, nearly one in five websites display Google AdSense advertisements.[7] These advertisements are

---

3. For instance, my Google Chrome browser on my laptop computer has the unique identifier "aab213735d8023ea".
4. Electronic Privacy Information Center, *Cookies, online: <http://epic.org/privacy/internet/cookies/>.*
5. *C.f.* Google Privacy Center, online: <http://www.google.com/privacy/ads/>
6. References to "AdSense" throughout this paper also refer to DoubleClick, a parallel advertising network owned by Google that is based on the same technology and even uses the same cookie. See also *note 5*.
7. W3Techs, *Usage of advertising networks for websites, online:* <http://w3techs.com/technologies/overview/advertising/all>.

not stored on the webservers of the website that users have chosen to visit; they are served directly from Google's servers to the browser, where they are displayed alongside the contents of the website that was requested. In the process of fetching the advertisement from Google's servers, browsers dutifully send Google their tracking cookies. This interaction provides Google with all of the above-mentioned information, including the URL of the page that the user has chosen to view.[8]

As a consequence, not only can Google mine every search you perform on the Google homepage[9] for information about your interests and browsing habits, but it also knows which of its partnered websites you visit independently. Google collects all of this information and, based on the content of sites that you frequent, infers which "interest categories" consumers might be interested in. On the basis of these categories and the contents of the page that you are presently viewing, Google can tailor the advertisements it sends you on its partner sites.[10] Thus, a user in Canada who frequently searches for travel information on Google and chooses to view a website about Mexican history might see advertisements about travelling to Mexico displayed on that site.

In the context of privacy law, it is significant to note that this browser data can be collected even if the browser has never been to a Google-owned webpage or had the opportunity to agree to Google's privacy policy directly. Google requires that partners provide notice of Google's collection of browsing information from the partner's site as well as other sites across the web for the purpose of serving advertisements based on that behaviour; they also require partners to notify users of cookie management options.[11] This is typically accomplished via the incorporation of Google's privacy policy into that of the partnered website. In addition, because ads are served simultaneously with webpages, users may be required to view ads – and thus disclose personal information – in order to find the third-party's privacy policy. Even if users disagree with the privacy policy of that third party, Google has already collected their personal information.

Prior to 2007, Google's tracking cookie was set to expire in 2038 (in effect, never), but in response to privacy concerns it now has a two-year rolling expiry date that is renewed every time the cookie gets used.[12] In practice, this means that the cookie is unlikely to expire before the user ceases using the browser permanently, either due to switching to a new browser, user account, or computer (at which point a new cookie is created). Google stores user interest information for at least as long as the cookie's active life - but anonymizes server logs (which include IP and URL information) after 18 months as a matter of policy.[13] Google insists that a shorter retention period would reduce their ability to protect user security and may put them in violation of the data retention laws of some countries.[14] Google's retention policies are not codified in its privacy policy.[15]

---

8. Google Privacy Center, *supra note 5*.
9. Google, online: <http://google.com>.
10. Google Privacy Center, *supra* note 5.
11. AdSense Terms and Conditions, online: <https://www.google.com/adsense/localized-terms>.
12. Peter Fleischer, "Cookies: expiring sooner to improve privacy" (16 July 2007), online: The Official Google Blog <http://googleblog.blogspot.com/2007/07/cookies-expiring-sooner-to-improve.html>.
13. Peter Fleischer and Nicole Wong, "Taking steps to further improve our privacy practices" (14 March 2007), online: The Official Google Blog <http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html>.
14. Google Log Retention Policy FAQ, online: Public Intelligence <http://publicintelligence.info/google-log-retention-policy-faq/>.
15. Google Privacy Policy, online: <http://www.google.com/intl/en/privacy/privacy-policy.html>.

Google provides an opt-out mechanism for users. Users must opt out for each browser on each computer that they use, due to the technical limitations discussed above.[16] Google also provides an interest-management tool that enables users to voluntarily disclose to Google the types of advertisements in which they are interested (referred to as "interest categories") and to remove interest categories from that list of interests.[17] Google is careful to note that no personally identifiable information is collected "without your explicit consent"[18] and that it "will not associate sensitive interest categories with your browser (such as those based on race, religion, sexual orientation, health, or sensitive financial categories)".[19] Google does, however, track user product interests; for instance, a perusal through my own aggregated list of interests revealed that Google was aware of my fondness for purchasing computer hard drives online.

Google's privacy policy states only that Google takes "appropriate security measures" to safeguard data acquired through tracking cookies, that employees and contractors may view it only on a need-to-know basis, and that third parties who do access it on this basis are bound by confidentiality agreements and may even suffer criminal consequences for a breach of security.[20]

B. Deep Packet Inspection

i. How Deep Packet Inspection Works

At a technical level, DPI is quite straightforward. Whenever you do anything on the Internet – such as loading a webpage or sending an e-mail – you either send or receive "packets" of digital information. Every packet you send goes directly to your Internet service provider ("ISP"), which then sends it off in the direction of its intended destination. Similarly, every packet you receive comes first to your ISP, which then sends it straight to you. As a result, your ISP can see all of your unencrypted digital communications directly, without resorting to the use of tracking cookies or the like. This allows for much broader disclosure than tracking cookies, as DPI reveals not only where users go, but also what they do.[21]

On the other hand, DPI is computationally expensive, meaning that it requires substantial equipment and technical expertise to perform effectively. Most ISPs do not have the equipment or the expertise to analyze the entire contents of every packet of information that passes through their networks. Every packet of information contains "header" information and "payload" information. Headers include the packet's source and destination IP addresses, the protocol being used, the port being used (which roughly corresponds to the application that sent it),[22] and other network-related technical information. The payload is the information that is being delivered. This payload may

16. Google Privacy Center, *supra* note 5. Google also offers a downloadable tool that will opt all browsers on a single computer out of AdSense's tracking program.
17. *Ibid.*
18. *Ibid.*
19. *Ibid.*
20. Google Privacy Policy, *supra note 15.*
21. *Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection* (3 September 2009), PIPEDA Case Summary #2009-010 at paras 4-8, online: OPC <http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.cfm>. This OPC decision goes into much more technical detail regarding the workings of DPI, but reaches the same conclusion: DPI can give ISPs the technical ability to see nearly everything.
22. I say "roughly" here because, ideally, each port number refers to one application. However, applications can select their own port numbers, meaning that some will "spoof" another application's number in order to get preferential treatment. *C.f.* note 23 at paras 10600-10602.

not be readable on its own, however; a single piece of information can be split up between several packets, so each of those packets can be collected and then read together. Bill Keenan, Director of Technology for CTV, described the technical challenges involved as follows:

> [T]he expense involved in doing true Deep Packet Inspection – which means not just inspecting the headers … which is, functionally, the address on the envelope, but actually opening all of the envelopes and pasting them together and seeing what it reads. Doing that for every piece of content that comes over the network would absolutely be prohibitively expensive.[23]

For this reason, DPI may consist either of merely reading packet headers or reading the entire contents of each packet. Throughout this paper, references to DPI will refer to the latter method. An inspection of a consumer's packet contents may reveal "photo images, [or] financial and contact information",[24] in addition to the information revealed in the packet headers. However, the reading of packets' header information should not be discounted. Canada's Privacy Commissioner has previously noted that headers are rich with personal information – if analyzed, they can identify the use of "most popular services or applications", "[s]ubscriber usage patterns", "[a]pplication usage patterns", "competing services and their presence on the network" and "malicious traffic on the network".[25]

ii. Case Study – Phorm Inc.

DPI provides incredibly detailed information about consumers' lives through their use of the Internet. Accordingly, it can be applied in a variety of circumstances. For instance, some Canadian ISPs routinely use DPI for traffic-management purposes (such as by prioritizing the transfer of time-sensitive packets issued by internet telephony applications).[26] However, no Canadian ISPs are presently using DPI for advertising purposes, and none examine the payload of packets for personal information – they read only the headers.[27] For examples of DPI-enabled advertising, we will need to look beyond our borders.

Phorm Inc. is the one of the most-publicized organizations pursuing DPI-enabled advertising. Phorm contracts with ISPs to do the heavy lifting of DPI for them. In these arrangements, the ISPs send Phorm all of their consumers' packets, from which Phorm generates a profile of a user's interests. This requires performing at least a header-level analysis on all packets sent *by* the user; Phorm also reads the contents of most packets sent *to* the user.[28] This allows Phorm to collect, at a minimum, "website addresses, searches [and] browsing history" as well as the full page contents of nearly everything that users read online.[29]

---

23. CRTC, Transcript of Proceedings, *Canadian broadcasting in new media* (10 March 2009) at para 10605.
24. *Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection, supra* note 21 at para 16.
25. *Ibid* at para 15.
26. *C.f.* note 21.
27. CRTC, Transcript of Proceedings, *Canadian broadcasting in new media* (27 February 2009) at para 8051.
28. Chris Williams, "How Phorm plans to tap your internet connection" *The Register* (29 February 2008), online: The Register <http://www.theregister.co.uk/2008/02/29/phorm_documents/>.
29. Technology, online: Phorm Inc. <http://www.phorm.com/technology/>.

To compensate for the broad scope of its data collection, Phorm has taken a strong initiative in limiting the retention and use of this data. The company is careful to note that users' IP addresses, browsing history, search terms and the like are not stored.[30] Phorm analyzes the information for indications of the user's interests, stores that derived user-interest information, and then deletes the information that was originally collected.[31] Like Google, Phorm does not associate "sensitive" user interests (such as medical or adult information) with consumers' accounts.[32] Phorm claims to substantially curtail the invasiveness of its DPI analysis by excluding non-web packets (such as e-mail or VOIP), certain web-based e-mail services and form submissions (that is, user content posted to the web) from its analysis.[33] As a result, although Phorm still collects far more personal information that Google, Phorm uses information in a similar manner to Google and claims to retain less of it.

Much like Google, Phorm uses the information it collects to serve ads on third-party websites. It also offers an opt-in website-recommendation service directly to users (dubbed PhormDiscover) and a security service directed at warning users about potentially fraudulent websites (PhormSecure). Although Phorm originally intended to use the information collected to serve ads as part of an opt-out scheme (rather than opt-in), it has been required by UK regulators to adopt an opt-in program, which it now uses in all markets.[34] Phorm currently operates in Brazil, Korea, the United Kingdom and the United States.[35]

Also similar to Google, Phorm's Privacy Policy promises "security measures", employee training, and contractual safeguards to govern third parties. Phorm is careful to note that no system is 100% safe, but reminds users that no personally identifiable information is stored by Phorm.[36]

II. THE SCHEME OF *PIPEDA*

A. Jurisdiction and Reasons for Focusing on *PIPEDA*

PIPEDA is not the only private-sector privacy statute in Canada, but it is the only one discussed in this paper. Although some provinces have enacted substantially similar legislation that supersedes *PIPEDA* within their jurisdictions, the federal *Act* is generally applied against collection, use or disclosure of information across provincial or national lines.[37] This generally describes the activities of telecommunications and online behavioural advertising organizations such as Google and Phorm. Additionally, since telecommunications and online advertising corporations are often federally incorporated (if they are incorporated within Canada at all), *PIPEDA* is the most consistently relevant

30. Phorm Service Privacy Policy, online: <http://www.phorm.com/privacy_policy/phorm_service_policy.html>.
31. "Andrew Walmsley on digital: Phorm and function fuel privacy fears" *Marketing* (26 March 2008), 14 (CPI.Q).
32. PhormDiscover: How it Works, online: <http://www.phorm.com/consumers/phormdiscover/how_it_works/ >. (*nb:* This page includes information not only on PhormDiscover, but on Phorm's advertising program as well)
33. Brooks Dobbs, "Phorm: A New Paradigm in Internet Advertising", online: Office of Privacy Commissioner of Canada <http://dpi.priv.gc.ca/index.php/essays/phorm-a-new-paradigm-in-internet-advertising/>.
34. "Controversy surrounds Phorm" *Computer Fraud & Security* 2008:5 (May 2008) 4.
35. About Us, online: Phorm Inc. <http://www.phorm.com/about_us/>.
36. Phorm Service Privacy Policy, *supra note 30.*
37. Stephanie Perrin et al, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin Law, 2001) at 4-56.

privacy statute with respect to online behavioural advertising carried out by Canadian organizations.

Although it is a federal statute, the Federal Court held in *Lawson* that *PIPEDA* (and thus the jurisdiction that it grants to the Privacy Commissioner of Canada) also applies to extraterritorial organizations that engage in "the transborder flow of personal information",[38] such as Phorm and Google. Accordingly, the jurisdictional waters surrounding foreign-incorporated organizations are less murky: *PIPEDA* plainly applies. In the age of the supranational Internet, this is perhaps the single most compelling reason to focus on *PIPEDA* in the context of online behavioural advertising.

B. Organization of *PIPEDA*

PIPEDA is organized around a set of ten "Principles" adopted from the Canadian Standards Association's *Model Code for the Protection of Personal Information*.[39] These Principles are codified in Schedule 1 to the *Act*, imported into law by s. 5 and modified by ss. 6-9 of the *Act*.[40] Some Principles, such as those mandating consent and limited collection (Principles 3 and 4, respectively), impose broad and foundational obligations on organizations within the behavioural advertising industry. Others, such as those relating to accountability and challenges concerning compliance (Principles 1 and 10), are unlikely to operate differently in the context of behavioural advertising than they do generally. Principles falling under the former class will be described individually, roughly in order of their significance in the context. Principles falling under the latter class will be lumped together and only briefly mentioned.

C. Principle 3 – Knowledge and Consent Respecting Collection, Use or Disclosure

This Principle stipulates that "knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate."[41] The term "inappropriate" is given its meaning exhaustively by *PIPEDA* s. 7.[42] That section permits collection, use or disclosure without knowledge or consent only in certain circumstances, such as where collection is clearly in the interests of the individual and cannot be otherwise accessed;[43] where use is required for action in an emergency that threatens an individual's life, health or security;[44] or where disclosure to a government agency is required for national security reasons.[45] In all other circumstances, some measure of knowledge and consent must be provided.

The question, then, is what form (or degree) of knowledge and consent must be provided in a particular circumstance. Consent may take a variety of forms, ranging from implied consent on the low end (where no actual consent has been provided by the individual affected) to explicit consent on the high end. *PIPEDA* summarizes this range in Schedule 1:

---

38. *Lawson v Accusearch Inc*, 2007 FC 125, 2007 CarswellNat 247 at para 51 *[Lawson]*.
39. CSA Standard Q830, online: <http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code>.
40. *PIPEDA* ss 5-9 and Schedule 1.
41. *PIPEDA* Schedule 1 clause 4.3.
42. *Turner v Telus Communications Inc,* 2007 FCA 21, 2007 CarswellNat 172 at para 23 *[Turner]*.
43. *PIPEDA* s 7(1)(a).
44. *PIPEDA* s. 7(2)(b).
45. *PIPEDA* s 7(3)(c.1)(i).

> The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered **sensitive**. Implied consent would generally be appropriate when the information is less sensitive.[46]

The Privacy Commissioner of Canada has taken the following view as to the distinction between express and implied consent, as a matter of policy:

> Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.[47]

The Privacy Commissioner of Canada has expressed a low opinion of "opt-out" program schemes, calling them a "weak form of consent" and observing that "[o]pt-out consent is in effect the presumption of consent."[48] The Commissioner incorporated elements of s. 5(3) of the Act (discussed under Principles 2, 4 and 5 – Purpose, below) in holding that circumstances in which opt-out consent would be appropriate should "remain limited, with due regard both to the sensitivity of the information at issue and to the reasonable expectations of the individual."[49,50] The Commissioner then laid out criteria that an organization would have to meet in order to lawfully pursue an opt-out scheme rather than an opt-in scheme:

> 1. The personal information must be demonstrably non-sensitive in nature and context.
>
> 2. The information-sharing situation must be limited and well defined as to the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure.
>
> 3. The organization's purposes must be limited and well-defined, stated in a reasonably clear and understandable manner, and brought to the individual's attention at the time the personal information is collected.
>
> 4. The organization must establish a convenient procedure for easily, inexpensively, and immediately opting out of, or withdrawing consent to, secondary purposes and must notify the individual of the procedure at the time the personal information is collected.[51]

In *Aeroplan*, the Privacy Commissioner considered the appropriate level of consent regarding Air Canada's sharing of customers' information with Aeroplan, an advertising partner, for the purpose of providing targeted advertisements to consumers. The

---

46. *PIPEDA* Schedule 1 clause 4.3.6. C.f. paras 4.3.4 and 4.3.7.
47. Office of the Privacy Commissioner, *Your Privacy Responsibilities: Canada's Personal Information Protection and Electronic Documents Act* - A Guide for Businesses and Organizations, online: <http://www.priv.gc.ca/information/guide_e.pdf> at 2.
48. *Air Canada allows 1% of Aeroplan membership to "opt out" of information sharing practices* (11 March 2002), PIPEDA Case Summary #2002-42, online: OPC <http://www.priv.gc.ca/cf-dc/2002/cf-dc_020320_e.cfm> [*Aeroplan*]. (As early OPC decisions are not given paragraph numbers, no pinpoint has been provided.)
49. *Ibid.*
50. *C.f. PIPEDA* Schedule 1 clause 4.3.5.
51. *Bank does not obtain the meaningful consent of customers for disclosure of personal information* (23 July 2003), PIPEDA Case Summary #2003-192, online: OPC < http://www.priv.gc.ca/cf-dc/2003/cf-dc_030723_01_e.cfm>.

Commissioner concluded that express consent was necessary where there was a potential for "use and disclosure of information customized according to individual plan members' purchasing habits and preferences".[52] Although using personal information for the purpose of advertising is not objectionable *per se*, the Commissioner applied a reasonableness standard in concluding that the potential sensitivity of the information caused that purpose to fall short of reasonableness:

> [A] reasonable person would not expect such practice to extend to the "tailoring" of information to the individual's potentially sensitive personal or professional interests, uses of or preferences for certain products and services, and financial status, without the positive consent of the individual.[53]

Similarly, knowledge must inform consent; an organization's description of the purposes for which information will be used must be "sufficiently conducive to [imparting] knowledge on the part of the individual" or the consent that was provided may be invalid.[54] That is, the organization must "**clearly explain** to all [affected individuals] the purposes for the collection, use, and disclosure of their personal information"[55] [emphasis added]. This requirement draws in elements of Principle 2, which deals with the obligation to identify such purposes.[56]

Organizations may not require consent to the collection, use or disclosure of personal information beyond that required to fulfill the "explicitly specified" and "legitimate" purposes.[57] With respect to marketing, the Privacy Commissioner often draws distinctions between so-called primary and secondary purposes. Primary purposes are essential to the service provided, and therefore organizations are permitted to require consent to those purposes as a condition of service.[58] Secondary purposes are inessential (and additional to the primary purposes), and therefore consent cannot be required as a condition of service.[59] Marketing is commonly considered a secondary purpose, although in *Facebook*, demographically-targeted advertisements were considered a primary purpose on the basis that Facebook provided its services for free and depended on those advertisements for most of its revenue.[60]

In sum, the standard for consent is fairly high. In the field of behavioural advertising, it is likely to default to express consent in the context of fulsome knowledge of the organization's purposes. The consent cannot be mandatory, unless the advertising is essential to the service provided. This standard is based, at least in part, on an assessment of whether the notional "reasonable person" would assume that such purposes (and the methods used to pursue them) are likely to be carried out without their knowledge. In the case of targeted advertising based on personal preferences, the Privacy Commissioner of Canada is of the view that reasonable people do not expect that organizations will use their personal information in this way.

---

52. *Aeroplan*, *supra* note 49.
53. *Ibid.*
54. *Ibid.*
55. *Ibid.*
56. *PIPEDA* Schedule 1 clause 4.2.
57. *PIPEDA* Schedule 1 clause 4.3.3.
58. *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.* (16 July 2009), PIPEDA Case Summary #2009-008 at 130, online: OPC <http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm> *[Facebook]. C.f. Chantal Bernier, "Online Behavioral Advertising and Canada's Investigation on Facebook" (Remarks at the Privacy Laws and Business 23rd Annual Conference, Cambridge, UK, 6 July 2010), online: <http://www.priv.gc.ca/speech/2010/sp-d_20100706_cb_e.cfm>.*
59. *Ibid.*
60. *Ibid.*

D. Principles 2, 4 and 5 – Purposes

Organizations must identify the purposes for which they intend to use individuals' personal information no later than the time of collection.[61] They may not use or disclose that information for any other purposes,[62] and they may not collect more information than is necessary for those identified purposes (that is, they may not collect information "indiscriminately").[63] Section 5(3) of the *Act*, referenced above, directly influences the analysis of an organization's stated (or perhaps unstated) purposes. That provision requires that personal information only be collected, used or disclosed "for purposes that a reasonable person would consider are appropriate in the circumstances."[64] As a consequence, *PIPEDA* establishes a system in which organizations' stated purposes define the scope of allowable use, collection and disclosure. Moreover, these purposes may be reviewed on the basis of their reasonableness (or lack thereof).

In assessing reasonableness, the Privacy Commissioner has delineated a four-part test that has been adopted by the Federal Court:

1. Is the measure demonstrably necessary to meet a specific need?

2. Is it likely to be effective in meeting that need?

3. Is the loss of privacy proportional to the benefit gained?

4. Is there a less privacy-invasive way of achieving the same end?[65]

In *Eastmond*, Canadian Pacific Railway had installed security cameras in one of its rail yards. The cameras were installed for the identified purpose of preventing theft and vandalism. The employees' union argued that the resulting surveillance (of employees) was not reasonable. The Federal Court concluded that it was in fact reasonable on the basis that the impact on the employees' privacy was not severe: employees knew which areas were under surveillance, it would only occasionally capture employees' work activities, and, most importantly, CP had put a number of safeguards in place to ensure that the records were not accessible unless an incident was reported. If no incidents were reported, the video would be deleted within 30 hours of its recording, and it could not be used for the purpose of evaluating employee work habits.[66] These safeguards sufficiently mitigated the loss of privacy experienced by the workers to render the surveillance reasonable.

In *Facebook*, the Privacy Commissioner found that Facebook's practice of sharing "potentially unlimited" personal information with application developers without actively monitoring the developers' use of that information was not reasonable in the circumstances. Relevant to the Commissioner's finding was the fact that developers needed much less information than they were given access to, and insufficient safeguards were put in place by Facebook.[67]

---

61. *PIPEDA* Schedule 1 clause 4.2.
62. *PIPEDA* Schedule 1 clause 4.5.
63. *PIPEDA* Schedule 1 clauses 4.4 and 4.4.1.
64. *PIPEDA* s 5(3).
65. *Employee objects to company's use of digital video surveillance cameras,* (23 January 2003), PIPEDA Case Summary #2003-114, online: OPC <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030123_e.cfm>, aff'd *Eastmond v Canadian Pacific Railway*, 2004 FC 852, 2004 CarswellNat 1842 at para 127 [*Eastmond*].
66. *Ibid* at para 176.
67. *Facebook, supra* note 59 at para 193.

The requirement that purposes be identified prior to collection is varied when organizations intend to use previously collected information for a new purpose. In these circumstances, the new purpose must be identified prior to the use of that information.[68] Organizations are still required to obtain consent from each individual in the usual way prior to using their information for a new purpose.[69] In any event, whether the purpose is identified prior to collection or prior to use, organizations are obliged to identify the purpose in such a way that the knowledge requirement of Principle 3 is satisfied by the time consent is obtained.[70]

E. Principle 5 – Retention of Information

Although this Principle has been included in the above discussion, retention is a sufficiently significant issue in the context of behavioural advertising that it deserves to be singled out at this stage. Personal information shall be retained only as long as is necessary for the fulfillment of an organization's identified purposes.[71] When this information is no longer necessary, it should be "destroyed, erased, or made anonymous."[72] The Privacy Commissioner requires that organizations set a maximum period of retention, despite the fact that the *Act* frames it as a suggestion.[73] It may also be necessary to institute a minimum length of retention in order to facilitate access to information that was involved in making a decision about an individual,[74] although it is not necessary to preserve that information in its original form.[75]

In *Credit Bureau*, the Privacy Commissioner considered the imposition of a 20-year retention policy for credit-related information to be sufficient for the purposes of the *Act* in light of the fact that an extended retention period benefitted some individuals, whereas others could still request to have their information disposed of prior to that time.[76] In *Facebook*, the organization had instituted an indefinite retention policy for deactivated accounts. The Privacy Commissioner objected to this arrangement even after Facebook created a process for account deletion, despite Facebook's claims that it was merely safeguarding it for users and did not disclose or use that information during the deactivation period.[77]

F. Principle 9 – Individual Access

Individuals may request from an organization confirmation of the existence, use and disclosure of their personal information as well as access to this information.[78] The *Act* permits exceptions to this rule, but requires that the individual be informed of the reasons for denying access.[79] Those exceptions are codified in s. 9(3), which exempts organizations from providing access where it would "reveal confidential commercial

---

68. *PIPEDA* Schedule 1 clause 4.2.4.
69. *Ibid.*
70. *Englander v Telus Communications Inc*, 2004 FCA 387, 2004 CarswellNat 4119 at para 58 [*Telus]*.
71. *PIPEDA* Schedule 1 clause 4.5.
72. *PIPEDA* Schedule 1 clause 4.5.3.
73. *Credit bureau sets retention period for positive information* (18 January 2006), *PIPEDA* Case Summary #2006-326, online: <http://www.priv.gc.ca/cf-dc/2006/326_20060118_e.cfm> [*Credit Bureau]*.
74. *PIPEDA* Schedule 1 clauses 4.5.2 and 4.5.4.
75. *Vanderbeke v Royal Bank,* 2006 FC 651, 2006 CarswellNat 1550 at para 20.
76. *Credit Bureau, supra* note 74.
77. *Facebook, supra* note 59 at paras 249-254.
78. *PIPEDA* Schedule 1 clause 4.9.
79. *Ibid.*

information"[80] (which refers here to information relating to commerce, and not merely information with commercial value),[81] along with a variety of other public-policy exceptions, such as where access "could reasonably be expected to threaten the life or security of another individual."[82] In addition, organizations are specifically prohibited from providing individuals with access to their personal information if doing so would reveal personal information about a third party.[83] If the third party's information is severable from the record at issue, then the organization should sever it prior to giving the individual access.[84] If the third party consents, then access may be granted without severing.[85]

Where information is inaccurate or incomplete, individuals have a right to challenge the organization's records and have their personal information amended accordingly.[86]

G. Other Principles

Not all Principles are as central to the issue of behavioural advertising as those listed above. Institutional Principles such as Accountability (Principle 1), Openness (Principle 8) and Challenging Compliance (Principle 10), though relevant to any organization subject to the *Act*, do not take on an appreciably different form in the context of behavioural advertising as they are focused primarily on conventional organizational structures. It is sufficient to note that all organizations subject to *PIPEDA* must provide an apparatus that monitors privacy issues, informs individuals of the organization's practices and enables individuals to make complaints under the *Act*. In addition, although personal information must be as "accurate, complete, and up-to-date"[87] as the organization's identified purposes require (Principle 6), this requirement is directed at "objective, verifiable fact", and not subjective matters such as personality profiles.[88] Organizations must also put in place multi-layered safeguards[89] and follow industry best practices to protect individuals' privacy (Principle 7).[90]

III. THE SOCIAL CONTEXT

The legal analysis presented above draws in elements of the surrounding social context by assessing circumstances on the basis of reasonableness, considering the sensitivity of the information at issue and reviewing common practices and industry standards relevant to the issue. These are all questions of fact arising from the surrounding social context. Accordingly, being familiar with how Canadians behave and how they perceive these issues is a critical part of a complete analysis of privacy issues under *PIPEDA*.

---

80. *PIPEDA* s 9(3)(b).
81. *Air Atonabee Ltd v Canada (Minister of Transport)* (1989), 37 Admin LR 245, 27 FTR 194, 27 CPR (3d) 180 at 36 (FC TD) *[Atonabee]*.
82. *PIPEDA* s 9(3)(c).
83. *PIPEDA* s 9(1).
84. *Ibid.*
85. *PIPEDA* s 9(2).
86. *PIPEDA* Schedule 1 clause 4.9. *C.f. PIPEDA* Schedule 1 clause 4.9.5.
87. *PIPEDA* Schedule 1 clause 4.6.
88. *Complaint under PIPEDA against Accusearch Inc., doing business as Abika.com (not dated),* at para 36, online: <*http://www.priv.gc.ca/cf-dc/2009/2009_009_rep_0731_e.cfm*>.
89. *PIPEDA* Schedule 1 clause 4.7.3.
90. *Report of an Investigation into the Security, Collection and Retention of Personal Information (25 September 2007)* at paras 70, 76 and 82, online: *OPC <http://www.priv.gc.ca/cf-dc/2007/TJX_rep_070925_e.cfm> [TJX].*

A. The Internet and Canadian Habits

Canadians are voracious Internet users, with 80% of the Canadian population going online for personal reasons[91] and most of them logging in every day.[92] Thirty-nine percent of Canadians aged 16 or older shop online, collectively placing 95 million orders and spending $15.1 billion.[93] Over a quarter of adult Canadians access educational resources online, as do 80% of students.[94] More than a third of adult Canadians, mostly women, access health-related information online. [95] More than half of these users looked up information on specific diseases or lifestyle information (*e.g.* relating to diet or exercise).[96] Canadians also engage in social, civic and political life online, with half of all home Internet users going online to read about specific social or political issues and 40% of home Internet users researching local community events.[97] In light of the significant portion of Canadians' personal and professional lives spent online, the Privacy Commissioner of Canada has expressed the view that "it is imperative, in our view, that their privacy is protected when engaged in Internet activity."[98]

B. The Public Debate Around Deep Packet Inspection

The debate around deep packet inspection reached a fever pitch during the CRTC's 2009 hearings into ISPs' use of the technology for non-advertising-related, network-maintenance purposes. The Privacy Commissioner of Canada was sensitive to the concerns of the Canadian public (or, at least, vocal parts thereof) and commissioned a collection of essays from interested parties.[99] Many of the essays cited deep reservations about the use of DPI without consent or, worse, without users' knowledge, calling it "spy[ing]",[100] "intrusive",[101] and a violation of the Internet's "presumption of privacy".[102] These deep reservations regarding a technology that the Privacy Commissioner has likened to the steaming-open of sealed letters[103] are indicative of the public's strongly held views about what constitutes a reasonable loss of privacy even in the context of a meritorious purpose (such as maintaining network infrastructure).

---

91. *Canadian Internet Use Survey, supra* note 1.
92. *Ibid.*
93. Statistics Canada, *E-commerce: Shopping on the Internet* (Business Special Surveys and Technology Statistics Division, 2010), online: The Daily <http://www.statcan.gc.ca/daily-quotidien/100927/dq100927a-eng.htm>.
94. Statistics Canada, *Study: Using the Internet for education purposes* (Business Special Surveys and Technology Statistics Division, 2005), online: The Daily <http://www.statcan.gc.ca/daily-quotidien/071030/dq071030b-eng.htm>.
95. Statistics Canada, *Study: Health information and the Internet (Business Special Surveys and Technology Statistics Division, 2005), online: The Daily <http://www.statcan.gc.ca/daily-quotidien/080221/dq080221c-eng.htm>.*
96. *Ibid.*
97. Statistics Canada, *Study: Internet use and social and civic participation* (Business Special Surveys and Technology Statistics Division, 2007), online: The Daily <http://www.statcan.gc.ca/daily-quotidien/081204/dq081204d-eng.htm>.
98. Office of the Privacy Commissioner of Canada, Essay, "Review of the Internet traffic management practices of Internet" (18 February 2009) at para 20, online: OPC <http://dpi.priv.gc.ca/index.php/essays/review-of-the-internet-traffic-management-practices-of-internet-service-providers/>.
99. Office of the Privacy Commissioner, "Collection of Essays" (2009), online: OPC <http://dpi.priv.gc.ca/index.php/essays/>.
100. Office of the Privacy Commissioner, "The Greatest Threat to Privacy" (2009), online: OPC <http://dpi.priv.gc.ca/index.php/essays/the-greatest-threat-to-privacy/>.
101. Office of the Privacy Commissioner, "Just Deliver the Packets" (2009), online: OPC <http://dpi.priv.gc.ca/index.php/essays/just-deliver-the-packets/>.
102. *Ibid.*
103. Office of the Privacy Commissioner, "Objecting to Phorm" (2009), online: OPC <http://dpi.priv.gc.ca/index.php/essays/objecting-to-phorm/>.

This debate is not limited to Canada. In the United States, the Federal Communications Commission ("FCC") has stated that the use of DPI in the context of network maintenance must be disclosed to consumers so as to enable them to reasonably recognize the effects of its use.[104] The House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet opined in 2008 that, due to the "obvious sensitivity" of the information being analyzed by DPI systems, consumers deserved "clear, conspicuous, and constructive notice" of the use of DPI, "meaningful" opt-in consent to that use, and no "monitoring or data interception" (*i.e.* collection) for users who had not opted in.[105] The National Advertising Initiative, an American organization that advocates self-regulation in the advertising industry, has recognized the public's uneasy regard for behavioural advertising with DPI by supporting an opt-in standard for such advertising.[106] The U.K.'s Information Commissioner's Office has taken it a step further by requiring Phorm to supply opt-in consent to all of its customers.[107]

C. The Public Debate Around Tracking Cookies

In many respects, the public debate surrounding tracking cookies has been just as impassioned as that surrounding DPI. Much of the controversy began in the United States, where lawsuits against major firms such as Yahoo, Toys-R-Us and DoubleClick (a targeted advertising firm that has since been acquired by Google) prompted those companies to voluntarily update their privacy policies to create opt-out consent schemes.[108] The FCC continues to endorse this self-regulating model.[109] The EU, however, has put regulations in place requiring opt-in consent for the use of tracking cookies.[110]

In Canada, most companies follow the opt-out approach popular in the United States. There has been evidence of a concerted public will to avoid tracking cookies; estimates of the proportion of users who clear their cookies on a monthly basis range from 39 to 50 percent of users, and 13.2 percent of users block third-party cookies outright.[111] Not all cookies are tracking cookies, however, and clearing all of one's cookies actually degrades some browser functionality. Still, this is a more practical route than opting out from every tracking cookie that a user runs across. Tracking cookies are numerous; Yahoo alone operates 34 advertising networks that use different tracking cookies.[112]

---

104. US, Federal Communications Commission, *Memorandum Opinion and Order In the Matters of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications (20 August 2008), File No EB-08-Ih-1518, WC Docket No 07-52 at 40 and 58, online: <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.doc>.*
105. US, *Markey: Consumers Have Right to Know What Broadband Providers Know About Web Use: Hearing Before the Subcommittee on Telecommunications and the Internet of the House Committee on Energy and Commerce, 110*th Cong (2008) (Rep Edward J Markey), online: <http://markey.house.gov/press-release/july-17-2008-markey-consumers-have-right-know-what-broadband-providers-know-about-web>.
106. "Network Advertising Initiative Affirms Support for Self-Regulation of Companies Using 'Deep Packet Inspection'" *Marketwire* (25 September 2008), online: Marketwire <http://www.marketwire.com/press-release/Network-Advertising-Initiative-903861.html>.
107. Controversy surrounds Phorm, *supra* note 34.
108. Amir M Hormozi, "Cookies and Privacy" *EDPACS* 32:9 (March 2005) 1 at 9.
109. *Ibid* at 11.
110. *Ibid.*
111. Brian Morrissey, "Wary Consumers Ward Off Tracking Cookies" *Adweek 46:31 (8 August 2005) 10.*
112. *Ibid.*

In response to grassroots user demand, some of the Internet's most popular browsers have added a "do not track" feature (suggested by Stanford University researchers)[113] to allow users to pre-emptively opt-out of some or all tracking cookies by simply requesting of sites that they not track them.[114]

Considering this context, it is clear that the public (in Canada and elsewhere) care deeply about the privacy issues arising from both DPI and tracking cookies.

IV. ANALYSIS

As with the above discussion of the legal scheme, each of *PIPEDA*'s Principles will be considered in turn (though some are grouped together for convenience). Due to the substantial overlap between the use of tracking cookies and DPI, many points of the legal analysis can be applied to both in similar fashions. Accordingly, the technologies will be dealt with together for the most part. Where differences in *PIPEDA*'s treatment of the two technologies are likely to arise, they will be discussed independently.

A. Principle 3 – Knowledge and Consent Respecting Collection, Use or Disclosure

Some form of knowledge and consent is clearly required by the *Act* prior to the time of collection (or use, if tracking for advertising purposes is a new use). In this commercial context, it is unlikely that one of the statutory exceptions to the requirement for explicit consent will apply. The largest question for operators of DPI- and tracking-cookie-based advertising networks is whether opt-out consent satisfies the scheme of the *Act*. On the basis of the Privacy Commissioner's previous findings, this is unlikely in all but the most limited behavioural advertising schemes.

i. The Sensitivity of the Personal Information at Issue

Three of the Commissioner's four preconditions for imposing an opt-out scheme are plainly met, leaving only the sensitivity of the personal information at issue. The information in question must be "demonstrably non-sensitive in nature".[115] This imposes a high bar, in part because it places the burden on the organization to demonstrate the non-sensitive nature of the information, but also because the standard of "sensitivity" is so easy to meet. In *Aeroplan*, the Commissioner held that information regarding an individual's "personal or professional interests, uses of or preferences for certain products and services, and financial status" were "potentially sensitive".[116] Clearly, "potentially sensitive" information cannot be "demonstrably non-sensitive", and yet this is precisely the sort of information that any effective behavioural advertising system is intended to collect and use.

Advertisers such as Google and Phorm are careful to state that no "personally identifiable" information is collected. The *Act* does equate anonymization with disposal of data (under

113. *C.f.* Do Not Track: Universal Web Tracking Opt-Out, online: <http://donottrack.us/>.

114. Jared Newman, "Apple Prepares 'Do Not Track' Feature in Safari" *PCWorld* (14 April 2011), online: PCWorld <http://www.pcworld.com/article/225210/apple_prepares_do_not_track_feature_in_safari.html>.

115. *Bank does not obtain the meaningful consent of customers for disclosure of personal information, supra* note 52.

116. *Aeroplan, supra* note 49.

Principle 5),[117] so it could be argued that non-identifiable information ceases to be sensitive, particularly if the reasonable expectations of the individual are the lens through which sensitivity is adjudged. Generally speaking, there are two issues with this view. The first is that supposedly anonymized data, when voluminous, is actually extremely difficult to anonymize effectively. AOL famously released "anonymized" records of the search history of hundreds of thousands of users, in which each user was identified only by a number (much like Google identifies its users). It was not long before the New York Times started attaching faces to numbers, starting with 62-year-old American widow Thelma Arnold of Lilburn, Ga.[118] This demonstrates the unsurprising proposition that an individual's behaviour can be an effective digital fingerprint. The second issue is that, so long as an IP addresses can be attached to the record, the organization saving the information will still be able to associate the information collected with the household from which it originated, if not the specific person. This is a particularly weak form of anonymity.

Accordingly, the information collected is likely sensitive if it is retained in any commercially useful form. This sensitivity is reinforced by the public's apparent expectation that their browsing habits should not be shared without their consent, as evidenced by the recent shift by mainstream browsers and knowledgeable users towards tracking-cookie avoidance. If so much of the public defaults to denying consent and requiring explicit exceptions to allow organizations to track them, it is likely that the "reasonable expectations" standard militates against an opt-out approach to consent. This is reinforced by the fact that personal information is collected as soon as a webpage loads, even before a user is given the chance to opt-out. This is collection before consent, which the *Act* prohibits. As a consequence, *PIPEDA* likely requires opt-in consent for all but the most limited behavioural advertising services. This consent must be accompanied by a clear explanation of the purposes to which individuals are consenting, which could be as simple as enumerating the types of user activities that are tracked and an explanation that they will be analyzed to infer the user's interests for the purposes of advertising.

ii. Can Consent be Mandatory for the Provision of the Service?

Whether the provision of [opt-in] consent may be a mandatory precondition to service depends on the facts. In the case of tracking cookies, users typically browse a site for the purpose of consuming some content or service, as in *Facebook*.[119] The user's browser receives a tracking cookie that is governed by the terms of the privacy policy on that website, even if the cookie is from a third party (such as Google). In cases where the site depends on that advertising to offer its services for free, this may be considered a primary purpose, and thus consent may be mandatory for visiting users. Although it is possible to advertise without behavioural analysis, *Facebook* reflects a willingness to allow sites to protect their primary revenue streams as primary purposes (if those purposes are themselves reasonable, discussed below).

In the case of DPI, however, it is highly unlikely that consent could be a mandatory requirement for service from an ISP. ISPs charge a fee for access to the Internet, and do not depend on advertising to provide a free service. Accordingly, DPI-based behavioural advertising is, like most advertising,[120] a secondary purpose for which consent cannot

117. *PIPEDA* Schedule 1 clause 4.5.

118. Michael Barbaro and Tom Zeller, "A Face Is Exposed for AOL Searcher No. 4417749" *New York Times* (9 August 2006), online: <http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482>.

119. *Facebook, supra* note 59.

120. *Ibid.*

be a mandatory requirement of service. This might change if an ISP chose to offer a free Internet connection on the condition that DPI-based behavioural advertising be built in, but thus far no ISPs have expressed an interest in such a system.

It bears noting, however, that permitting a mandatory consent requirement on most of the web's resources may run afoul of the overarching reasonableness requirement. In a system where all free websites may demand a substantial loss of privacy in order to obtain access, individuals could be left with the choice of surrendering their privacy or surrendering their Internet connections. This ties in to the reasonableness assessment of the purpose itself, below, as it could reduce the benefit to the individual and thus render the purpose for collection, use and disclosure unreasonable.

iii. Case Studies

In light of the above analysis, it is likely that Google is violating *PIPEDA* by providing opt-out (rather than opt-in) consent for its tracking cookie. Google collects personal information across broad regions of the web and, although it does promise to avoid connecting users' identifiers with certain sensitive interests (such as "race, religion, sexual orientation, health, or sensitive financial categories"),[121] it does not avoid all categories that the Privacy Commissioner considers sensitive. Accordingly, it likely fails to meet the criteria for imposing opt-out consent.

Phorm, on the other hand, likely meets its obligations under this Principle of *PIPEDA* by using a system of opt-in consent with appropriate knowledge prior to collection, use or disclosure.

B. Principles 2, 4 and 5 – Purposes

An organization's stated purposes define the scope of their lawful collection, use and disclosure. These purposes must be reasonable, as defined by the Privacy Commissioner's four-part test.[122] Taking the view that an organization adopts behavioural advertising in order to raise revenues, and that many organizations (most notably Google) are highly successful in that pursuit, the first two conditions (necessity and effectiveness) are plainly met. The last condition, that there not be a less privacy-invasive way of achieving the same end, is unlikely to be a serious issue; although it could be argued that organizations could simply charge users directly rather than obtain funding through advertising, the Commissioner declined to dictate radical changes in business models in *Facebook* and is unlikely to start doing so. Accordingly, the crucial consideration is the third.

i. Is the Loss of Privacy Proportional to the Benefit Gained?

This is the question that divides critics of behavioural advertising. Both interests are substantial: The individuals' interest in protecting their privacy online, particularly in light of the sensitivity of the information that behavioural advertising schemes are capable of collecting, is highly compelling. So too is the business model of an entire industry, the Internet, which runs on ads. This latter interest is weakened by the fact that the benefit is merely *increased* revenue, and not the ability to earn revenue *per se* (after all, organizations can always display non-behavioural advertisements). Nevertheless, the commercial interest is not insignificant. Some industry representatives are quick to note that users also derive an indirect benefit in the form of free content and more relevant ads.[123]

---

121. Google Privacy Center, *supra* note 5.
122. *Eastmond, supra* note 66.
123. Wary Consumers Ward Off Tracking Cookies, *supra* note 112.

Relevant to this balancing of interests is a consideration of the sensitivity of the information, the safeguards in place,[124] the organization's retention policy, individuals' actual knowledge of the loss of privacy, and the scope of the collection.[125] With both tracking cookies and DPI, the scope of collection is extremely large, so organizations hoping to satisfy *PIPEDA* will need to offset that extensive collection by tightening up the other factors to reduce the degree of privacy loss experienced by individuals.

Arguably, the most significant factor in favour of proportionality is fulsome, meaningful consent obtained through an opt-in scheme. Unlike *Eastmond*, where employees had no say in the matter,[126] users may choose whether to participate and, should they choose to opt-in, they enter the program with full knowledge of their loss of privacy. This consent, along with a robust, multi-level set of safeguards (including encryption and secure storage facilities), a collection policy that avoids collecting the most sensitive types of personal information and a retention policy that emphasizes speedy deletion, may be sufficient to render this purpose reasonable. Note that the imposition of mandatory consent (discussed above) may negatively impact this reasonableness assessment; it is far less likely that a reasonable person would consider such a system appropriate in the circumstances.

As DPI has a greater scope of disclosure, organizations employing DPI-based behavioural advertising will likely need to take the strictest steps to reduce the loss of privacy. In addition to the features mentioned above, such organizations may need to institute an aggressively limited retention policy, where all personal information that is collected is immediately aggregated into interest categories and then deleted, leaving only the aggregate data behind. This is a necessary consequence of such broad collection; even short-term retention can pose serious privacy risks when the data being retained is so voluminous. Similarly, such organizations need to be incredibly delicate in selecting the information that gets aggregated – having access to literally everything that an individual does online makes it necessary to only pick out the least sensitive information available. It is not enough that such organizations avoid serving ads based on a user's financial information, health records, political interests and the like; organizations that take it upon themselves to sift through a person's entire digital life should be careful never to learn these things in the first place.

This places these organizations in a fairly restricted position, as the Privacy Commissioner recognizes broad (and, to some, apparently innocuous) classes of information as "sensitive", leaving a fairly limited class of data eligible for collection without requiring stronger privacy protections than they presently implement. But this is the result of casting a wide net; organizations must normally justify every piece of information that they collect (indiscriminate collection being expressly forbidden),[127] so it is not surprising that a technology that is designed to collect everything will have comparatively onerous restrictions imposed upon it.

ii. Case Studies

Both Google and Phorm have pledged to enforce powerful safeguards. Both companies attempt to avoid associating sensitive interest categories with users' identifiers, although their conceptions of "sensitive information" are far more limited than that of the Privacy Commissioner.

---

124. *Facebook, supra* note 59 at para 193.
125. *Eastmond, supra* note 66.
126. *Ibid.*
127. *PIPEDA* Schedule 1 clause 4.4.1.

Google's AdSense is capable of indefinite retention of user interest categories (despite its two-year rolling deletion policy), but only if users are consistently interacting with the system and, as a consequence, interacting with that information. Google collects data from numerous partner websites and retains most of the information it collects, such as browser history and IP addresses, for a period of 18 months prior to anonymization. This pattern of retention is troubling, particularly in light of the *Facebook* decision, which casts suspicion on indefinite retention of personal information. It also lacks an opt-in consent process to mitigate the severity of the privacy loss. However, Google claims to strike a balance between legitimate interests – privacy and security. As in *Credit Bureau*, this may go a long way towards establishing reasonableness (at least with respect to retention). The aggregate interest category information that is indefinitely retained may be sensitive, but it is less sensitive than the browsing history that Google eventually anonymizes, and it likely is the minimal amount of information necessary to provide behaviourally-targeted ads.

Google appears to be treading a thin line when it comes to balancing individuals' privacy interests against the benefits gained. Google anonymizes the most sensitive personal information after 18 months, an apparently reasonable period of time, and retains user interest information for the duration of its use plus two years. This policy satisfied the Commissioner in *Facebook*, but the scope of collection (and thus loss of privacy) in this case is considerably broader. Despite this, Google's balancing appears to be largely reasonable, and thus its purposes are likely *PIPEDA*-compliant. Such a finding is not guaranteed, however; revising its retention policy to store less information for less time or instituting an opt-in consent process would dramatically improve the likelihood that Google's purposes would be found to be in line with *PIPEDA*.

Phorm, in contrast, retains nothing but users' aggregated interest categories and their unique identifiers. The only issues that can be taken with Phorm's approach is that Phorm's definition of sensitive information is much narrower than the Privacy Commissioner's, and it stores users' interest categories indefinitely. This concern is likely resolved by Phorm's opt-in consent scheme, which reduces the severity of privacy loss resulting from the collection, use and retention of sensitive information. Overall, Phorm likely satisfies these Principles of *PIPEDA*.

C. Principle 9 – Individual Access

Access to personal information is a particularly problematic aspect of these technologies. Multiple individuals may contribute personal information to a single identifier, simply by virtue of using the same browser on the same computer (as is common in family homes). As a consequence, it is likely that providing an individual access to his or her personal information would reveal the personal information of a third party that cannot be severed. Worse, if a third party gains access to an individual's computer account they would be able to view the interest categories associated with it even if none of the personal information collected was theirs. To get around this, an individual would have to be able to demonstrate that he or she was the originator of the personal information associated with a particular identifier, and either demonstrate that no other individual had used the same browser on the same computer (or, at least, that such an occurrence was unlikely) or obtain consent from all individuals who were likely to have access to the computer in order to gain access to the personal information. In view of the practical difficulties that arise, the most effective route to ensure *PIPEDA*-compliance is to deny access entirely (absent convincing proof of the above requirements). This is not the only solution; in theory, organizations could allow users to authenticate their identities before browsing, but requiring users to log in to the service is precisely what most behavioural advertisers want to avoid.

Google and Phorm both allow users to view and edit their user preferences by visiting a particular webpage in their browser. The page recognizes the browser and provides access to the associated user interests. Although this functionality is likely provided in an attempt to satisfy access requirements, in many cases it may actually allow individuals to view the personal information of third parties. In order to be compliant with *PIPEDA*, Google and Phorm should either deny access to these records entirely or establish some mechanism by which users can authenticate their identities.

CONCLUSION

PIPEDA anticipates the need for a delicate balance between individuals' reasonable expectation of privacy and organizations' legitimate business interests. In general, it does not aim to prevent consumers from trading their privacy for commercial benefits, but it does demand that individuals obtain fulsome knowledge of the arrangements that they are entering, that the consent they provide be meaningful and that the arrangements themselves strike a reasonable balance between the privacy lost and the benefit gained. Behavioural advertising technologies test this balance by being pervasive, surreptitious and highly invasive by nature. The *Act* is intended to guide organizations through these untested waters by providing a baseline of protection appropriate to the circumstances.

Under *PIPEDA*, users should consent to both tracking cookies and deep packet inspection via an opt-in process due to the sensitive information that these technologies collect and use. Using these technologies for the purpose of targeted, behavioural advertising is not unreasonable *per se*, but failing to adopt stringent retention policies that reduce the amount of information stored and limited collection policies that avoid collecting the most sensitive classes of information may render it unreasonable. Limiting retention is also critical, in addition to the institutional and physical protections that all organizations handling sensitive information should take. Finally, as these technologies cannot distinguish between one individual and another if they are using the same browser, access to personal information should be limited to cases where it can be demonstrated that the only person who has contributed the personal information attached to a particular identifier is the person requesting it (or that all other contributing individuals have consented to the access).

On the basis of the above, I have concluded that Google may be violating *PIPEDA* due to its reliance on opt-out consent despite its collection of sensitive personal information, and its practice of permitting users to access personal information without demonstrating that the personal information of third parties is not likely to be disclosed without their consent. I recommend that Google adopt an opt-in consent process and either deny individuals access to personal information or put in place a process that enables them to authenticate their identities in a manner that satisfies the *Act*. It may also be appropriate for Google to limit its retention and collection of personal information more aggressively (particularly with respect to highly sensitive classes of information), although its current practices likely do not violate the *Act*.

I have also concluded that Phorm may be violating *PIPEDA* (or would be, if it performed business in Canada) on the basis that it too is permitting users to access personal information without demonstrating that the personal information of third parties is not likely to be disclosed without their consent. I recommend that it either deny individuals access to personal information or put in place a process that enables them to authenticate their identities in a manner that satisfies the *Act*.