A “Do Not Track List” for Canada?

Written By: Janet Lo
Public Interest Advocacy Centre
1204 - ONE Nicholas St.
Ottawa, Ontario
K1N 7B7

October 2009

With Funding from Industry Canada

The Public Interest Advocacy Centre
(PIAC)
Suite 1204
ONE Nicholas Street
Ottawa, ON
K1N 7B7
Tel: (613) 562-4002 Fax: (613) 562-0007

E-mail: piac@piac.ca Website: www.piac.ca

Canadian Cataloguing and Publication Data

Lo, Janet

A “Do Not Track List” for Canada?

1-895060-92-3

Acknowledgement

Financial support from Industry Canada to conduct the research on which this report is based is gratefully acknowledged. The views expressed in this report are not necessarily those of Industry Canada or of the Government of Canada.

Additional research for this report was provided by Michelle Kelly & Kathryn Bortolussi.

The author would also like to thank John Lawford for his support and guidance in the writing of this report.

EXECUTIVE SUMMARY

This report examines online behavioral targeted advertising and online behavioral tracking, the practice of tracking consumers' online activities to target advertising to individual consumers based on their online history, preferences and attributes. Marketers and businesses suggest that targeted advertising would benefit consumers in the form of more relevant advertisements and offers tailored to their interests and needs. Consumer advocates have voiced several concerns with the practice of online tracking, from privacy invasion and data collection practices to concerns with discriminatory advertisements and the potential to target vulnerable consumers. However, it has been difficult for consumers to voice their concerns with behavioural targeted advertising practices, as industry practices have often been conducted covertly with little or vague notice to consumers hidden in privacy policies or terms of use. As online behavioural targeted advertising becomes the ubiquitous industry standard, consumers are at the mercy of online advertisers with few options to control how their personal information is collected, used, disclosed and retained.

This report is informed by a survey designed by PIAC and conducted by Environics which examines consumer awareness and attitudes towards online tracking and behavioural advertising, with specific questions about a potential "Do Not Track List" in Canada. This paper concludes that consumers are not aware of consumer surveillance on the internet and technical tools used by companies to track their behaviour online. Futhermore, consumers are not aware of the extent to which their personal information is collected and used to serve behaviourally targeted advertising to appeal to their consumer profile.

Consumers want the ability to control their personal information online – not only when and how it is collected, but also how it is used and shared with other parties. Consumer consent is only meaningful when proper notice is present, thus transparency in online behavioural targeted advertising practices is very important. In order to obtain informed consent to their practices, websites must clearly and openly notify their users of the tracking tools used by their websites and affiliates to track their behaviours online.

Consumer education through proper notice is only part of the solution. At the moment, there is a great power imbalance between the online advertising industry and consumers, as online behavioural targeted marketing has become the norm and industry standard without any oversight by regulatory bodies. These practices have evolved without proper consideration to protect consumer autonomy and privacy and only with the goal of advertising revenues in mind.

Canadian consumers surveyed by PIAC expressed discomfort with online tracking for the purpose of targeted and behavioural advertising. The majority of survey respondents supported the creation of a "Do Not Track List," which would be a service

wherein consumers who sign up for the list would not have information about their online activities collected, used or disclosed. However, it would be very difficult to design and deploy a "Do Not Track List" without assigning users a unique identifier. Furthermore, efforts to establish a "Do Not Track List" would face opposition and lobbying by industry to create loopholes and exceptions for businesses. Implementing a "Do Not Track List" in Canada would give Canadian consumers better control over their personal information while they surf the internet. However, while a "Do Not Track List" would certainly be a step to better protection for consumers from online tracking, it cannot be expected to provide holistic or foolproof consumer protection, especially given the logistical and technical barriers to effective implementation.

The report makes several recommendations, including a requirement for consumer opt-in consent to online tracking and behavioural targeted advertising. Greater transparency and consumer education are needed for tracking technologies and behavioural targeted advertising practices on the internet. Canadian legislators and regulators should begin studying the issue of online behavioural targeted advertising to catch up to American and European regulators, who have already begun considering how their regulatory frameworks protect their consumers on the internet. The Privacy Commissioner should review the existing *Personal Information Protection and Electronic Documents Act* to set out guidelines for how website operators can deploy behavioural advertisement technology in order to comply with the law and protect the privacy of Canadians. The Government should review existing privacy legislation and regulatory framework and bring forward new rules as necessary to ensure that these systems only operate on an explicit, informed, opt-in basis and that an effective enforcement mechanism with fines exists to punish marketers who operate outside the rules. Special consideration must also be given to the issue of behavioural advertising targeting children and young people.

While a "Do Not Track List" would likely encounter considerable industry objection and operational and technical barriers, regulators are in a position to set down clear guidelines for online behavioural targeted advertising practices. Given the prevalence of personal information collection, use and disclosure for the purposes of behavioural targeted advertising on the internet, only clear, enforceable rules can make a significant impact to protect consumers from unwanted online surveillance and behavioural targeted advertisements. The extent of online behavioural targeted advertising and consumer tracking on the internet is troubling, and better privacy and data protection must be afforded to consumers while they conduct everyday activities on the internet.

Detailed Table of Contents

INTRODUCTION

> *"Behavioural targeted marketing is marketing based on the study of behaviours, preferences and decisions we all express while acting in the role of consumers."*[1]

In Daniel Solove's book, *The Digital Person*, he argues that the collection and use of personal information in databases present a different set of problems than government surveillance.[2] To demonstrate the problem, he uses the metaphor of Franz Kafka's *The Trial*, in which a bureaucracy with inscrutable purposes uses people's information to make important decisions about them, while denying these people the ability to participate in how their information is being used. Solove states that this problem is derived from information processing – that is, the storage, use and analysis of data – rather than simply just with information collection.[3] This sort of information processing affects power relationships between people and the institutions of the modern state, frustrating the individual by creating a sense of helplessness and powerlessness and affecting social structure by altering the kinds of relationships people have with the institutions that make important decisions about their lives.

This report examines online behavioral targeted advertising and online behavioral tracking, the practice of tracking consumers' online activities to target advertising to individual consumers based on their online history, preferences and attributes. Marketers and businesses suggest that targeted advertising would benefit consumers in the form of more relevant advertisements and offers tailored to their interests and needs. Consumer advocates have voiced several concerns with the practice of online tracking, from privacy invasion and data collection practices to concerns with discriminatory advertisements and the potential to target vulnerable consumers. However, it has been difficult for consumers to voice their concerns with behavioural targeted advertising practices, as industry practices have often been conducted covertly with little or vague notice to consumers hidden in privacy policies or terms of use. As online behavioural targeted advertising is ubiquitous and is quickly becoming the industry standard, consumers are at the mercy of online advertisers with few options to control how their personal information is collected, used, disclosed and retained.

The methodology of this report relies on a survey designed by PIAC and conducted by Environics which examines consumer awareness and attitudes towards online tracking and behavioural advertising, with specific questions about a potential "Do Not Track List" in Canada. Part I of this report discusses PIAC's survey findings and compares these findings to similar surveys conducted in the United States examining American

---

[1] Canadian Internet Policy and Public Interest Clinic, "Online Privacy Threats: A Review and Analysis of Current Threats" (Fall 2008), online: http://www.cippic.ca/uploads/publications/CIPPIC-Online_Privacy_Threats-Final.pdf.

[2] Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, NYU Press (2004).

[3] Daniel J. Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," 44 San Diego Law Review 745 (2007), online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565&rec=1&srcabs=930514.

consumers attitudes towards online tracking. Part II traces the evolution of the traditional advertising and marketing industries in the internet age.

Part III of this report describes various techniques and technologies used to track consumers online and serve behaviourally targeted advertising, from cookies to search advertising to deep packet inspection to social networking sites. In Part IV, we examine the benefits and harms of online tracking and analyze the privacy and social concerns with behavioural advertising.

Recently, consumer groups in the United States have called upon their regulators for a "Do Not Track List" to provide consumers with control over their online and corporately held digital profiles. The goal of the "Do Not Track List" is to ensure that users are not unduly inconvenienced or harassed by marketing messages delivered to their computers and mobile devices. Part V of this report examines the "Do Not Track List" proposal and similar initiatives by consumer groups, regulators and politicians in the United States.

As will be seen, American regulators and politicians have spent considerably more time than their Canadian counterparts examining the issue of online tracking and online behavioural targeted advertising. Part VI examines the desirability and feasibility of a "Do Not Track List" in Canada by considering how current Canadian laws and regulations would apply to protect Canadian consumers. Using the comments of academic and industry experts, the barriers to implementing a "Do Not Track List" in Canada are identified and discussed. This report closes by providing recommendations on the issue of online behavioural targeted advertising for Canadian regulators and the possibility of a "Do Not Track List" in Canada.

PART 1: CONSUMER ATTITUDES TO ONLINE TARGETED ADVERTISING AND ONLINE TRACKING

1.1. PIAC's survey of consumer attitudes

1.1.1. Research methodology

PIAC constructed a survey to examine consumer knowledge of online behavioural targeting practices and attitudes to behavioural marketing and a "Do Not Track List" in Canada. The survey was conducted by research firm Environics. The survey was conducted with 1,570 Canadians aged 18 and over who had internet access between April 1 and April 8, 2009. The margin of error is plus or minus 2.5%, 19 times out of 20.

Survey respondents were representative of gender, age, family income, education, language, employment, regional, and community size demographics across Canada.

1.1.2. Key findings

In our survey, we asked a range of questions to gauge consumer comfort levels with online behavioural targeted advertising and whether Canadian consumers believe a "Do Not Track List" would be desirable.

The first question asked respondents to identify their level of familiarity with the existence of tracking devices and techniques such as persistent cookies and web beacons. Overall, the response was varied, with 20% of total respondents very familiar, 30% of respondents somewhat familiar, 19% not very familiar, and 31% not at all familiar with the technologies. Further analyses of the demographic categories revealed trends that certain groups were less familiar with the tracking technologies. For example, as family income decreased, a higher percentage of respondents stated that they were not very familiar or not at all familiar with tracking technologies.[4] Similarly, as education level decreased or age increased, respondents were less familiar with

[4] Respondents with a family income of $80,000 or more were more familiar with tracking technologies – with 22% stating they were very familiar and 35% stating they were somewhat familiar, compared to 19% not very familiar and 24% not at all familiar. 54% of respondents with a family income of $40,000 to $80,000 stated they were not very familiar (20%) or not at all familiar (34%) with tracking technologies, compared to 52% of respondents with a family income of $20,000 to $40,000 (23% not very familiar, 29% not at all familiar) and 61% of respondents with a family income of less than $20,000 (19% not very familiar, 42% at all familiar).

tracking technologies.[5] As well, males were generally more familiar with tracking technologies than females.[6]

Canadian consumers generally expressed discomfort with online tracking for the purpose of targeted and behavioural advertising, with only 8% of consumers very comfortable and 17% of consumers somewhat comfortable with tracking-based advertising. Consumers were either not very comfortable (25%) or not at all comfortable (49%). Even more consumers expressed discomfort with companies and organizations that share information about their behaviours as consumers with third party organizations for the purpose of targeting advertising (25% not very comfortable, and 53% not at all comfortable).

Our survey suggests that consumers are more comfortable with online tracking for the purpose of customer service or advertising by a company or organization they have prior dealings with. The majority of consumers were most likely to consent to use of information about their internet activities for customer service purposes by a company or organization that they deal with (47%). A minority of consumers are most likely to consent to the use of information about their internet activities for targeted advertising by a company or organization that they deal with (22%). Few consumers were likely to consent to the use of information about their internet activities for market research studies by companies or organizations they have not dealt with (11%) or targeted advertising by companies or organizations they had not previously dealt with (6%).

Consumers were more comfortable with online tracking and targeted advertising by companies and organizations with websites that they regularly visit (41%) compared to government (28%). Very few consumers were more comfortable with online tracking and targeted advertising by market researchers and data brokers (9%).

Finally, we asked a series of questions to gauge consumer desirability for a "Do Not Track List" in Canada. As explained in the survey, consumers who choose to sign up for the "Do Not Track List" would not have information about their online activities collected, used or disclosed. The majority of respondents (54%) strongly supported the creation of a "Do Not Track List", and an additional 27% of respondents somewhat supported a "Do Not Track List", compared to 8% who somewhat opposed and 10% who strongly opposed the List. As well, a majority of respondents indicated that they

[5] 40% of respondents with a university degree stated they were not very familiar (19%) or not at all familiar (21%) with tracking technologies, compared to 46% of respondents with some university education (16% not very familiar, 30% not at all familiar), 51% of respondents with community college education (17% not very familiar, 34% not at all familiar), 65% of respondents who completed high school (24% not very familiar, 41% not at all familiar), and 65% of respondents with less than high school education (19% not very familiar, 46% not at all familiar). Of the respondents between the age of 18 to 29, 49% stated that they were not very familiar (26%) or not familiar at all (23%) with tracking technologies, compared to 44% of respondents aged 30 to 44 (19% not very familiar, 25% not at all familiar), 53% of respondents aged 45 to 59 (15% not very familiar, 38% not familiar at all) and 58% of respondents over 60 years old (17% not very familiar, 41% not familiar at all).

[6] 16% of male respondents were not very familiar and 25% of male respondents were not at all familiar with tracking technologies. 22% of female respondents were not very familiar and 37% of female respondents were not familiar at all with tracking technologies.

would either definitely (33%) or probably (37%) sign up for a national “Do Not Call List”, compared to 17% of respondents who would probably not sign up and 12% of respondents who would definitely not sign up.

Most respondents wanted the ability to specify exceptions for specific companies or organizations on a “Do Not Track List” (58%). More convincingly, the majority of respondents (75%) preferred an “opt-in” consent model whereby websites would not be allowed to track them unless they checked the box, compared to 19% of respondents who preferred an “opt-out” consent model whereby websites would be allowed to track their online activities until they checked the box, and 4% of respondents selected neither model, as there should be no tracking at all.

Finally, respondents were split regarding who should bear the most responsibility for the costs of creating and maintaining a national “Do Not Track List”. 39% of the respondents thought that the online marketers, data brokers, and other groups who track behavior should bear the most responsibility of the associated costs, compared to 21% of respondents who believed that the federal government should bear the cost and 20% of respondents who believed that internet service providers should bear the cost. A smaller percentage of respondents (16%) believed that consumers who signed up for the “Do Not Track” list should bear the responsibility for the associated costs of creating and maintaining the list.

To summarize, about half of Canadian consumers are aware of online tracking technologies and most consumers are uncomfortable with behavioural targeting advertising practices. Most consumers are concerned enough with their privacy that they would support the creation of a national “Do Not Track List” that would prevent websites and online marketers from collecting, using and disclosing their online activities. A majority of Canadians would sign up for the service.

To see the full survey and the results that were collected, please see Appendix A.

1.1.3. Survey limitations

PIAC’s survey provides a good starting point for understanding consumer attitudes regarding the desirability and feasibility of a “Do Not Track List” in Canada. However, PIAC’s questions asking consumers to gauge their familiarity with tracking technologies required each respondent to self-evaluate their own personal knowledge about the internet. The survey results suggest that consumers believe that they are aware of these technologies.

As well, PIAC’s survey asks consumers whether they would support the concept of a “Do Not Track List” without explaining how such a list would actually work. Given Canada’s track record with the implementation of the “Do Not Call List” in 2008, a “Do Not Track List” would need to overcome the operational barriers of the “Do Not Call List” and gain credibility in the eyes of Canadian consumers.

1.2. American surveys of consumer attitudes to online tracking

1.2.1. TRUSTe surveys

TRUSTe is a privacy program founded by the Electronic Frontier Foundation and the CommerceNet Consortium in the United States to act as an independent, unbiased trust entity helping consumers and businesses identify trustworthy online organizations through its Web Privacy Seal, Email Privacy Seal and Trusted Download Programs trademarks. TRUSTe also resolves individual privacy disputes between internet users and websites and often undertakes surveys to gauge consumer trust in privacy issues on the internet.

In 2008, TRUSTe revealed the results of a study regarding American internet users' knowledge, attitudes and concerns about behavioural targeting and online privacy. The survey revealed that 71% of respondents were aware that their browsing information might be collected by a third party for advertising purposes but only 40% were familiar with the term "behavioural targeting." Furthermore, 57% of respondents stated that they were not comfortable with advertisers using their browsing history to serve relevant ads, even when the information could not be connected to their name or any other personal information. The survey also found that 42% of consumers would sign up for an online registry to ensure that advertisers were not able to track browsing behaviours, even if it meant that they would receive ads that were less relevant to their interests.[7]

In March 2009, TRUSTe published the results of another online survey examining consumer attitudes about behavioural targeting. The survey found that most consumers know that their behaviour is being targeted (68%) and re-gauged consumer familiarity with the term "behavioural targeting" (43%). As well, 50% of respondents stated that they were uncomfortable with being tracked by advertisers to be served relevant ads, even with the assurance of anonymity. Most individuals favoured tools and features to control targeted advertising. Notably, the 2009 TRUSTe survey found that consumer discomfort with tracking declined by six percentage points, suggesting that although American consumers worry about protecting their personal data online, they are getting used to behavioural targeting.[8]

---

[7] TRUSTe, "TRUSTe Report Reveals Consumer Awareness and Attitudes About Behavioral Targeting: Consumers indicate a high level of awareness that tracking and targeting occur" (March 26, 2008), online: http://www.truste.org/about/press_release/03_26_08.php.

[8] TRUSTe, "2009 Study: Consumer Attitudes About Behavioral Targeting" (4 March 2009), research independently conducted by TNS.

1.2.2. Americans reject tailored advertising

A new September 2009 survey supported by the Rose Foundation for Communities and the Environment and the Annenberg School for Communication found that most adult Americans (66%) do not want marketers to tailor advertisements to their interests.[9] As well, after being informed about the common methods that marketers use to gather data to tailor ads, a higher percentage of respondents (between 73% and 86%) stated that they did not want tailored advertising. Even among younger adults between the ages of 18 to 24, 55% of respondents stated that they did not want tailored advertising. The study also found that a majority of Americans did not want discounts or news fashioned specially for them.

As well, the survey found that Americans want openness with marketers so that individuals can learn how their information is being collected and used and exercise control over their data. To demonstrate this point, 69% of Americans felt that there should be a law that gives people the right to know everything that a website knows about them. As well, 92% of respondents agreed that there should be a law requiring websites and advertising companies to delete all stored information about an individual if requested to do so. Finally, 63% of respondents agreed that advertisers should be required to immediately delete information about their internet activity.

1.2.3. Other American surveys on collection of personal information and profiling

There is evidence from a number of other studies conducted in the United States to demonstrate that users are concerned about the collection of personal information by websites and behavioural profiling. Several of these surveys are discussed in a 2009 UC Berkeley, School of Information report called "KnowPrivacy":

> A Consumer Reports poll found that '72 percent are concerned that their online behaviors were being tracked and profiled by companies' and '54 percent are uncomfortable with third parties collecting information about their online behavior' [Consumers Union, 2008].
>
> A Harris Poll found that 'a six in ten majority (59%) are not comfortable when websites like Google, Yahoo! And Microsoft (MSN) use information about a person's online activity to tailor advertisements or content based on a person's hobbies or interests' [Harris Interactive, 2008]. …
>
> Surveys from academic research also show high levels of concern. Papers from the Annenberg Public Policy Center suggest an increase in concern: in 2003, '70% of respondents agreed or agreed strongly with the statement that, "I am nervous about websites having information about me,"' and 'in 2005, the

[9] Joseph Turow et al., "Americans Reject Tailored Advertising and Three Activities that Enable It" (29 September 2009), online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

> same response was reported by 79% of respondents' [Turow, et al., 2006].
>
> The Pew Internet and American Life Project asked participants the following question: 'if an Internet company did track the pages you went to while online, do you think that would be…helpful because the company can provide you with information that matches your interests or harmful because it invades your privacy?' This question is interesting, as tracking could be both helpful and harmful. When asked to choose between the two words the majority of users said tracking was harmful, though a few insisted it was either both or neither: 27% Helpful, 54% Harmful, 11% Both (vol.), 4% Neither (vol.), 4% Don't know/Refused [Pew, 2000].[10]

Despite the varied wording of the questions, the numbers from these United States surveys reflect the main finding of PIAC's survey: the majority of consumers are not comfortable with the concept of online tracking for the purpose of serving more relevant, targeted advertising. Also of note, some American surveys were repeated after a couple years and the results demonstrate that more consumers are concerned with the collection of information by websites.

The UC Berkeley study also summarized American survey findings with respect to users' desire to have control over how their information is collected and for what purposes it may be used:

> These surveys also show that users wish to have greater control over how their information is collected and for what purposes it may be used. The Pew Internet & American Life Project asked survey participants about the importance of 'controlling who has access to your personal information.' 85% responded that it was very important and 9% said that it was somewhat important [Pew, 2006].
>
> The Consumer Reports poll found that '93 percent of Americans think internet companies should always ask for permission before using personal information,' and '72 percent want the right to opt out when companies track their online behavior' [Consumers Union, 2008].[11]

These findings parallel PIAC's survey results finding that most Canadian consumers prefer an opt-in model for online tracking, whereby websites would not be allowed to track their behaviours unless they checked the box. Consumers want greater control over the collection and use of their personal information.

---

[10] Joshua Gomez et al., "KnowPrivacy" UC Berkeley, School of Information (1 June 2009), online: http://www.knowprivacy.org at p. 17.

[11] *Ibid.* at pp. 17-18.

Finally, the UC Berkeley study summarized American survey results concerning user awareness about data collection:

> Despite concerns about data collection and profiling, the surveys revealed a large level of ignorance on the part of users about how data is collected. The Consumer's Report poll found that '61% are confident that what they do online is private and not shared without their permission,' and '57% incorrectly believe that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations' [Consumers Union, 2008].
>
> In 2003, the Annenberg surveys found that 57% of the survey participants agreed with the false statement 'when a website has a privacy policy, I know that the site will not share my information with other websites or companies.' Two years later 59% said the same statement was true [Turow, et al., 2006].[12]

Comparing these results with PIAC's survey, it appears that consumers are split as to whether they believe themselves to be familiar with online tracking devices and techniques, however with more probing questions examining consumers' understanding of privacy practices and policies, it is revealed that most consumers misunderstand the extent to which their privacy is protected on the internet. Stated differently, online business privacy practices are not in line with consumer expectations.

[12] *Ibid.* at p. 18.

PART 2: FROM TRADITIONAL ADVERTISING TO ONLINE TARGETED ADVERTISING

Traditionally, marketers relied on segmentation that involved placing consumers in various pigeonholes with labels such as age, social class, frequency of product use, and income in order to make general assumptions about their spending patterns and behaviours. Qualitative researchers and advertising planners would use segmentation and the way in which consumers switch between different pigeonholes to identify marketing opportunities and give advanced warning of any significant changes in consumer behaviour.[13] According to Dr. David Lewis and Darren Bridger, the backbone of segmentation methods consists of "measures of statistical differences between members of a population, such as occupation, education, sex, ethnic background, size of family, postal or zip code."[14] This type of information can help advertisers locate and predict the size of markets for many products, ranging from home mortgages to brooms and can openers.

Aware that demographics alone could not give marketers the feel for either individuals or lifestyles, market researchers developed a more sophisticated technique of analysis and categorization called "psychographics" in the 1970s. This method involved creating psychological profiles of consumers within groups first segmented using standard demographics. Consumers would then be analyzed according to their interests, lifestyles, attitudes and aspirations in order to find those who share a similar profile.[15] The process of slotting consumers into boxes was a major preoccupation of market researchers in order to develop various systems of psychographics. An article in the trade journal *Admap* pointed out that: "[m]ost such pigeonholes are arbitrary, as often interrupting a continuum in, say, status or behaviour as marking off a real watershed between inherently dissimilar groups."[16]

The mass market can be disintegrated by splitting the market into smaller and smaller niches, some of which may comprise a single consumer, within which individual buying habits are unique and personal. With the advance of computing technology, marketers quickly recognized that the future of segmentation was contained in the data already collected in organizations' computer systems. As marketing expert Keith McNamara claimed: "[t]he historic data of who buys individual products is the key to creating models that predict future behaviour."[17] Market researchers have mostly agreed that segmentation of consumers into buying groups is no longer realistic or effective: marketers now have the means to "[identify] ... individual consumers by gathering and analyzing sufficient data on their patterns of consumption and lifestyles to identify something as unique and as personal as their fingerprint – their tastespace."[18] Lewis

---

13 David Lewis & Darren Bridger, *The Soul of the New Consumer: Authenticity, What We Buy and Why in the New Economy*, Nicholas Brealey Publishing, London (2000) at p. 73.

14 *Ibid.* at p. 74.

15 *Ibid.* at pp. 76-77.

16 *Ibid.* at p. 78.

17 Keith McNamara, ICL internal white paper (1998) cited in Lewis & Bridger, *supra* note 14 at p. 79.

18 Lewis & Bridger, *supra* note 14 at p. 80.

and Bridger further explain: "[b]y means of a technique called data mining, huge quantities of information can be analyzed, abstracting personal preferences, identifying individual choices and creating tastespace charts for every single consumer."[19]

With the advance of the internet and electronic commerce, online advertising provides enormous opportunities for advertisers and firms that provide the tools and technologies that support online advertising. For advertisers, internet marketing allows them to focus their pitch to an audience that is most likely to buy their products or subscribe to their services. A number of market research firms study consumer behaviour and usage patterns on the internet. Companies developing the software to enable online targeted marketing have the incentive of potential revenues as more advertising dollars migrate to the internet every year.

Online advertising is big business. Internet advertising was barely visible in 1996, bringing in $267 million but tripling to $907 million in 1997 and reaching nearly $3 billion in 1999.[20] The internet's share of total media ad spending is rising by at least 1 percentage point every year in the United States.[21] The Interactive Advertising Bureau of Canada reported that in 2006, Canadian online advertising revenues amounted to $1.01 billion dollars, an 80% increase over the 2005 figures.[22]

Computers can compile massive amounts of information about consumers, especially in a data-rich environment that lends itself to tracking user movement. For example, a more simplistic online consumer tracking mechanism such as an HTTP cookie can authenticate, track and maintain specific information about a website's users such as their website preferences, other websites the user has visited and the contents of their online shopping carts. More sophisticated consumer tracking mechanisms have also been developed, such as web beacons and deep packet inspection, which will be discussed later in this report. These sophisticated technologies can deliver more personalized content and services to customers with the aim of establishing stronger relationships and cementing customer loyalties.

These technologies are the new business products of a fast growing industry of several companies that specialize in combining commercial databases and publicly available databanks (a process called "data mining") to create very specific data about internet use patterns which can predict the online consumer behaviour of individual customers with surprising accuracy.[23] eMarketer, a research and analysis firm on digital marketing and media, describes behavioural targeting on the internet as an advertising

---

[19] *Ibid.* at p. 82.

[20] Benjamin M. Compaine & Douglas Gomery, eds. *Who Owns the Media? Competition and Concentration in the Mass Media Industry*, 3rd ed. (Mahwah: Lawrence Erlbaum Associates, Publishers, 2000) at 438.

[21] Interactive Advertising Bureau of Canada, "May 2009: US Advertising Spending: The New Reality", online: http://www.iab.net/insights_research/947883/1675/804370.

[22] Interactive Advertising Bureau of Canada, **"**2006 Canadian Online Advertising Tops $1 Billion Dollars" (30 April 2007), online: http://www.iabcanada.com/newsletters/070430.shtml.

[23] Jan Samioriski, *Issues in Cyberspace: Communications, Technology, Law and Society on the Internet Frontier* (Boston: Allyn & Bacon, 2002) at 115.

mechanism that segments the audience based on observed and measured data such as "the pages or sites the user visits, the content they view, the search queries they enter, the ads they click on, the information they share on social networking sites and the products they put in their shopping carts."[24] This data is combined with the time, length and frequency of visits on websites. Recency is also important, as data from two weeks ago is far less accurate at predicting a user's interests than data from two days ago.

One estimate indicates that spending for internet advertising with a behavioural targeting component will soar from $575 million [in 2007] to $1 billion in 2008.[25] In a more recent report, eMarketer contradicts this estimate, reporting that spending for behaviourally targeted online advertising will only reach $775 million in 2008 due to incomplete development of this complex technology and concerns raised at American regulatory hearings about violating consumer privacy. However, eMarketer projects a steep rise in spending for online behavioural targeted advertising in 2009 to $1.1 billion, with a further increase to $4.4 billion in 2012.[26]

[24] Interactive Advertising Bureau, "July 2008: Behavioral Targeting: Secret Weapon in Display Ad's Arsenal" by eMarketer, online: http://www.iab.net/insights_research/947883/1675/368205.

[25] Del Sesto & Frankel, quoted from *Behavioral Advertising on Target… to Explode Online*, June 11, 2007, online: http://www.emarketer.com.

[26] Interactive Advertising Bureau, *supra* note 24.

PART 3: ONLINE BEHAVIORAL TARGETED ADVERTISING & TRACKING: HOW IT WORKS

"Online behavioural tracking" is defined by the Federal Trade Commission in a Staff Report on Online Behavioral Advertising Principles. The Staff report defines online behavioural tracking as "tracking consumers' online activities over time … in order to deliver advertising that is targeted to the individual consumer's interests. This definition is not intended to include 'first party' advertising, where no data is shared with third parties, or contextual advertising, where an ad is based on a single visit to a web page or single search query."[27]

Behavioural targeting is a technique used by online publishers and advertisers to increase the effectiveness of their marketing campaigns. There are many technologies that enable behavioural targeting, such as cookies, persistent cookies, web beacons and deep packet inspection. These technologies will be discussed in greater detail in the next section. Recently, these types of tracking technologies have been extended to the delivery of advertisements on mobile devices with internet browsing capabilities. Here, we focus on the general model of online behavioural targeted advertising.

First, details about an individual's web browsing behaviours are collected. For example, the website's server typically collects the user's IP address, web browser and operating system type, the page visited, the referring page, and the time of visit. The server may also collect information about the sites visited by an individual, his or her previous purchases, and search queries made. The typical approach uses web analytics to break down the mass of visitors into a number of more discrete channels. Each channel is analyzed and a virtual profile is created to deal with each channel. Some platforms identify users by assigning them a unique identifier cookie that allows the user to be tracked while they are surfing the internet so that the platform can serve relevant advertising while the user is browsing. This information is used to perform predictive data mining, drawing inferences from the regularities and patterns found in datasets. By examining individuals' web browsing patterns, predictions can be made about their preferences, interests, political or religious affiliations or illnesses from which they may suffer.[28]

The collected information is then used to serve targeted advertisements to the user based on what the platform decides should be relevant to the interests of the user. Often, advertisements are served by third party advertising networks, which partner with many different sites and build up a picture of the likely demographic makeup of internet users. Websites may provide their databases on customer profiles to these third party advertising networks to better tune their ad serving technologies.

---

[27] Federal Trade Commission, *FTC Staff Revises Online Behavioral Advertising Principles* (February 2009), online: http://www.ftc.gov/opa/2009/02/behavad.shtm.

[28] The practice of predictive data mining is discussed by Jason Millar in "Core Privacy: A Problem for Predictive Data Mining" at pp. 103-119, published in Ian Kerr & Valerie Steeves & Carole Lucock eds., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (2008), online: http://www.idtrail.org/content/view/799.

Notably, because the purpose of behaviourally targeted advertising is to serve advertisements relevant to the interests of particular users, the seller can ask for a premium for targeted advertisements over random advertising or ads based on the content of the site, as targeted ads are more likely to increase spending or result in increased conversion (actual "clicks" on the advertisement).

The information collected about individuals' web surfing behaviours and responses to served advertising may be sold or rented to third parties. Often, the website operators will share the data with marketing partners or corporate affiliates and subsidiaries, meaning that the user behaviour will be profiled not only by the site visited by a user, but also by any other entities with whom those website operators may choose to share information. As well, the data collected to build profiles on different segments of internet users or individual users may be retained for a period of time to fine tune the delivery of future behavioural targeted advertisements. This information is very valuable, as it assists advertising networks and marketers to build predictive models of behaviour for the individual and guarantee at least a fine degree of segmentation of the individuals, close to "fingerprinting" the user's unique behaviour on a website.

Below, we describe various technologies for consumer tracking and the concerns that have arisen with each technique.

3.1. Cookies

Online businesses use cookies and log files to track consumer behaviour online. Cookies are small text files that are automatically installed by a distant party on a user's computer for the purpose of identifying the user the next time he or she visits the website. Cookies allow a website to store information on a user's hard drive for retrieval at a later date. Cookies may be set up by the entity whose website the user is browsing or may be set up by a third party with whom the website owner has a relationship, usually a marketing relationship such as a third party advertising network.

A website may generate a unique identifier for each visitor and store the identification number on the cookie installed on the user's computer. In some cases, the cookie may assign a unique identifier to each session started on the user's machine. Cookies may not always contain personal information such as a full name, but they may contain information such as the user's e-mail address or IP address, what browser the consumer is using to view the webpage, purchases the consumer has completed, information the consumer has provided to the website (such as name and address information for shipping purchases), advertisements the consumer has clicked on, and the consumer's navigation activities.[29] Online merchants use this information to customize their website according to the consumer's personal preferences and to

[29] Information about the consumer's browser is fairly revealing, as it details the hardware and software the consumer is using, details of the link the consumer clicked on and possibly even the consumer's email address. See Junkbusters, "How Web Servers' Cookies Threaten Your Privacy," online: http://www.junkbusters.com/ht/en/cookies.html.

populate fields requesting consumer address and payment information so that the consumer does not need to re-enter it each time they visit the site.

A recent study documented the use of Flash-based cookies to track users. Flash-based cookies can be used in much the same way as HTTP cookies, except that the technology can also be used as "secondary, redundant unique identifiers that enable advertisers to circumvent user preferences and self-help."[30] These cookies are sometimes used as a means to "undelete" the information in browser-based cookies that a user cleared from their system when they deleted their browsing history. The study goes on to outline the prevalence of Flash-based cookies on the internet:

> We find that more than 50 per cent of the sites in our sample are using flash cookies to store information about the user. Some are using it to 'respawn' or re-instantiate HTTP cookies deleted by the user. Flash cookies often share the same values as HTTP cookies, and are even used on government websites to assign unique values to users. Privacy policies rarely disclose the presence of Flash cookies, and user controls for effectuating privacy preferences are lacking.[31]

Flash cookies are more effective at tracking users' visits around websites than traditional HTTP cookies because they operate in the shadows and are infrequently removed. As well, Flash cookies do not have a built-in expiry date. Third party advertising networks were the most common source of Flash cookies.

Some infrastructure providers can create cookies that are visible on multiple websites, such as DoubleClick.[32] Many companies will partner with digital marketing service providers like DoubleClick so that these marketing service providers will serve ads on their websites. DoubleClick cookies will track user movements across multiple sites, potentially gathering data about user search strings as well.[33] Companies like DoubleClick have the capability to perform cross-site profiling because they have several clients that allow them to collect information about individuals as they surf the internet.

Cookies feed information on the clickstream of a user at that site and any website that hosts the third party advertiser's cookie and those that the user visits back to the third party advertiser for analysis. The third party advertiser processes metrics, such as the number of "impressions," "clicks," "conversions" (when a user clicks on a banner ad) and "performance" (when a user follows a banner link and purchases the product or service advertised). The third party cookie provider also has more individual "cookie-based" reports to track the user's individual surfing behaviour.

---

30 Ashkan Soltani *et al.*, "Flash Cookies and Privacy" (10 August 2009), online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.

31 *Ibid*.

32 Note that DoubleClick uses HTTP cookies, not Flash cookies.

33 Search advertising will be discussed in the next section.

Cookies can be temporary, lasting only for a single browsing session, or persistent, staying on the user's computer for possibly years. For example, Google made headlines in 2007 when it was discovered that its persistent cookie was not set to expire until 2038. Google has since changed the default expiration date on their persistent cookies to two years, but the cookie renews every time a user uses a Google site.[34] Persistent cookies are designed to track individual users as they surf the internet. Third party cookies can be persistent cookies and are often used to develop and enhance consumer profiles.

The user is often unaware that a cookie has been placed on their hard drive to track their activities on that website or serve more relevant targeted advertising to the user. Some merchants explain their use of cookies up front, but many do not. Many merchants state that they use cookies to enhance a user's web experience and may expand on how the cookie works by explanations buried in the small print Terms of Service or Privacy Policy posted on the website. Some websites may have a Privacy Policy that promises not to sell or share any personal information about their users with any third party unless explicitly allowed by the user, however, an increasing number of websites have business models that are premised on sharing user information with their affiliates. Third parties partnered with websites may combine data collected about the user's online behaviour with other information to sell to third party data aggregators to conduct particularized market research.

Often, marketers characterize the data collected by cookies as "anonymous," however the information provided by a user's web browser is often sufficient to identify the user by their internet protocol (IP) address.[35] As well, cookies may contain identifiers that are unique to a user in conjunction with other data such as their e-mail address, therefore the individual could be identified.

One often suggested solution calls on the consumer to manage their cookies. Consumers can customize their browser settings so that cookies are not accepted or a notification appears when a website is attempting to place a cookie. Most internet browsers' default settings accept cookies. Some browsers may not allow consumers to stop cookies. Thus, setting up browsers to reject cookies can be a tricky process, especially for consumers who are not very technically savvy. One possible solution is to routinely delete cookies and temporary internet files. However, even if the user

---

[34] See Michael Agger, "Google's Evil Eye: Does the Big G know too much about us?" *Slate Magazine* (10 October 2007), online: http://www.slate.com/id/2175651.

[35] An IP address is unique to the computer that is connected to the internet and assigned by internet service providers (ISPs). ISPs generally assign IP addresses dynamically, meaning the address may be different each time the computer connects to the internet. Some ISPs assign static ISPs such that the IP address persists for all of the computer's internet sessions. ISPs maintain network logs so that individual IP addresses, both dynamic and static, can be traced back to the subscriber account. The Privacy Commissioner of Canada has ruled that IP addresses is "personal information" as defined under the *Personal Information Protection and Electronic Documents Act* in "PIPEDA Case Summary #315: Web-centered company's safeguards and handling of access request and privacy complaint questioned" (9 August 2005), online: http://www.privcom.gc.ca/cf-dc/2005/315_20050809_03_e.asp. This will be discussed later in this report.

attempts to delete cookie files, they may remain, such as in the case of Flash cookies described above.[36]

3.2. Search advertising and online behavioural advertising: Microsoft-Yahoo and Google

The online advertising space has been divided into several different types of online advertising. For the purposes of simplified explanation, contextual advertising focuses solely on content, whereby advertisements are based on the content of the site the user is viewing. True contextual advertising does not monitor the user's behaviours.[37] Search advertising refers to advertisements displayed on the search results page that are based on the user's search query. The use of behavioural targeted advertising has recently been implemented by companies such as Microsoft, Yahoo and Google, where a user's online activities are tracked and advertisement is targeted to the user based on their profile. Microsoft and Yahoo's behavioural targeting practices involve the tracking of a user's search queries in their search engines. Google's behavioral targeting practices are more limited in that Google search queries are not used to target advertising to users, but because Google holds such a large proportion of search engine market share, its privacy practices have come under much scrutiny by regulators and privacy advocates.[38]

Search engines can collect a lot of information about a user and search engines could leverage this information to record a user's surfing habits and attempt to determine a user's behavioural pattern and interests with the intention of targeting advertisements that provide users with "a more meaningful and rich experience." Indeed, Yahoo filed a series of patent applications describing a "behavior targeting system" that attempts to determine user profiles from the online activities of people so that it can get a sense of which ads to show to users.[39]

---

[36] Microsoft Help and Support, "Emptying Temporary Internet Files Folder Leaves Cookies Files", online: http://support.microsoft.com/kb/q158769/.

[37] These explanations of online advertisements are borrowed from Anand Subramanian, "The Difference Between Search, Behavioral and Contextual" MediaPost (2 June 2005), online: http://www.mediapost.com/publications/?fa=Articles.printFriendly&art_aid=30698.

[38] According to comScore, Google's search engine market share in Canada in January 2008 was 80%. See online: Erick Schonfeld, "The Web in Charts – Google vs Microsoft-Yahoo vs China" TechCrunch (18 March 2008) online: http://www.techcrunch.com/2008/03/18/the-web-in-charts—google-vs-microsoft-yahoo-vs-china/. Note of course, that in July 2009, Yahoo and Microsoft announced a deal that would make Bing, Microsoft's search engine, the search engine for all of Yahoo's sites. This partial merger has been approved by regulatory authorities in Canada and Australia but is still being examined by the US Department of Justice and the EU's Competition Commission.

[39] Bill Slawski, "Yahoo on Search Advertising and Behavioral Targeting" (12 November 2007), online: http://www.seobythesea.com/?p896. Yahoo's patent filings included a Method and apparatus for selecting advertisements to serve using user profiles, performance scores and advertisement revenue information, Behavioral targeting system, Incremental update of long-term and short-term user profile scores in a behavioral targeting system, Behavioral targeting system that generates user profiles for target objectives, Model for generating user profiles in a behavioral targeting system, and Generating a degree of interest in user profile scores in a behavioral targeting system.

The Internet Advertising Bureau reported that in 2008, search marketing dominated the online advertising space with a sustained growth of 40% yearly since 2004. To put the 40% growth into perspective, no other online advertising format (display ads, classified ads, rich media/video, lead generation, email and sponsorships) contributes more than half that amount.[40]

3.2.1. Microsoft and Yahoo's Search Advertising and Behavioural Targeting Practices

Microsoft search advertising offers pay-per-click search ads to connect ads to user search queries. Microsoft offers marketers the opportunity to serve contextual advertisements to the target consumer with MSN sites and Windows Live. As well, Microsoft has targeted search advertising to connect marketers with consumers "by aiming for specific demographics, including location, age group, gender or even where someone might be searching online."[41] Microsoft allows its advertisers to target specific demographic attributes, such as household income, day of the week, and time of day combined with user search queries:

> Targeting consumers based on the way they act is powerful. Now you can target users who are likely to be receptive to your ads based upon their online search behavior. We combine this keyword search behavior with demographic data to identify a very specific audience – which means you can deliver highly relevant advertising.[42]

Microsoft's Online Privacy Statement states that one or more persistent cookies will be placed on a user's computer in order to recognize the computer each time an ad is displayed. The cookies have an expiration date of no more than two years. According to the Privacy Statement:

> Because we may serve advertisements on many different Web sites, we are able to compile information over time about where you, or others who are using your computer, saw and/or clicked on the advertisements we display. We use this information to make predictions about your characteristics, interests or preferences and to display targeted advertisements that we believe may be of interest to you. We may also associate this information with your subsequent visit, purchase or other activity on participating advertisers' Web sites in order to determine the effectiveness of the advertisements.[43]

---

[40] Interactive Advertising Bureau, "February 2008: Search Marketing, the Behemoth Online Advertising Format", online: http://www.iab.net/insights_research/530422/1675/334424.

[41] Microsoft Advertising, "Targeting" online: http://advertising.microsoft.com/canada/en/Advertise/ad-solutions/targeting.

[42] *Ibid.*

[43] Microsoft Online Privacy Statement, online: http://privacy.microsoft.com/en-us/fullnotice.mspx.

Microsoft selects ads to target users based on general interest categories or segments that they have inferred based on demographic or interest data, including information provided when the user created an account for a Microsoft product or information associated with the user's IP address. As well, ads are served based on the pages viewed and links clicked by users when using Microsoft's and its advertising partners' websites and services and search terms entered by a user when using Microsoft's internet search service and information about other users that the user frequently interacts with through Microsoft's communications or social networking services such as MSN Messenger.[44]

Microsoft states that it protects user privacy by storing information used for ad personalization targeting separately from a user's contact information or "other information that directly identifies [the user]." Furthermore, Microsoft gives users the ability to opt-out of receiving personalized targeted ads.[45] However, even where a user chooses not to receive personalized ads, Microsoft will continue to collect the same information as the user browses the web and use Microsoft's online services. Opt-out means that Microsoft will not the information collected for displaying personalized ads.

As noted in its Privacy Statement, Microsoft links behavioural targeting across all its products, not only online but also across its mobile network and the Xbox. Microsoft launched a Mobile Behavioral Targeting Solution on its mobile networks in September 2009 to "[enable] advertisers to reduce advertising waste and maximize the impact and ROI of their mobile campaigns by targeting consumers who have already demonstrated an interest in specific product categories."[46] This technology does not rely on cookies but instead uses behavioural profiles associated with hotmail email and Xbox accounts through a user's Windows Live ID. When a user using a mobile phone uses the same Windows Live ID to access Microsoft's products and services, Microsoft can link their behaviour on the web with behaviour on their mobile phone and Xbox.[47]

Yahoo serves most of the advertisements displayed to users using the Yahoo network of websites, but also allows third party ad servers and ad networks to serve ads within their webpages. Yahoo uses cookies and web beacons to track users. Yahoo Canada lists nearly 50 third party ad networks with which it has relationships.[48] If a user wants

---

[44] *Ibid.*

[45] Personalized Advertising from Microsoft, Opting out of personalized advertising, online: http://choice.live.com/advertisementchoice/.

[46] Jamie Wells, "Microsoft Launches Behavioral Targeting for Mobile" Microsoft Advertising Blog (16 September 2009), online: http://community.microsoftadvertising.com/blogs/analytics/archive/2009/09/16/microsoft-launches-behavioral-targeting-for-mobile.aspx.

[47] See also Laurie Sullivan, "Microsoft links behavioral targeting across web, mobile, Xbox" MediaPost (23 September 2009), online: http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=114165.

[48] Yahoo Privacy Canada, "Network Advertisers and Third-Party Ad Servers" online: http://info.yahoo.com/privacy/ca/yahoo/adservers/. Also discussed by Mark Simon, "What Yahoo Behavioral Targeting Means for Your Search Marketing" eMarketing and Commerce (9 April 2009), online: http://www.emarketingandcommerce.com/story/what-yahoo-behavioral-targeting-means-your-search-marketing.

to prevent a third party from sending and reading cookies on their computer, the user must visit each ad network's website and individually opt out if they offer this capability.

In February 2009, Yahoo added behavioural targeting features for its search and display ads:

> **Search Retargeting for Display Ads** – lets advertisers target display advertising based on a user's search activity. So a user that searches on a term like "sandals" could be served a display ad for footwear elsewhere on Yahoo's network.
> **Enhanced Retargeting for Display Ads** – allows advertisers to deliver dynamically generated display ads across the Yahoo network based on user activity on an advertiser's site. Going beyond standard site retargeting, the new technology would allow an advertiser to target users who visit an airline website to check offers for flights from SFO-JFK, and serve them a personalized offer for that specific flight when they visit a page within the Yahoo Network.
> **Enhanced Targeting for Search Ads** – adds capabilities for Sponsored Search and Content March ads, including ad scheduling and demographic targeting within search. New features are designed to extend the advertiser's control over where and when an ad is shown at both the campaign and ad group level, including what time of day and day of the week an advertiser would like campaigns to run (ad scheduling), and what age and gender they'd like to reach (demographic). Advertisers will be able to vary their bids for different segments in order to increase their ability to reach the desired audience.[49]

In May 2009, Yahoo! opened its Smart Ad platform to third party companies to bring behavioural targeting services to its mobile network.[50] In July 2009, Yahoo and Microsoft announced a deal that would "improve the web search experience for users and advertisers, and deliver sustained innovation to the industry."[51] Microsoft would now power Yahoo search while Yahoo would become the exclusive worldwide relationship sales force for both companies' premium search advertisers. According to Microsoft:

> Providing a viable alternative to advertisers, this deal will combine Yahoo! and Microsoft search marketplaces so that advertisers no longer have to rely on one company that dominates more than 70 percent of all search. With the addition of Yahoo!'s search volume, Microsoft will achieve the size and scale required to unleash competition and innovation in the market, for consumers as well as advertisers.

---

[49] Kevin Newcomb, "Yahoo Adds Behavioral Targetin Features for Search and Display Ads" (24 February 2009), online: http://blog.searchenginewatch.com/090224-091627.

[50] *Supra* note 46.

[51] Microsoft Press Pass, "Microsoft, Yahoo! Change Search Landscape" (29 July 2009), online: http://www.microsoft.com/Presspass/press/2009/jul09/07-29release.mspx.

This partial merger has been approved by regulatory authorities in Canada and Australia but is still being examined by the US Department of Justice and the EU's Competition Commission.[52]

3.2.2. Google search and advertising programs

Google is the world's top search engine and the primary means by which individual users find and access content on the internet. It is the *de facto* search engine for MySpace and AOL. Google generates revenue through its advertising program with AdWords for advertisers and AdSense for publishers, which are text-based ads targeted based on search queries. Paid search is a lucrative form of internet advertising. Following the publicity surrounding the 2005 Department of Justice subpoena to Google for one week's worth of search query records (absent identifying information), it became clear that generally, search service providers systematically monitor, analyze and store search queries. The extent to which this information is shared with third parties is unclear. When a 2006 news investigation revealed that identities of certain searchers could be extracted from anonymized search query logs provided to the research community,[53] an interest in search privacy has emerged, with many reports detailing how major search companies log, store and analyze individual search queries. Privacy advocates in particular were concerned about how detailed search query logs would be used to further hone targeted personalized advertising.

Google's search advertising product displays ads to the user based on their search query. The user's behaviour in response to the search query results and search ads associated with those results are monitored during the browsing session in order to increase the relevance of Google's search advertisements.

3.2.2.1. Google's acquisition of DoubleClick prompts concerns by privacy and consumer advocates

When Google acquired DoubleClick in 2007, privacy advocates and consumer groups around the world launched complaints against the merger, fearing that this merger would have an unprecedented impact on the privacy of internet users as each company separately held a wealth of information about internet users. These public interest groups were concerned that the merger of Google and DoubleClick's user profiles would create a hugely dominant internet company with a large database about users' internet activities gathered without the users' knowledge or informed consent.

---

[52] "Microhoo Deal Approved in Australia, Canada" Media Post News, Computerworld (25 November 2009), online: http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=118032. See also "ACCC gives Yahoo!-Microsoft search deal the go-ahead" Computerworld (25 November 2009), online: http://www.computerworld.com.au/article/327637/accc_gives_yahoo_-microsoft_search_deal_go-ahead.

[53] See Michael Barbaro et al., "A Face Is Exposed for AOL Searcher No. 4417749" *The New York Times* (9 August 2006), online: http://www.nytimes.com/2006/08/09/technology/09aol.html.

DoubleClick is a leading provider of internet-based advertising, placing advertisements on websites on behalf of their over 1,000 clients. Using cookies and web beacons, DoubleClick offers a range of products that enables clients to track user online activity, create user profiles and target advertisements to individual users based on those profiles. When a user is served a DoubleClick ad for the first time, DoubleClick assigns the user a unique number which is recorded in a persistent cookie file stored on the user's computer. As the user visits other websites that partner with DoubleClick, the user is identified and recorded as having viewed each ad. This information is automatically compiled and analyzed, resulting in very rich profiles about individual users, upon which targeted advertisement is based.[54] While DoubleClick claims that these user profiles are anonymous, they still contain a wealth of information about an individual.

In the United States, the Electronic Privacy Information Center (EPIC), the Center for Digital Democracy (CDD) and the United States Public Interest Research Group (USPIRG) filed a joint complaint to the Federal Trade Commission (FTC), arguing that the Google's acquisition of DoubleClick posed an anti-competitive threat to the online advertising market that would have an adverse effect on consumer privacy. Google's position as the largest internet search engine and the leading ad network for the online search advertising market combined with DoubleClick's position as the leading provider of ad-serving tools to publishers and advertisers would enable the world's largest network for the sale of non-search online advertising to own and control the dominant provider of stand-alone ad-serving tools used by web advertisers to connect to other networks. The public interest groups argued that Google's failure to properly notify users of its data collection practices and its retention of user search terms constitute deceptive and unfair trade practices. Furthermore, Google's acquisition of DoubleClick would give Google access to more personal information about the internet activities of consumers than any other company in the world, invading consumer privacy operating with virtually no legal obligation to ensure the privacy, security and accuracy of the personal data collected.[55]

The public interest groups requested an investigation of the Google acquisition of DoubleClick "specifically with regard to the ability of Google to record, analyze, track and profile the activities of Internet users with data that is both personally identifiable and data that is not personally identifiable."[56] As well, the groups requested an order requiring DoubleClick to remove user-identified cookies and persistent identifiers from its records and requiring Google to provide for reasonable access to all personally identifiable data maintained by the company to the person to whom the data pertains.

---

[54] For more information about how DoubleClick works, see their website at http://www.doubleclick.com. See also the Electronic Privacy Information Center's complaint to the Federal Trade Commission against DoubleClick for unfair and deceptive trade practices in 2000, online: http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

[55] Electronic Privacy Information Center, Center for Digital Democracy & United States Public Interest Research Group, "Complaint and Request for Injunction, Request for Investigation and for Other Relief" (submitted to the Federal Trade Commission on 20 April 2007), online: http://epic.org/privacy/ftc/google/epic_complaint.pdf at para. 54.

[56] *Ibid.* at para. 55.

The FTC held a hearing on the Google-DoubleClick merger and the online advertisng industry and in December 2007, the Commission approved the proposed merger without conditions, finding that Google's proposed acquisition of DoubleClick is unlikely to substantially lessen competition.[57] The Commission found that the privacy concerns raised by interested parties was not an issue unique to Google and DoubleClick and extended to the entire online advertising marketplace. Because the sole purpose of federal antitrust review of mergers and acquisitions is to identify and remedy transactions that harm competition, the FTC lacked the legal authority to block the acquisition on privacy grounds. The FTC also found that there was insufficient evidence to show that DoubleClick has market power in the third party ad serving markets. The FTC however stated that they would closely watch the online advertising market for future unlawful tying or other anticompetitive conduct.

The American complaint was based on a June 2007 letter by the European Consumers' Organisation (BEUC) to the European Commission expressing privacy and competition concerns about the Google-DoubleClick merger.[58] In response to BEUC's complaint, the European Parliament held hearings on the issue and cleared the acquisition of DoubleClick by Google in March 2008, considering the deal "unlikely to have harmful effects on consumers."[59] The European Commission concluded that the transaction would be unlikely to have harmful effects on consumers, either in ad serving or in intermediation in online advertising markets, thus the acquisition would not significantly impede competition within the European Economic Area (EEA) or a significant part of it.

Both the European and American complaint prompted subsequent complaints by the Canadian Internet Policy Public Interest Clinic (CIPPIC) to two regulatory bodies in Canada. CIPPIC requested that the Office of the Privacy Commissioner of Canada conduct an audit into the personal information management practices of Google and DoubleClick in light of the proposed acquisition.[60] In particular, CIPPIC alleged that Google did not allow consumers to opt out of unnecessary data sharing and engaged in

---

[57] Federal Trade Commission, "Federal Trade Commission Closes Google/DoubleClick Investigation" (20 December 2007), online: http://www.ftc.gov/opa/2007/12/googledc.shtm. See also Federal Trade Commission, "Statement of Federal Trade Commission Concerning Google/DoubleClick" FTC File No. 071-0170, online: http://ftc.gov/os/caselist/0710170/071220statement.pdf.

[58] BEUC, "Proposed acquisition of DoubleClick by Google" (letter to European Commission on 27 June 2007), online: http://epic.org/privacy/ftc/google/beuc_062707.pdf. In December 2007, BEUC filed a follow up letter to the European Commission to further underline consumers' concerns with the proposed merger. See online: http://docshare.beuc.org/docs/1/FHPCKIEAJIKPOEFNMKOGOFNFPDB39DWYT69DW3571KM/BEUC/docs/DLS/2007-01173-01-E.pdf and http://docshare.beuc.org/docs/2/FHPCKIEAJIKPOEFNMKOGOFNFPDB39DWYTK9DW3571KM/BEUC/docs/DLS/2007-01174-01-E.pdf.

[59] See Europa Press Release, "Mergers: Commission clears proposed acquisition of DoubleClick by Google" (11 March 2008) online: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/426. "EU gives green light to Google/DoubleClick merger" EurActiv.com (5 October 2009), online: http://www.euractiv.com/en/infosociety/eu-gives-green-light-googledoubleclick-merger/article-170895.

[60] Canadian Internet Policy Public Interest Clinic, "Request for Audit of Google Inc. and DoubleClick Inc." (submitted to the Privacy Commissioner of Canada on 17 September 2007), online: http://www.cippic.ca/uploads/G-DC_%20Privacy_complaint_17Sept07(1).pdf.

excessive personal information collection and use for the purpose of targeted advertising. While the Privacy Commissioner found CIPPIC's concerns regarding Google's transparency with respect to their privacy practices well-founded, the office decided not to audit the personal information management practices of Google and DoubleClick, stating that the scope of behavioural marketing is larger than the ramifications of a merger. The Privacy Commissioner responded with a broad approach, promising to incorporate examination into Google's online practices into the work undertaken b the Privacy Commissioner's Research, Education and Outreach branch.[61]

CIPPIC also requested that the Canadian Competition Bureau inquire into Google's proposed acquisition of DoubleClick on the grounds that the acquisition is likely to prevent or lessen competition substantially in the targeted online advertising industry.[62] The Competition Bureau conducted an inquiry into the matter and concluded that the parties to the transaction compete in separate segments of the online advertising industry and that there were not sufficient grounds to make an application to the Competition Tribunal for a remedial order. The Bureau also found that privacy issues fall outside the Competition Bureau's mandate.[63]

Since the acquisition approval, reports have revealed that Google is using the same tracking cookie across both AdSense and DoubleClick's online advertising network. This allows Google to collect individual's surfing habits as they move from AdSense partner sites to sites using DoubleClick's ad management platform. Google claims that in some cases, the data is not combined, depending on their contract with the customer.[64] A University of California, Berkeley study revealed that Google AdSense was used by 35% of a nearly 400,000 site cross-section of the internet and DoubleClick was used by over 26%.[65] According to the study, the next most prevalent web tracker is Omniture used by 6% of the sites in the cross-section.

---

[61] Response letter by Trevor Shaw, Director General of the Audit & Review Branch of the Office of the Privacy Commissioner of Canada to Philippa Lawson, Director of CIPPIC, dated 28 August 2008.

[62] Canadian Internet Policy Public Interest Clinic, "Section 9 Application for an Inquiry into the Proposed Merger of Google, Inc. and DoubleClick Inc." (submitted to the Commissioner of Competition on 2 August 2007), online: http://www.cippic.ca/uploads/Google-DC_s.9_CompAct_complaint_FINAL.pdf.

[63] Response letter by Melanie L. Aitken, Senior Deputy Commissioner of Competition to Philippa Lawson, Director of CIPPIC, dated 19 March 2008.

[64] Cade Metz, "Google tracking cookie spans AdSense, DoubleClick" *The Register* (4 June 2009), online: http://www.register.co/uk/2009/06/04/google_doubleclick_cookie.

[65] KnowPrivacy report, *supra* note 10.

3.2.2.2. Google's interest-based advertising

Despite the approval of Google's acquisition of DoubleClick in early 2008, Google did not launch behavioural targeting products until March 2009. Google launched an interest-based advertising service with technology that displays ads to particular users based on their interest categories. DoubleClick collects information about user behaviour via cookie technology. The interest-based advertising service uses information about an individual user's web behaviour to deliver targeted ads as users spend time on YouTube and traverse across the many third-party sites in Google's AdSense networks.

It is important to note that unlike Microsoft and Yahoo's behavioural targeting practices, Google's interest-based advertising service does not currently combine data from user search queries to further profile users for behavioural targeting. Google's behavioural targeting practices are more privacy protective than their competitors, given that they do not use information acquired about users through account-based services (such as Gmail) for behavioural targeting.[66] Google monitors only individuals' web behaviour across its network sites for behavioural targeting using a unique ID cookie. Google states that they protect users' data by not using sensitive interest categories such as those based on race, religion, political affiliation, sexual orientation, health or sensitive financial information.[67]

Google provides users with the ability to opt out of the DoubleClick cookie for interest-based advertising through an Ads Preferences Manager. This means that Google's AdSense partners and certain Google services using the DoubleClick cookie will know that the user has opted out of the cookie and will not attempt to assign other DoubleClick cookies in the future.[68] If the user clears cookies from their browser, the opt-out cookie will be deleted and they will have to opt out again unless the user installs a plug-in to make opt-out permanent.[69] The Ads Preferences Manager also allows users to change their interest categories instead of wholly opting out of the service. For

---

[66] Unlike Microsoft and Yahoo, Google does not combine its server logs with search advertising for behavioural targeting. Google's behavioural targeting practices use DoubleClick cookies installed on the user's browser. Google has stated that it does not currently use search terms for behavioural targeting, but notes that its competitors Microsoft and Yahoo do. While Google believes that it has enough data to deliver effective advertising to its users now, it is uncertain when the competitive pressure may lead Google to join Microsoft and Yahoo in using search data to target advertisements to users.

[67] Google uses the European Commission, *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Article 8 definition for sensitive personal data: "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".

[68] Google, "Opt-out completed successfully", online: http://www.google.com/ads/preferences/html/opt-out.html. Notably, the Network Advertising Initiative has set up an Opt-out Tool to allow consumers to opt out of behavioural advertising delivered by member companies. Opting out does not mean that the user will no longer see all ads, only that the user will no longer receive tailored ads based on their web preferences and usage patterns from the network from which they have opted out. See the tool online: http://www.networkadvertising.org/managing/opt_out.asp.

[69] Note that Google built their tool for persistent opt-out and open sourced it so that anyone could build their own, working with the Electronic Frontier Foundation. See: http://www.eff.org/deeplinks/2009/03/google-begins-behavioral-targeting-ad-program. The Advertising Cookie Opt-out Plugin can be found here: http://www.google.com/ads/preferences/plugin/.

example, a user can delete an interest category that Google has automatically placed them into or they can add an interest category that they wish to receive ads regarding.[70]

With this announcement, Google has come under close scrutiny by Consumer Affairs Commissioner Meglena Kuneva in the European Union, who has threatened EU intervention to set tougher rules on how internet users' personal data is collected, analyzed and shared by search engines and service providers. Kuneva criticizes Google's opt out measures, stating that they are partial and sometimes nowhere to be found, often cumbersome for consumers and unstable. Kuneva claimed that avoiding tracking is currently technical difficult, if not impossible.[71] This issue is being addressed in some Member States, such as in France.[72] The European Commission has since been subject to intense lobbying campaigns by Google and Microsoft regarding regulation of how data is used for online targeted advertisement and user tracking.[73]

[70] The Google Ads Preferences Manager can be found here: http://www.google.com/ads/preferences.

[71] Bate Felix, "EU threatens action to defend Web users' privacy" Reuters (30 March 2009), online: http://www.reuters.com/article/technologyNews/idUSTRE52T5YA20090330.

[72] "Online Behavioral Advertising Attracts Attention in Europe" Privacy & Information Security Law Blog, Hunton & Williams LLP (7 April 2009), online: http://www.huntonprivacyblog.com/2009/04/articles/european-union-1/online-behavioral-advertising-attracts-attention-in-europe/.

[73] Chris Williams, "Google and Microsoft bombard Brussels over ad tracking" The Register (15 September 2009), online: http://www.theregister.co.uk/2009/09/15/brussels_behavioural_targeting/.

3.3. Advertising using information from internet service providers and Deep Packet Inspection

In recent years, commercial services have begun offering tracking tools to internet service providers (ISPs) that allow ISPs to inspect their customers' traffic and sell this data to third parties. ISPs have started deploying technologies like deep packet inspection equipment (DPI), which offers new monitoring capabilities far broader than the common computer cookie discussed earlier. These technologies can be deployed to filter or to intercept, copy and read packets of internet traffic midstream, so that the system can analyze their customers' online activities and manage the flow of traffic. One potential use of the information gleaned from DPI technology is an examination of consumers' online activities and communications in order to tailor advertisements to their unique tastes.[74] Furthermore, DPI products are not applications that are installed on a user's personal computer. They are elaborate systems set up by the product's developer in collaboration with an ISP, with all software and hardware existing "in the cloud."[75]

Below are two recent examples of ISPs implementing DPI technology to roll out targeted advertising to their customers.

3.3.1. NebuAd

An American company called NebuAd developed technology to enable internet service providers (ISPs) to target behavioral advertising to ISP customers based on an individual's web surfing history. In 2008, NebuAd partnered with ISPs in order to gain access to their raw data. The company mostly partnered with American ISPs, most notably Charter Communications and also partnered with some Canadian ISPs. These ISPs would receive a portion of NebuAd's ad revenues in return for providing NebuAd with their raw user data.[76] NebuAd would act as an ad network to serve as a broker between advertisers and Web publishers. NebuAd purchased its ad impressions from other ad networks, such as ValueClick.[77]

---

[74] Danielle Keats Citron, "The Privacy Implications of Deep Packet Inspection", online: http://dpi.priv.gc.ca/index.php/essays/the-privacy-implications-of-deep-packet-inspection/.

[75] Maxim Weinstein, "BadWare and DPI", online: http://dpi.priv.gc.ca/index.php/essays/badware-and-dpi/.

[76] See Stacey Higginbotham, "NebuAd Bites The Dust" (May 19, 2009), online: http://gigaom.com/2009/05/19/nebuad-bites-the-dust/. See also Nate Anderson, "NebuAd loses CEO, business model in wake of tracking furor" (September 5, 2008), online: http://arstechnica.com/tech-policy/news/2008/09/nebuad-loses-ceo-business-model-in-wake-of-tracking-furor.ars. See also Zachary Rodgers, "Questions for Bob Dykes, NebuAd CEO" (January 3, 2008), online: http://www.clickz.com/3628009.

[77] Robert D. Hof, "Ad Networks Are Transforming Online Advertising" Business Week (February 19, 2009), online: http://www.businessweek.com/magazine/content/09_09/b4121048726676.htm.

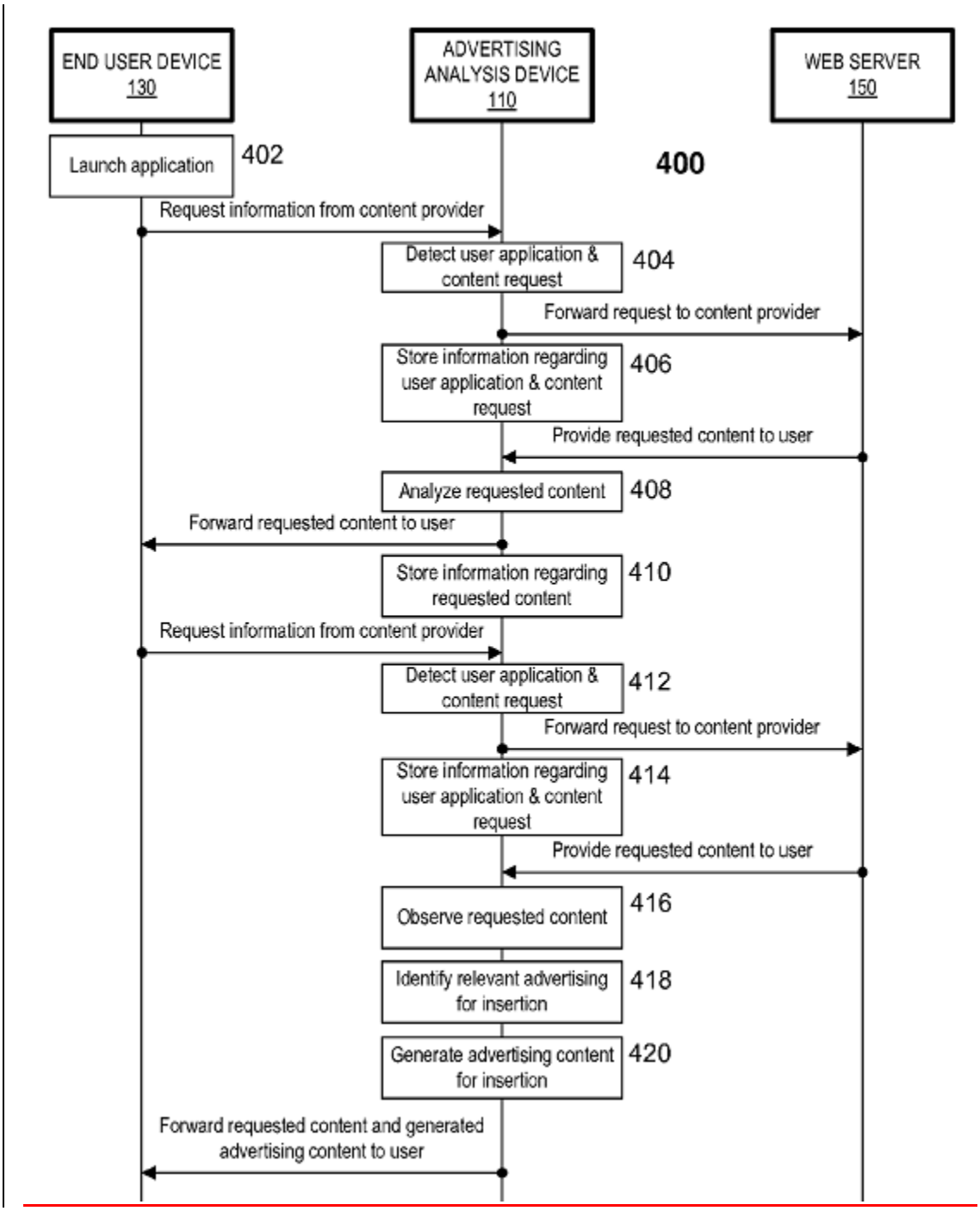

Figure 1: Flowchart filed by NebuAd in its patent application[78]

[78] This diagram was taken from an article by Ryan Singel, "Can Charter Broad Band Customers Really Opt-Out of Spying? Maybe Not" *WIRED Magazine* (May 16, 2008), online: http://www.wired.com/threatlevel/2008/05/theres-no-optin/.

NebuAd's system works by:

> …[i]nstall[ing] a hardware device it has designed inside the network of I.S.P.s. One device can monitor all of the information going to and from 30,000 to 50,000 users. The device associates the information it sees with the I.P. address of the user … [T]he I.P. address is encoded before it is stored using a technique called hashing. That makes it harder for someone who might get access to NebuAd's system to get a list of the I.P. addresses about which it has information. For each of the I.P. addresses it is monitoring, the NebuAd system analyzes the Web traffic including the addresses of the pages visited, the search terms entered, and keywords that appear on those pages. This information is distilled to about 1000 categories representing various purchase interest: shopping for a mortgage, researching lawnmowers, and so on. The system keeps track of how often and how recently users visited pages in these categories, but … the system does not keep the list of the actual pages visited.[79]

In its Privacy Policy, NebuAd states that they do not collect personally identifiable information such as e-mail addresses, last names, street addresses, telephone numbers, social security numbers, numbers associated with health plans, or financial information.[80] However, NebuAd does collect and use web pages viewed by users, web search terms, the amount of time spent at web sites, response to advertisements, and postal codes. The information that NebuAd collects is stored on servers in the United States, and therefore, NebuAd may share that information with governments, courts of law, or enforcement agencies.

Privacy advocates, such as the Center for Democracy and Technology and the Public Knowledge and Free Press, criticized NebuAd's partner ISPs for failing to obtain customer consent before providing NebuAd with customer search and browsing data.[81]

NebuAd's opt-out cookie has also received much criticism.[82] In order to opt out, customers must visit the Privacy Policy on NebuAd's web page.[83] If a customer chooses to opt out, NebuAd places a cookie on his or her system.[84] When a customer opts out, he or she is only able to opt out of receiving the targeted ads. Opting out does

---

[79] Saul Hansell, "NebuAd Observes 'Useful, but Innocuous' Web Browsing" New York Times (April 7, 2008), online: http://bits.blogs.nytimes.com/2008/04/07/nebuad-observes-useful-but-innocuous-web-browsing/.

[80] An archive of NebuAd's Privacy Policy can be found online at: http://web.archive.org/web/20080209125953/www.nebuad.com/privacy/serviceprivacy.php.

[81] Cade Metz, "Hitwise and Compete: The user data ISPs do sell Data Pimping it old school" The Register (October 8, 2008), online: http://www.theregister.co.uk/2008/10/08/hitwise_compete_and_isps/print.html.

[82] Declan McCullagh, "NebuAd grilled over hot coals in Congress on privacy" CNET News (July 17, 2008), online: http://news.cnet.com/8301-13578_3-9993554-38.htm.

[83] NebuAd privacy policy, *supra* note 80.

[84] Cade Metz, "NebuAd makes meal of opt-out cookie" The Register (July 9, 2008), online: http://www.theregister.co.uk/2008/07/09/nebuad_promises-cookieless-outout/.

not prevent a user's information from being collected, tracked and resold, meaning there is no mechanism for a user to opt out of deep packet inspection.[85] The opt-out cookie is also not permanent, meaning that if that cookie disappears, which will occur for those users who regularly delete browser cookies from their computers, the user is no longer opted-out of receiving targeted ads.[86] In addition, NebuAd's system raises concerns regarding its retention of personal information, the anonymity of personal information, and the tracking of young computer users.[87]

Much political attention has been paid to the issue of DPI and NebuAd's practices. When NebuAd partnered with American ISP Charter Communications in the summer of 2008, there was consumer backlash that resulted in a congressional investigation on targeted advertising. U.S. politicians expressed concerns that the deep packet inspection of internet traffic is too privacy invasive and the practice could be acceptable only if customers give affirmative consent by opting in to the practice.[88] Once Congress started holding hearings on NebuAd's technology, ISPs started backing out of their partnerships with NebuAd. Critics likened the practice to wiretapping:

> The fact is that it would have allowed profiling of an individual – where they were going and what they were doing online, and there was no guarantee that this information could not ultimately be compromised. … They made the right decision in halting their test.[89]

Customers are also very upset with NebuAd. In a class action lawsuit, fifteen customers are suing NebuAd and several of the ISPs who partnered with NebuAd.[90] As a result of the controversy regarding NebuAd's behavioral advertising, NebuAd has shut down.[91]

---

[85] "Embarz, WOW Bury Snooping In Terms of Service" DSL Reports (April 7, 2008), online: http://www.dslreports.com/shownews/Embarq-WOW-Bury-Snooping-In-Terms-Of-Service-93375.

[86] Cade Metz, "NebuAd makes meal of opt-out cookie" The Register (July 9, 2008), online: http://www.theregister.co.uk/2008/07/09/nebuad_promises-cookieless-outout/.

[87] John Timmer, "Behavioral Advertisers discover the self-regulation gospel" (July 2, 2009), online: http://arstechnica.com/tech-policy/news/2009/07/behavioral-advertisers-state-principles-for-self-regulation.ars.

[88] Declan McCullagh, "NebuAd grilled over hot coals in Congress on privacy" CNET (July 17, 2008), online: http://news.cnet.com/8301-13578_3-9993554-38.htm. There were also concerns that opt-in consent may apply under section 631 of the *Communications Act of 1934*.

[89] Rep. Edward J. Markey (D-Mass.), Chairman of the House Energy and Commerce subcommittee on Telecommunications and the Internet, quoted in Peter Whoriskey, "Internet Provider Halts Plan to Track, Sell Users' Surfing Data", Washington Post (25 June 2008), online: http://www.washingtonpost.com/wp-dyn/content/article/2008/06/24/AR2008062401033_pf.html. See also Grant Gross, "Senators Question NebuAd, Targeted Ad Privacy" PC World (July 9, 2008), online: http://www.pcworld.about.com/od/securit1/senators-question-nebuAd-targ.htm.

[90] Dan Valentine, et al. v. Nebuad, Inc., et. al, (compl.). This class action suit was filed against NebuAd in a California federal court. The class action lawsuit alleges that NebuAd and the ISPs violated the U.S. Electronic Communications Privacy Act (18 U.S.C. § 2510, the U.S. Computer Fraud and Abuse Act (18 U.S.C. § 1030), California's Invasion of Privacy Act (California Penal Code §631) and California's Computer Crime Law (California Penal Code § 502).

[91] Stacey Higginbotham, "NebuAd Bites The Dust" (May 19, 2009), online: http://gigaom.com/2009/05/19/nebuad-bites-the-dust/. "Online Tracking Company NebuAd closes doors

3.3.2. Phorm

Phorm, a UK based technology company, has developed a solution that allows advertisers to deliver targeted behavioral advertising by collecting data from users' internet service providers. Phorm's behavioral advertising technology works by examining users' web traffic and tracking them with assigned identification numbers stored in browser cookies.[92] "The browsing habits of each number are associated with categories of interest, which advertisers can then place ads for."[93] While Phorm tracks the web pages a user visits, it states that its system does not retain personally identifiable information, as information is processed automatically, in real time and deleted as soon as an "interest match" has been made, storing only the interest match.[94]

---

after privacy woes" CBC News (May 21, 2009), online: http://www.cbc.ca/technology/story/2009/05/21/nebuad-target-advertising-consumer-privacy.html.

[92] Out-law.com, "online advertisers team up on privacy principles self-regulation to head off Phorm backlash" The Register (January 16, 2009), online: http://www.theregister.co.uk/2009/01/16/online_advertising/print.html.

[93] Jeremy Kirk, "BT Opts Not to Deploy Phorm Behavioral Ad System" PC World (July 6, 2009), online: http://www.pcworld.com/businesscenter/article/167883/bt_opts_not_to_deploy_phorm_behavioral_ad_system.html.

[94] Phorm, online: http://www.phorm.com. See also United Kingdom, All Party Parliamentary Communications Group, "Can we keep our hands off the net? Report of an Inquiry by the All Party Parliamentary Communications Group" (October 2009), online: http://www.apcomms.org.uk/uploads/apComms_Final_Report.pdf at p. 13.

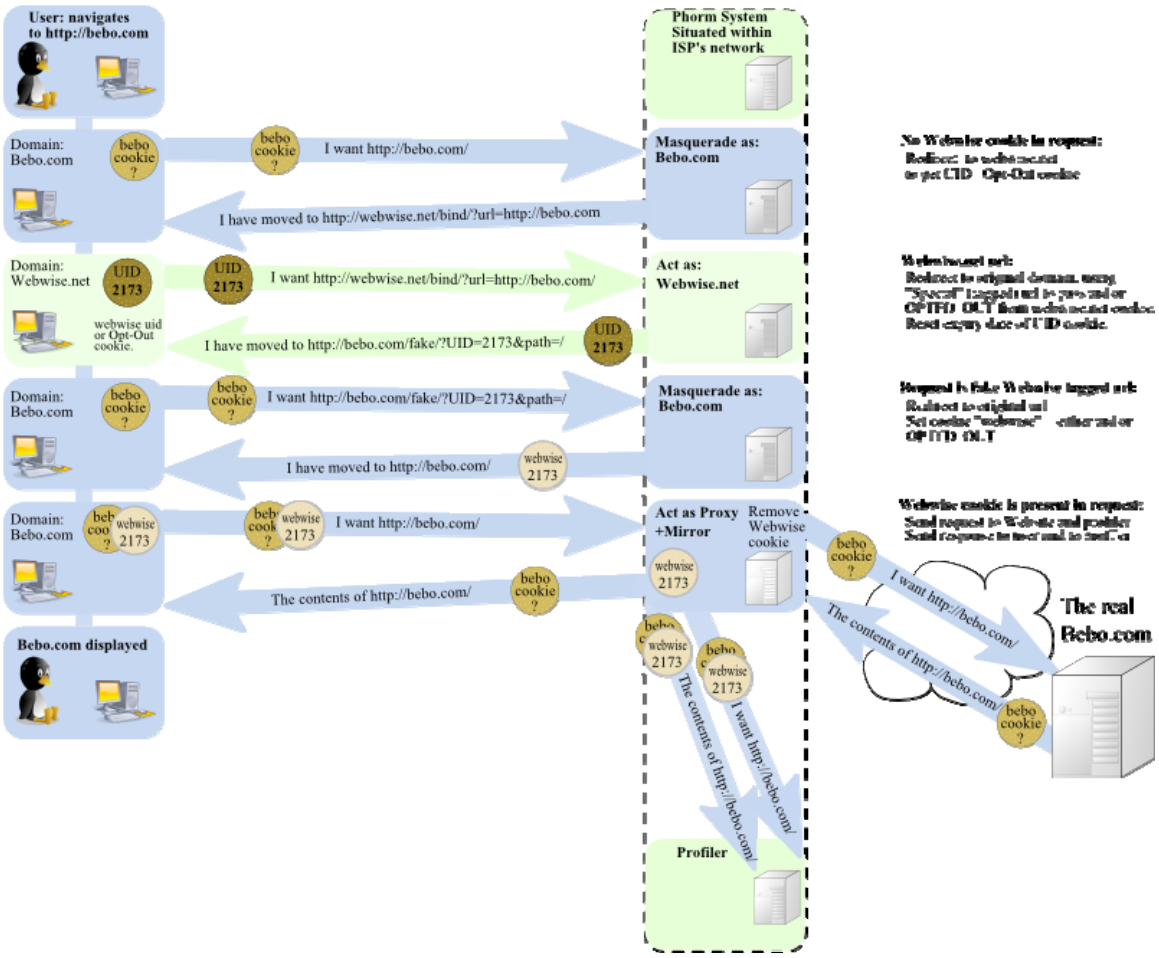

Figure 2: How Phorm's "Webwise" system creates copies of its tracking cookie in each domain the end-user visits[95]

Although Phorm has stated that consumers are in control of their personal data because it uses an opt-in and opt-out privacy policy, there is concern that Phorm is receiving customer browsing data from ISPs without the customer's consent.[96]

In April 2008, British Telecom admitted that it had used a developmental version of Phorm's traffic inspection system without customer consent in 2006 and 2007.[97] During the trials, BT and Phorm denied what was happening to the press and customers. As a

[95] Richard Clayton, "The Phorm 'Webwise' System" (18 May 2008), online: http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf. Diagram from Wikipedia entry: http://en.wikipedia.org/wiki/Phorm.

[96] Cade Metz, "Hitwise and Compete: the user data ISPs do sell Data pimping it old school" The Register (October 8, 2008), online: http://www.theregister.co.uk/2008/10/08/hitwise_compete_and_isps/print.html.

[97] European Union, "Telecoms: Commission launches case against UK over privacy and personal data protection" (April 14, 2009), online: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570&format=HTML&aged=0&language=EN&guiLanguage=en.

result, consumers felt betrayed and still continue to express distrust in their ISPs.[98] This debacle prompted complaints to the Information Commissioner, the Interception Commissioner, government departments, OfCom and the police, however, none of these bodies took action.[99] The Home Office and Department for Business, Enterprise & Regulatory Reform (BERR) has stated that Phorm's service is capable of being deployed legally and does not fall afoul of the *Regulation of Investigatory Powers Act 2000*. The Information Commissioner's Office took the view that to conform to data protection laws, the system had to be "opt in," but the ICO decided to take no action on consumer complaints because they did not expect similar trials to be conducted in the future.

As a result of the UK's non-action, Viviane Reding, the EU Commissioner on Information Society and Media, commenced infringement proceedings asking the UK to adopt national laws to prohibit surveillance without the user's consent.[100] Reding is basing her request on the EU Directive on Privacy and Electronic Communications, which requires EU Member States to ensure confidentiality of the communications and related traffic data by prohibiting unlawful interception and surveillance unless the users concerned have consented. The EU Data Protection Directive specifies that user consent must be freely given, specific, and informed.[101]

In the midst of the infringement proceeding, Amazon and Wikipedia opted out of using Phorm's behavioral advertising technology.[102] However, Phorm recently stated that they have exclusive agreements with ISPs representing approximately 70% of UK broadband subscribers with agreements from three of the largest UK ISPs – BT, Virgin Media and TalkTalk – and "are at various stages of engagement with partners in leading internet economies around the world."[103]

---

98 All Party Parliamentary Communications Group, *supra* note 94 at p. 14.

99 Sean Hargrave, "How long can Phorm go on?" The Guardian (June 11, 2009), online: http://www.guardian.co.uk/business/2009/jul/07/phorm-internet

100 European Union Press Release, *supra* note 92.

101 The UK has two months to reply to the first stage of this infringement proceeding. If the EU Telecoms Commissioner does not receive a reply or if the observations presented by the UK are not satisfactory, the Commission may issue a reasoned opinion asking the UK to comply with EU law. If the UK still fails to fulfill its obligations under EU law, the Commission will then refer the case to the European Court of Justice. The legal process could potentially end in legal proceedings to change UK statutes.

102 Mike Harvey, "Wikipedia latest to reject Phorm 'snooping' technology" The Times (April 21, 2009), online: http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article6143577.ece?p.

103 All Party Parliamentary Communications Group, *supra* note 94 at p. 13.

3.3.3. Use of deep packet inspection by internet service providers in Canada

In a recent telecommunications proceeding before the Canadian Radio-television and Telecommunications Commission (CRTC), the issue of deep packet inspection technologies was explored in the context of the broader issue of internet traffic management practices by internet service providers in Canada.[104] In the proceeding, several ISPs admitted to deploying DPI technology on their networks, including Bell Canada, Rogers, Shaw, Cogego, Eastlink and Barrett Xplore. A report commissioned by the CRTC suggested that ISPs could use DPI technology for personalized advertising and targeted service offers.[105]

The Privacy Commissioner of Canada submitted comments to the proceeding, stating that the use of DPI technology on ISP networks raised important issues regarding the protection of personal information on the internet, in particular with the technology's ability to target advertising based on an analysis of users' web-browsing behaviour. The Privacy Commissioner raised several concerns with the use of DPI for behavioural advertising, such as the lack of adequate notice by service providers to their users that this type of tracking is taking place, the lack of an adequate consent model for this tracking and the inadequacy of opt-out cookies, as they are only a temporary mechanism to comply with the individual's choice not to have their online activity tracked. As well, the Privacy Commissioner stated that anonymization of user profiles does not solve the problem as it may still be possible to link a profile to a particular individual.[106]

In May 2008, CIPPIC launched a complaint against Bell Sympatico for its use of DPI technology to collect and use personal information from its customers without their consent.[107] The initial complaint stated that there was no information to suggest that Bell Sympatico has deployed DPI for the purpose of targeted advertising, but in a follow up supplement letter, CIPPIC outlined the concerns with the possible use of DPI for behavioural targeting.[108] For example, CIPPIC alleged that Bell Sympatico uses DPI technology during internet transmissions to collect and use personal information from its customers without their consent and that this practice collects more personal information than is necessary to fulfill the company's stated purposes of ensuring

---

[104] Telecom Public Notice CRTC 2008-19, *Review of the Internet traffic management practices of internet service providers*, online: http://www.crtc.gc.ca/ENG/archive/2008/pt2008-19.htm.

[105] Graham Finnie, "Report: ISP Traffic Management Technologies: The State of the Art" *Heavy Reading* (January 2009), online: http://www.crtc.gc.ca/PartVII/eng/2008/8646/isp-fsi.htm.

[106] Office of the Privacy Commissioner submission to Telecom Public Notice CRTC 2008-19, *Review of the Internet traffic management practices of Internet service providers* (18 February 2009), online: http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1027577.PDF.

[107] Canadian Internet Policy Public Interest Clinic, "Bell Canada/Bell Sympatico Use of Deep Packet Inspection: PIPEDA Complaint" submitted to the Privacy Commissioner of Canada (9 May 2008), online: http://www.cippic.ca/uploads/Bell-DPI-PIPEDAcomplaint_09May08.pdf. CIPPIC also launched parallel complaints to the Privacy Commissioner against Rogers, Shaw and Eastlink for their use of DPI for traffic shaping in July 2008.

[108] Canadian Internet Policy Public Interest Clinic, first supplementary letter to the Office of the Privacy Commissioner filed 26 May 2008, online: http://www.cippic.ca/uploads/File/Bell-PIPEDAsup1-behavioural%20targeting_26May08.pdf.

network integrity and quality of service. As well, CIPPIC alleged that Bell does not adequately inform its customers of its practices regarding the collection of personal information during internet transmissions.

In August of 2009, the Privacy Commissioner released a decision, finding the complaint not well-founded with regard to the matters of consent, as it found there was no evidence that Bell was conducting targeted advertising, and of limiting collection, as it found the purpose of traffic management to be legitimate. The Privacy Commissioner found CIPPIC's complaint to be well-founded regarding the matter of openness. The Privacy Commissioner requested that Bell add to their privacy FAQ answering the question of how Bell's traffic management practices impact the privacy of their customers and indicate that personal information is collected in its use of DPI on their website. As well, the Privacy Commissioner stressed that if Bell chose to expand its use of DPI by collecting, using or disclosing the personal information of its customers for a purpose other than managing their network traffic, renewed, meaningful and informed consent from its customers would be required.[109]

3.4. Targeted advertising on social networking websites

Social networking sites are increasingly popular across the world. Marketers say that up to 44 percent of internet users use social media sites like Facebook, Twitter, LinkedIn or MySpace and nearly four of ten internet users use social networking once a day.[110] As these services often offer memberships to their services for free, they rely on advertisement subsidizations in order to provide their services at no cost to their members. Social networking services have launched various advertising platforms on their services to reach a significant audience. Using the information of their subscribers, advertising on social networks can target users' specific interests.[111] Furthermore, social networking sites allow marketers to inject themselves into conversations and manipulate participants into being favourably disposed towards their products by using loyal consumers' word-of-mouth to communicate a firm's bottom-line to new prospects.[112]

According to the Interactive Advertising Bureau, marketers will spend an estimated $2.35 billion to advertise on social networks worldwide in 2009, a 17% increase from 2008 levels. Social networking continues to rise as a consumer activity around the

---

[109] PIPEDA Case Summary #2009-010, "Report of Findings: Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection" (September 2009), online: http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.cfm.

[110] "Kibitzing Online" *Privacy Journal* (September 2009) Volume 35, Number 11.

[111] An example of targeted advertising on social networking websites that is not discussed in this report is that of MySpace and its use of the HyperTargeting advertising platform that capitalizes on users' interests and passions. See CIPPIC, "Online Privacy Threats" *supra* note 1 at p. 29-30 for an excellent description of MySpace's targeted ad platform.

[112] "Kibitzing Online" *supra* note 110.

world and Facebook is quickly becoming a leader in social networking advertising in multiple markets worldwide.[113]

A 2009 study by AT&T Labs and Worcester Polytechnic Institute found that online social networking sites leak personal information, raising the possibility that third party aggregators can potentially link social network identifiers to past and future website visits, thereby tracking a user's online activities.[114] Social networking sites often assign a unique identifier to its registrants and when these sites make personal information available to companies that track users' browsing habits, they often include this unique identifier. This allows businesses to link anonymous browsing habits to specific people.[115]

3.4.1. Facebook

When a user registers on Facebook, Facebook requests the person's full name, email address, birthday and gender and encourages users to provide personal information to post on their profiles, such as their hometown, political and religious views, sexual orientation, instant messaging screen names, telephone numbers, address, relationship status, schools attended, current and previous employers, personal interests and preferences. Facebook also collects users' browser types and IP addresses.[116]

Because Facebook users often share a lot of information about themselves with their friends on their profile pages, Facebook has amassed a large amount of personal details about individual's personal interests, hobbies, employment and group affiliations. Tim Kendall, director of monetization at Facebook, gave some examples of how marketers worked with Facebook's user base by using user-provided information about their personal interests and personal information:

> When apparel brand Anchor Blue wanted to promote its new Heidiwood line, it tapped into this user-declared info to target ads to Faebook members whose pop-culture interests were aligned. H&R Block has used this site to aim ads at new filers during tax season, and J.C. Penney used Facbeook to target new college students with a campaign focused on dorm life. Marketers looking for more of a direct-response sale than a long-term

---

113 Interactive Advertising Bureau, "April 2009: Worldwide Social Network Ad Spending", online: http://www.iab.net/insights_research/947883/1675/804264.

114 Thomas Claburn, "Social Networks Leak Personal Information" *InformationWeek*, (24 August 2009), online: http://www.informationweek.com/news/internet/social_network/showArticle.jhtml?articleID=219401268. The study examined twelve social networking sites: Bebo, Digg, Facebook, Friendster, Hi5, Imeem, LinkedIn, LiveJournal, MySpace, Orkut, Twitter, and Xanga.

115 This practice was discussed in "Online Kibitzing" *supra* note 110.

116 Facebook's Privacy Policy, online: http://www.facebook.com/policy.php.

> branding effect also see the benefits in targeting at social networking sites.[117]

Facebook markets itself as a medium that allows advertisers to "reach the exact audience with relevant targeted ads."[118] Facebook aggregates user profile information about user preferences to target personalized advertisements and promotions to its users. Advertisements that appear on Facebook are served to users by third party advertisers, who receive the user's IP address and "may download cookies to the user's computer or use other technologies such as JavaScript or 'web beacons' … to measure the effectiveness of their ads and to personalize advertising content."[119]

Facebook has also created a number of programs to allow businesses to customize their presence on Facebook to target specific audiences. The most notorious of these features is Facebook Beacon, released in 2007 and undergoing intense scrutiny by privacy advocates and the public. Beacon publishes actions on third party websites owned by partners of Facebook to the user's newsfeed, thus broadcasting the user's internet activity to the user's friends.[120] Partners would determine the most relevant set of actions from their sites to distribute onto the Facebook newsfeed, such as a high score on a game, a purchase, posting an item for sale or viewing a video.[121] Beacon was criticized for imposing an opt-out regime rather than an opt-in system and a month after its rollout, Facebook changed the consent requirements to opt-in and added a privacy control, allowing users to turn off the feature. In August 2008, a class action lawsuit was filed in California against Facebook, alleging that Facebook and its Beacon affiliates violated a series of laws.[122] The lawsuit settled in September 2009 when Facebook discontinued Beacon.

In conjunction with the Facebook Beacon program, Facebook rolled out a marketing program called "Social Ads", which allows businesses to set up Facebook profile pages where visitors who take certain actions can trigger sending a "Social Ad" to their network of friends.[123] According to Facebook, Social Ads "[enable] advertisers to deliver more tailored and relevant ads to Facebook users that now include information

---

[117] Becky Ebenkamp, "Behavioral Targeting: A Tricky Issue for Marketers" Brandweek.com (21 October 2008), online: http://www.brandweek.com/bw/content_display/news-and-features/digital/e3i9e2284979c0b8c78ba188179079a495b.

[118] Facebook Ads, online: http://www.facebook.com/ads/?src=gca2.

[119] Facebook's Privacy Policy, *supra* note 116.

[120] Facebook, "Facebook Beacon" online: http://www.facebook.com/business/?beacon.

[121] At its launch, Facebook announced that 44 websites were using Facebook Beacon "to allow users to share information from other websites for distribution to their friends on Facebook" calling it a "new way to socially distribute information on Facebook." Facebook Beacon partners included eBay, Fandango, CollegeHumor, iWon, Blockbuster, Bluefly.com, Joost, LiveJournal, Live Nation, National Basketball Association, NYTimes.com, Sony Online Entertainment LLC, Sony Pictures, TripAdvisor, TypePad and WeddingChannel.com.

[122] The suit alleged that Facebook and its Beacon affiliates violated laws including the *Electronic Communications Privacy Act*, the *Video Privacy Protection Act*, the *California Consumer Legal Remedies Act* and the *California Computer Crime Law*.

[123] CIPPIC notes that Social Ads grew out of an advertising alliance with Microsoft. See Facebook, "Microsoft and Facebook Team Up for Advertising Syndication" (22 August 2006), online: http://www.facebook.com/press/releases.php?p=635.

from their friends so they can make more informed decisions."[124] Social Ads offers more advanced targeting by age, location, gender, interests and more.

Canada's Privacy Commissioner has been a world leader in addressing privacy issues with respect to Facebook. Following a complaint launched by CIPPIC alleging that Facebook violated Canada's private sector data protection law, the Privacy Commissioner investigated several of Facebook's privacy practices, including its advertising practices. In particular, CIPPIC alleged that Facebook:

> (1) was not making a reasonable effort to notify users clearly that it used their personal information for advertising purposes, in violation of Principle 4.3.2;
>
> (2) for Social Ads in particular, was improperly using opt-out rather than opt-in consent in accordance with Principle 4.3.6, given the sensitivity of users' personal information;
>
> (3) was not allowing users to opt out of Facebook Ads, in contravention of Principle 4.3.8; and
>
> (4) since users were not allowed to opt out of Facebook Ads, was unnecessarily requiring users to agree to such ads as a condition of service, in violation of Principle 4.3.3.[125]

The Privacy Commissioner found that because Facebook's business model is premised on obtaining revenues from advertising in order to provide the service free to users, advertising is essential to the provision of the service and persons who wish to use Facebook must be willing to receive a certain amount of advertising.[126] However, the Privacy Commissioner found that users should be able to opt out of active use of their personal information for Social Ads, given that Social Ads are more inherently intrusive in their nature by using the user to endorse a particular product. The Privacy Commissioner recommended that Facebook expand the advertising section of the Privacy Policy to more fully explain the role of advertising in Facebook and users' ability to opt out and inform users of the use of their profile information for targeted advertising

---

[124] Facebook, "Facebook Unveils Facebook Ads" (6 November 2007), online: http://www.facebook.com/press/releases.php?=9176.

[125] Office of the Privacy Commissioner of Canada, "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*" (16 July 2009), online: http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf. See also complaint by CIPPIC, "PIPEDA Complaint: Facebook" (submitted to the Privacy Commissioner of Canada on 30 May 2008), online: http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf.

[126] This finding follows from the Privacy Commissioner's typical distinction between marketing for primary and secondary purposes. A primary purpose is that which is essential to the service, compared to a secondary purpose, which is additional to the information that was needed in the first place. In previous decisions, the Privacy Commissioner found advertising to be a secondary purpose, which users could opt out of in certain circumstances.

purposes.[127] Facebook agreed to describe advertising more clearly and update its ad guidelines.

The Privacy Commissioner's Facebook decision has set a precedent for privacy and data collection, use and disclosure practices of social networking sites. Social networking sites should take notice and assess their own privacy practices for compliance with Canada's private sector privacy legislation and the guidelines set by the Privacy Commissioner.

3.4.2. Advertising on other social networking websites

Many social networking sites have platforms to advertise to their members, leveraging the personal information of their members to reap advertising revenues. As the technology becomes more widespread, social networking sites are starting to recognize the ability of targeted advertising platforms to increase their ad revenues.

For example, Twitter is a relatively new social networking service, providing a real-time short messaging service that works over multiple networks and devices, often described as "micro-blogging." In September 2009, Twitter proposed changes to their Terms of Service to leave the door open for customized, targeted advertising depending on what users are tweeting about. Twitter is currently advertising-free, even though they had to address the issue of spammers sending messages to individual users.[128] Twitter has recently announced it will begin advertising early next year.[129]

The Privacy Commissioner of Canada recently published a comparison of six social networking websites that are popular among Canadians.[130] The six sites under review were Facebook, Hi5, Linked In, LiveJournal, MySpace and Skyrock. All of these sites advertise to their members and most of these sites use targeted advertising, often served by third party advertising companies based on aggregated or anonymous user data such as age, gender and location. Some sites had capabilities to offer targeted advertising based on user-chosen interest categories. In some cases, users were able to opt out of certain technologies being used to process their personal information, such as web beacons, or opt out of information collection by third party advertisers.

---

[127] Facebook findings by the Privacy Commissioner, *supra* note 125 at pp. 37-38.

[128] CTV.ca News Staff, "New Twitter rules leaves ads 'open for exploration'" CTV News (11 September 2009), online: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20090911/twitter_changes_090911/20090911?hub=TopStories.

[129] Financial Times Techblog, "What's happening? A lot, says Twitter COO" (20 November 2009), online: http://blogs.ft.com/techblog/2009/11/whats-happening-a-lot-says-twitter-coo/.

[130] Jennifer Barrigar, "Social Network Site Privacy: A Comparative Analysis of Six Sites" commissioned by the Office of the Privacy Commissioner of Canada (February 2009), online: http://www.priv.gc.ca/information/pub/sub_comp_200901_e.cfm.

3.5. Web bugs

As noted in the KnowPrivacy report, web bugs are small graphics that are embedded in a web page's or e-mail HTML code to enable monitoring of who is reading the page or e-mail.[131] The graphic is usually a single pixel or a transparent image such that it is invisible to the user.[132] Web bugs are also called "web beacons," "gif bugs," "clear GIFs" or "pixel tags." There are two types of web bugs. One type is an executable web bug, which is a file that monitors a machine's traffic and hard drive and periodically sends the information back to the website that planted the bug on the machine. The second type is not physically located on the machine and uses scripts (i.e. JavaScript, ActiveX and Perl) to scan a hard drive searching for files.[133]

Ad networks can use web bugs to aggregate information to create a profile of what sites a user is visiting. The personal profile is identified by the browser cookie of an ad network, allowing the network to track behaviour across sites over time. Web bugs may transmit several pieces of information to a server, including the IP address of the computer that fetched the web bug, the URL of the page where the web bug is located to reveal the content that the user was looking at, the time the web but was viewed, the type of browser the user uses and a previously set cookie value.

In the KnowPrivacy report, data from Ghostery, an add-on for the Firefox web browser, showed that many websites featured multiple web bugs, with some sites containing several dozen web bugs. The two sites with the most web bugs were Blogspot and Typepad.

It can be very difficult to block web bugs. Blocking third party cookies can limit the types of information the web bug can collect, but not all browsers offer this functionality and blocking third party cookies does not remove the web bug since it is part of the website. In addition, web bugs provide advertisers with the capacity to track users without the use of a cookie, as a user's browser will send information such as IP address and URL when requesting the web bug from the advertiser's server.[134] Furthermore, websites' Privacy Policies are often unclear in their disclosure about whether they use web bugs and how these web bugs are used (i.e. what personal information these web bugs collect).

---

131 KnowPrivacy report, *supra* note 10 at pp. 8-9.

132 CIPPIC, "Online Threats to Privacy" report, *supra* note 1 at p. 28.

133 Cary A. Deck & Bart J. Wilson, "Tracking Customer Search to Price Discriminate" 44 *Economic Inquiry* 2 (April 2006) 280-295 at p. 281.

134 Electronic Frontier Foundation, "The Web Bug FAQ" (11 November 1999) online: http://w2.eff.org/Privacy/Marketing/web_bug.html.

PART 4: THE BENEFITS AND HARMS OF ONLINE BEHAVIOURAL TARGETED ADVERTISING AND ONLINE CONSUMER TRACKING

4.1. How online behavioral targeted advertising might benefit the user's experience

Tracking technologies such as cookies have uses that benefit the user, such as remembering customization settings for individual users regarding content and layout. For example, websites can be customized to display news stories that would be relevant and of interest to the user. As well, cookies allow e-commerce sites to implement convenient shopping carts and "quick checkout" options. E-commerce sites can use information collected about users to make product recommendations based on the user's previous purchases or browsing history. The data collected can also be used to develop and improve the website to increase its usability for users and to customize how information is displayed on the website to appeal to a particular user's tastes.

Behavioural advertising provides benefits to consumers in the form of free web content and personalized advertisements. The average web user may also benefit from an array of free services, from Google's Gmail to social networking services such as Facebook, which are partially supported by revenues from advertisements. As well, the general public is able to access newspaper content on the internet for free because they are subsidized by online advertising.

Proponents of online behavioural targeted advertising argue that it provides benefits to consumers, by displaying more relevant advertisements that reflect the user's interests. Advertising relevancy provides added value to the consumer, as they may receive offers that are of particular interest to them or receive advertisements for products that are tailored to their needs and interests. Tailored advertisements could facilitate comparison-shopping for specific products that can potentially reduce a consumer's search time or exposure to unwanted or unwelcome advertising. Marketers claim that online behavioural targeted advertising will improve the user experience by not repeatedly bombarding the user with the same advertisement.

Professor Eric Goldman suggests that data mining for direct marketing has a private utility for the direct marketing recipient. Goldman argues that the economics of marketing are such that marketing can create negative utility by consuming the recipient's attention. But marketing can also produce positive private and social utility when marketing provides better informed buyers and increased competition. Thus, Goldman posits that data mining can help marketers with targeting such that recipients would only receive substantive utility positive messages from marketer, resulting in an increase in social welfare.[135]

---

[135] Eric Goldman, "Data Mining and Attention Consumption" in Eric Goldman, *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, Springer (2005), online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=685241.

4.2. The harm of online behavioral targeted advertising and online tracking

While consumers may value the benefits provided by behavioural targeted advertising, the surveys suggest that few consumers fully understand the role and extent that data collection plays in providing these ads. This is largely attributed to the lack of transparency and consumer autonomy, which are critical to the development and maintenance of consumer trust in the online marketplace. This raises a general concern about the purpose of consumer data collection and the threat of unanticipated and unwelcome uses of such information.

4.2.1. Consumer awareness: notice and transparency

Consumers are not fully aware of the tracking technologies and degree of user tracking that is performed on the internet while they are engaging in online activities.[136] If companies and website operators actually disclose information about their tracking practices, explanations are often placed in the Privacy Policy or Terms of Use of a website which are not necessarily an effective mechanism for consumer notice and disclosure of tracking practices.

There are several reasons that privacy policies are ineffective, which were discussed in the KnowPrivacy report.[137] First, these polices are often difficult to read because of the use of legal jargon and often, consumers do not bother to read them. Second, a 2008 study found that consumers "do not read privacy policies because they believe that they do not have to; to consumers, the mere presence of a privacy policy implies some level of often false privacy protection."[138] Third, the time required to read privacy policies is too great. Fourth, even if consumers could understand and had the time to read privacy policies there is not enough market differentiation for users to make informed choices.[139] Many privacy policies are vague about what information they collect and how it is used. Finally, the potential privacy dangers are not salient to most users.

Because privacy policies are not effective in informing consumers about what information is collected by the website operator, how this information is used and the purposes for the collection and use of this information, consumers cannot be said to have provided informed and meaningful consent to these practices. Without adequate notice and informed and meaningful consumer consent, consumers have no control over their personal information.

---

136 As far as PIAC is aware, Google is the only online advertising model that displays a notice

137 KnowPrivacy report, *supra* note 10 at pp. 11-12.

138 Chris Hoofnagle & Jennifer King, "What Californians Understand about Privacy Online," Samuelson Law, Technology & Public Policy Clinic (2008), online: http://www.law.berkeley.edu/clinics/samuelsonclinic/files/online_report_final.pdf.

139 In the study by Aleecia McDonald & Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," CyLab, Carnegie Mellon University (2008), the study estimated that if users actually read privacy policies, it would take approximately 200 hours a year to read the policy for every unique website visited in a year, not including policy updates for sites visited on a repeating basis.

4.2.2. Consumer control: opt-in consent and access

Where consumers have a real, prominent and easily understood opportunity to decide about participation, their consent must be sought using clear, non-technical language and terms must not be hidden in the website's privacy policy. Consumers want control over their personal information and they want that control to be individualized. The Internet Advertising Bureau Good Practices Principles specify the default to be an "opt-out" regime: users must actively request that their data not be used for behavioural advertising, and if they say nothing, the default is that they have consented to the use of their personal information for targeted behavioural advertising.

However, opting out is not entirely foolproof. Even where websites provide consumers some control by allowing them to opt-out of receiving targeted advertising from the website or its affiliates, the website may still collect information about the user. For example, Microsoft's opt out policy is clear that the user cannot opt out of the collection of their personal information by Microsoft as opting out only means that the user will not receive targeted personalized advertising. In the case of DoubleClick, where a user opts out of the DoubleClick ad-serving and search cookies, the user will still receive targeted ads based on non-personally identifiable information, such as the user's browser type, internet service provider, information about the general content of the site or page displayed in the browser and other non-personally identifiable information provided by the site.[140] Other opt-out policies are simply vague as to whether opt-out is limited to the receipt of targeted advertisements. Further, opt out is rarely permanent, as the opt-out setting may be deleted if the user clears his or her cookie file or updates their browser.[141] All too often, opt-out schemes are confusing and not friendly to consumers. For example, Yahoo's opt-out scheme requires the user to contact each of its third party ad network's websites individually and opt out, if that network offers that capability.

Furthermore, data mining threatens the consumer's ability to control the flow of their personal information, as personal information has different privacy implications from one social context to another. Data mining involves the purchase, sale and trade of so-called public data for use in new contexts – for the purpose of this paper, for the context of delivering more targeted advertising to an individual internet user with the aim of producing a deliverable, often in the form of a sale. Consumers rarely realize that commercial bartering of their personal data is a blossoming and lucrative industry.

---

[140] DoubleClick, "DART Ad-Serving and Search Cookie Opt-Out", online: http://www.doubleclick.com/privacy/dart_adserving.aspx.

[141] Note that Google built their tool for persistent opt-out and open sourced it so that anyone could build their own, working with the Electronic Frontier Foundation. See: http://www.eff.org/deeplinks/2009/03/google-begins-behavioral-targeting-ad-program. The Advertising Cookie Opt-out Plugin can be found here: http://www.google.com/ads/preferences/plugin/. Also note that after opting out, users should close their browser and reload the Ads Preferences Manager page to ensure opt out.

Finally, data mining does not always collect accurate information about individuals.[142] Where errors are collected and inputted as part of a consumer's profile, targeted online advertising may be based on these errors and negatively affect the user's online experience. Consumers may not even realize that there are errors in their profile, as they may have difficulty accessing database records or it may be to correct accurate information.

Philippa Lawson summarizes additional consumer concerns regarding accuracy and transparency:

> … [e]ven if no single company's data collection or profiing activities is sufficiently invasive to attract public censure, the cumulative effect of all this ["Customer Relationship Management"] activity is to strip individuals of privacy and control over their personal information. Consumers are exposed not only to endless direct marketing pitches, but also to identity theft and other informational abuses. Research also suggests that the information in consumer profiles is often riddled with errors. Yet important decisions are made on the basis of this information by employers, insurance companies, governments and others. Such decision [*sic*] are made without the individual's knowledge and thus without any opportunity for them to explain, to correct inaccurate information, or to expose decision-making based on prejudice or misinterpretation.[143]

4.2.3. Aggregation, disclosure and selling to third parties

As mentioned earlier, site operators often sell or rent personal and behavioural data about users to third parties or share this information with their marketing partners or corporate affiliates and subsidiaries to build more full profiles about individual consumers.[144] It is often unclear what a website means by the terms "affiliate," "third party" and "partner" as no definitions are provided. The KnowPrivacy report analysis of privacy policies found that:

---

[142] Tal Z. Zarsky, "Mine Your Own Business!: Making the Case for the Implications of Data Minng of Personal Information in the Forum of Public Opinion" 5 Yale J.L. & Tech. 1 (2002-2003) at pp. 47-48.

[143] Philippa Lawson, "Techniques of Consumer Surveillance and Approaches to their Regulation in Canada and the USA" (March 2005), online: http://www.idtrail.org/index2.php?option=com_content&do_pdf=1&id=110 at p. 7. Lawson cites the testimony of Marc Rotenberg, President, EPIC, before a committee of the USA House of Representatives, in a hearing on "Protecting Consumer's Data: Policy Issues Raised by ChoicePoint" (15 March 2005) at pp. 2-3, online: http://www.epic.org/privacy/choicepoint/testimony3.15.05.pdf. Examples of abuses are documented on the Privacy Rights Clearinghouse website at http://www.privacyrights.org/cases/index.htm#3.

[144] For example, companies like Acxiom and Experian use cookies on their affiliate websites to gather data about users that surf their sites and sell this information to advertising networks to add to these networks' profiles about users. For example, data that these companies sell include income level, interests, age and gender. See Stephanie Clifford, "Your Online Clicks Have Value, for Someone Who Has Something to Sell" New York Times (25 March 2009), online: http://www.nytimes.com/2009/03/26/business/media/26adco.html.

> … many stated that they do not share data with third parties, but they do share data with affiliates, suggesting that they only share data with companies under the same corporate ownership. However, many of these websites also allow third parties to track user behavior directly through the use of web bugs. In a conversation with one of the website's Chief Privacy Officer, he claimed that they consider the advertising serving company DoubleClick to be a "marketing partner," and not a third party.[145]

Without providing a definitive distinction between the types of parties with whom the website may share personal information of its visitors, consumers do not know the extent to which their personal information has been shared with other companies.

Besides sharing personal information about their visitors, website operators can purchase more data about consumers in order to build better profiles, a practice referred to as data mining. For example, ChoicePoint based their business model on the aggregation and selling of personal information by acquiring information from public records. In the KnowPrivacy report's analysis of privacy policies, they found that "about a quarter of the websites expressly stated that they buy information about users from third parties to supplement data collected directly from their users."[146]

4.2.4. "Anonymization" of data

Marketers and market researchers often attempt to quell privacy concerns by stating that they anonymize the data in their databases. To anonymize the data, details such as name, phone number and e-mail addresses may be stripped from the database. However, studies have shown that anonymized information about a user's online history can be "de-anonymized" to identify users using publicly available data. In the most recent example, anonymized information about the film preferences of Netflix customers combined with digital trails left on blogs, chat rooms and Twitter were used to positively identify Netflix customers.[147] In a previous example, anonymized AOL search queries were used to identify individuals and their search patterns.

---

145 KnowPrivacy report, *supra* note 10 at p. 9.

146 *Ibid.* at p. 9.

147 Natasha Singer, "When 2+2 Equals a Privacy Question" The New York Times (18 October 2009), online: http://www.nytimes.com/2009/10/18/business/18stream.html?_r=3&adxnnl=1&adxnnlx=1256572818-Q9UvohAQV7pfxZ1TkU/C+Q.

4.2.5. Discrimination

"Profiling" is a tool to facilitate the practice of discrimination, as vendors have the ability to discriminate between consumers based on their profile. This discrimination could include creating a pricing scheme tailored to each customer by offering a different basket of services to distinctive groups of clients or by avoiding certain customer based on their purchase histories.[148] Profiling methods can result in harm to poorer sections of the population and vulnerable consumers, who might be neglected or avoided based upon their personal information.

Britain's competitive watchdog, the Office of Fair Trading (OFT), has expressed a concern that consumers could suffer if information about their personal web usage is used to set the price they are offered for a particular service or product, especially if consumers are not aware this is happening. OFT is conducting tow market studies into websites using behavioural data to set customized pricing, where prices are individually tailored using information collected about the user's behaviour. The OFT hopes to finish its investigation into online advertising and pricing by spring 2010.[149]

4.2.6. Loss of consumer autonomy

Though Professor Goldman believes that data mining can be used to benefit direct marketers and increase the social welfare of direct marketing messages, privacy and consumer advocates generally agree that data mining can produce very dangerous social impacts and threaten consumer privacy. Predictive data mining relies on Knowledge Discovery in Databases (KDD) for their resulting data, often searching for psychological profile information. The theory is that an individual's underlying psychological properties (i.e. the individual's beliefs, desires or intentions) are the causal roots of action production, thus an individual's underlying beliefs, desires and intentions combine to motivate purchases and mouse clicks. This information then, is the "holy grail" of psychological profiling through predictive data mining.[150] According to Jason Millar, this predictive data mining has the potential to violate our core privacy because the emergent data attempts to outline an individual's beliefs, intentions and desires.[151]

Zarsky highlights the concern that data mining practices manipulate and threaten consumer and societal autonomy, referring to this as the "autonomy trap." Targeted online marketing based on data mining practices will push individuals towards certain products or services in which they were not initially interested by narrowing the options they receive and offering persuasive arguments at the right time to lower the resistance of the consumer.[152] In the broader societal context, thoughts and beliefs would be

---

148 Tal Z. Zarsky, *supra* note 141 at p. 22.

149 Julia Kollewe, "Office of Fair Trading to probe use of personal data by online retailers" The Guardian UK (15 October 2009), online: http://www.guardian.co.uk/business/2009/oct/15/retail-pricing-tactics-oft-investigation.

150 Millar, *supra* note 27 at p. 111.

151 *Ibid.* at p. 119.

152 Zarsky, *supra* note 141 at p. 38.

directed by pre-sorted information chosen by others in the case where there is not sufficient diversification in the media market.[153] Consumer Focus stated that "[p]rofiling potentially limits the diversity of content, restricting choice and concentrating the market as the tendency to generalize may lead to a diminution of preferences, differences and values."[154]

4.2.7. Abuses and misuses of consumer information

Data mining could lead to abuses and misuse of information, for example, publication of personal information counter to the will of the relevant person, use by the holder without consent by the relevant person, and cause embarrassment. While there are legal tools to provide partial protection or recourse against these practices, they do not always prove effective.[155] One particular concern is with data security, where breaches of the database could lead to harmful actions against individuals, such as identity theft or fraud.

4.2.8. Concerns with sensitive information

Data mining enhances marketers' ability to discover hidden traits of their customers and possibly cause them additional distress, leading to seclusion of certain vulnerable consumers. Behavioural targeted advertising could potentially result in the collection of sensitive information, such as health or medical issues, and potentially target the vulnerability of certain users in a way that is not known in traditional commercial arrangements.

4.2.9. Online behavioural targeted advertising to youth and children

Online behavioural targeted advertising is ubiquitous and pervasive throughout the internet. Today, youth are engaging with their peers and society using internet and technological tools, developing social skill and cognitive abilities to manage how they will interact with society at large. Young internet users are an important consumer demographic for marketers because they represent the consumers of tomorrow. Almost every website used by young people is commercial, with content funded by three methods: selling advertising space to third parties who want to target children; selling merchandise direct from the site; and/or collecting children's data to sell to other organizations.[156] Information about how children's online activity is extremely valuable to marketers.[157]

---

153 *Ibid.* at pp. 41-43.

154 All Party Parliamentary Communications Group, *supra* note 94 at p. 13.

155 Zarsky, *supra* note 141 at p. 44.

156 All Party Parliamentary Communications Group, *supra* note 94 at p. 20.

157 The Electronic Privacy Information Center recently filed a complaint to the Federal Trade Commission against Echometrix, the developers of parental control software that monitors children's online activity. The software collects and sells information about how children use the internet and what children are saying on the internet from various sources, including instant messaging conversations, social networking sites and chat rooms. This information is sold to third parties for market intelligence research purposes. The EPIC complaint alleges that Echometrix engages in unfair and deceptive trade

However, children are a vulnerable population and must not be exploited by marketing. With online behavioural targeted advertising technologies, marketers could unduly exploit children and teens' impressionability and susceptibility to peer or social pressures. As the Child Exploitation and Online Protection Centre in the UK noted: "[c]hildren are very often not able to distinguish what is and what is not an advert on the websites that they frequently use. This is epitomized by hidden product placement where advertisement is subtly blended into content."[158]

In the 2008 Annual Report of the Office Privacy Commissioner of Canada, youth privacy was identified to be a key issue requiring better legislation to safeguard youth privacy, as well as further resources and public education initiatives.[159] With increasing numbers of young Canadians actively connecting with friends in the online world, they may not have the time, resources or inclination to consider the impact of how they are sharing information, opinion or gossip. Going forward, the Privacy Commissioner is focused on helping young Canadians develop appropriate information-management practices "to ensure that their personal information is collected by organizations only with their permission, distributed only according to their wishes and used only in ways to which they agree."[160] The Privacy Commissioner also reported that the office was working with their counterparts in the United States in Europe to understand the privacy implications of increased data collection, data mining and behavioural advertising.[161]

While it is encouraging to see the Privacy Commissioner of Canada take youth privacy seriously, the issue of online behavioural targeted advertising directed at youth requires special examination by Canadian regulators. PIAC has previously published a paper on children's privacy on the internet, examining the reality of "immersive advertising" and market surveillance as a business model for social networking services targeting children.[162] The report makes several recommendations, including increasing the readability and simplicity of privacy notices for children and adults and better education of children and parents in online privacy protection and rights. The report also

---

practices by representing that parental control software protects children online without informing parents that this information about their children's online activity is collected and disclosed, thus parents are unaware that this information is sold to third parties. See EPIC's complaint online: http://www.epic.org/redirect/100809_Echometrix.html. EPIC also alleges that Echometrix's practices violate the Children's Online Privacy Protection Act by collecting and disclosing information from children under the age of 13.

158 All Party Parliamentary Communications Group, *supra* note 94 at p. 20.

159 Office of the Privacy Commissioner of Canada, "Annual Report to Parliament, 2008: Report on the *Personal Information Protection and Electronic Documents Act*" Minister of Public Works and Government Services Canada (2009), online: http://www.priv.gc.ca/information/ar/200809/2008_pipeda_e.pdf at pp. 15-19. The Privacy Commissioner launched an educational resource website devoted to helping youth understand privacy on the internet, with a host of resources for parents and teachers, see online: http://www.youthprivacy.ca.

160 Privacy Commissioner Annual Report, *ibid.* at p. 17.

161 *Ibid.* at p. 18.

162 For more information and analysis of children's privacy online, please see PIAC publication by John Lawford, "All in the Data Family: Children's Privacy Online" (September 2008), online: http://www.piac.ca/files/children_final_small_fixed.pdf. This paper reviewed the privacy risks posed to children when commercial entities target children through their personal information on the internet.

recommends that Canadian privacy law be amended to add specific rules in relation to the protection of children's privacy. The paper advocates for a general prohibition on the collection, use and disclosure of all personal information of children under the age of 13.

In Canada, there is currently a voluntary Code of Ethics by the Canadian Marketing Association that stipulates special considerations for marketing to children and teenagers. The Code of Ethics requires companies who collect any personal information from children under 13 to obtain opt-in consent from the child's parent or guardian. For teenagers between 13 and 15, the collection of personal information beyond contact information requires opt-in consent from both the teenager and the parent or guardian. Teenagers aged 16 and over must consent to the collection of their personal information, however, a parent or guardian can withdraw consent to use or disclose the teenager's personal information.[163] This Code is voluntary and not all online Canadian businesses follow them. It would be very unlikely that non-Canadian online businesses follow these practices with respect to marketing to children. However, the Code of Ethics is meant to be general and does not specifically address challenges of modern targeted online behavioural marketing strategies and how children use the internet. Guidance from the CMA for online behavioural marketing is some way off.

On the international front, the British All Party Parliamentary Communications Group has examined the issue of behavioural advertising and expressed great concern with the deployment of behavioural advertising systems without sufficient consideration given to protecting the interests of children and young people. The Communications Group stated that the matter requires urgent consideration and recommended that the UK Council for Child Internet Safety consider how behavioural advertising that is aimed at children and young people should be regulated.[164]

While there have been efforts to regulate online behavioural targeted advertising in the United States, the marketing industry has been very resistant of any regulation efforts and has advocated for industry self-regulation in this area. Efforts to regulate online behavioural targeted advertising in Europe and in the United States have been met with intense lobbying from the marketing industry and technology innovators. Websites and online marketers have a very lucrative incentive to collect and share data about their users. This incentive should be balanced by the market and consumer choice, but users in the context of online behavioural targeted advertising, users are unable to make informed decisions based on the notice explanations provided in privacy policies.

---

[163] Canadian Marketing Association Code of Ethics and Standards of Practice, online: http://www.the-cma.org/?WCE=C=47|K=225849.

[164] All Party Parliamentary Communications Group, *Supra* note 94 at p. 21.

PART 5: PROPOSAL FOR A "DO NOT TRACK LIST" IN THE UNITED STATES

5.1. History of regulatory action and complaints about online targeted behavioural advertising and online tracking

Since the 1990s, the Federal Trade Commission (FTC) in the United States has engaged in investigations, law enforcement, studies and other policy developments to protect consumer privacy in the online environment. Currently, the collection, use, maintenance and disclosure of personal and behavioural information for marketing purposes are largely self-regulated by the Network Advertising Initiative (NAI), which will be discussed below. The rapid expansion of behavioural tracking and targeting of consumers through the internet and other networked devices have led many to question the effectiveness and adequacy of protection for consumers' privacy rights.

The Electronic Privacy Information Centre first launched a complaint to the FTC against DoubleClick in 2000, alleging that DoubleClick engaged in unfair and deceptive trade practices by tracking the online activities of internet users and combining the tracking data with detailed personally identifiable information contained in a massive, national marketing database.[165] The FTC concluded that the company never actually used or disclosed personally identifiable information in violation of its privacy policy. The FTC noted DoubleClick's commitment to abide by self-regulatory guidelines for online profiling.

In June 2004, the Federal Trade Commission (FTC) presented a report on a "Do Not Email Registry" to the United States Congress. The report addressed the problem of spam, explaining practical and technical obstacles and also addressed privacy and security concerns regarding the implementation and operation of a "Do Not Email Registry" in the United States based on consultation and interviews with various stakeholders. The FTC concluded that the implementation of a "Do Not Email Registry" would not reduce the volume of spam, given the current technologies to authenticate the origin of email messages. Thus, the Commission proposed a program to encourage the widespread adoption of email authentication standards to help law enforcement and ISPs better identify spammers.[166]

In November 2006, the Center for Digital Democracy (CDD) and the United States Public Interest Research Group (USPIRG) filed a joint complaint to the FTC regarding unfair and deceptive online marketing practices.[167] The complaint details online

---

[165] Electronic Privacy Information Centre, "Before the Federal Trade Commission in the Matter of DoubleClick Inc., Complaint and Request for Injunction, Request for Investigation and for Other Relief" (10 February 2000), online: http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

[166] Federal Trade Commission, "National Do Not Email Registry: A Report to Congress" (June 2004), online: http://www.ftc.gov/reports/dneregistry/report.pdf.

[167] Center for Digital Democracy & United States Public Interest Research Group, "Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practice" (submitted to Federal Trade Commission on 1 November 2006), online: http://www.democraticmedia.org/files/FTCadprivacy_0.pdf.

advertising and online tracking practices. The groups requested an inquiry into new online advertising practices, focusing on five areas of concern: 1) user tracking and web analytics; 2) behavioural targeting; 3) audience segmentation; 4) data gathering and data mining; and 5) industry consolidation. In response to this joint complaint, the FTC held a three-day public hearing called "Protecting Consumers in the Next Tech-ade" to examine anticipated technological developments that could raise consumer protection policy issues over the next decade. Online behavioural advertising received considerable attention at the hearing.

Behavioural targeted advertising received regulatory attention again in the summer of 2007 when public interest groups filed complaints against the Google/DoubleClick merger, as discussed above. Following these complaints, the FTC hosted a Town Hall entitled "Ehavioral Advertising: Tracking, Targeting, and Technology" in November 2007 to continue the dialogue and debate over specific key issues relating to online behavioural advertising. Special attention was paid to the issues of what consumers know about the practice, whether consumer disclosures in the area are necessary and effective, how data collected for behavioural advertising is used and protected and what standards currently exist or should exist to govern the practice.

5.2. The "Do Not Track List" proposal

In November 2007, nine public interest advocacy groups in the United States jointly recommended that the FTC create a "Do Not Track List" that would function much like the "Do Not Call" list.[168] The proposal urged the FTC to take proactive steps to protect consumers as online behavioural tracking and targeting become more ubiquitous. The public interest groups emphasized the need for consumer choice, adequate disclosure to consumers, and meaningful consumer consent.

The groups then proposed the creation of a "Do Not Track List." The List would target websites who used persistent identifiers, not all advertisers. Thus, consumers would still receive some advertisements.

---

[168] "Privacy and consumer groups recommend 'Do Not Track List' and other policy solutions to offer consumers more control over online behavioral tracking" (press release by the Center for Democracy & Technology on 31October 2007), online: http://www.cdt.org/press/20071031press.php. "Consumer Rights and Protections in the Behavioral Advertising Sector" (letter to the Federal Trade Commission on 31 October 2007), online: http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf. Signatories on the proposal were the Center for Democracy & Technology, Consumer Action, Consumer Federation of America, Electronic Frontier Foundation, Privacy Activism, Public Information Research, Privacy Journal, Privacy Rights Clearinghouse, and World Privacy Forum.

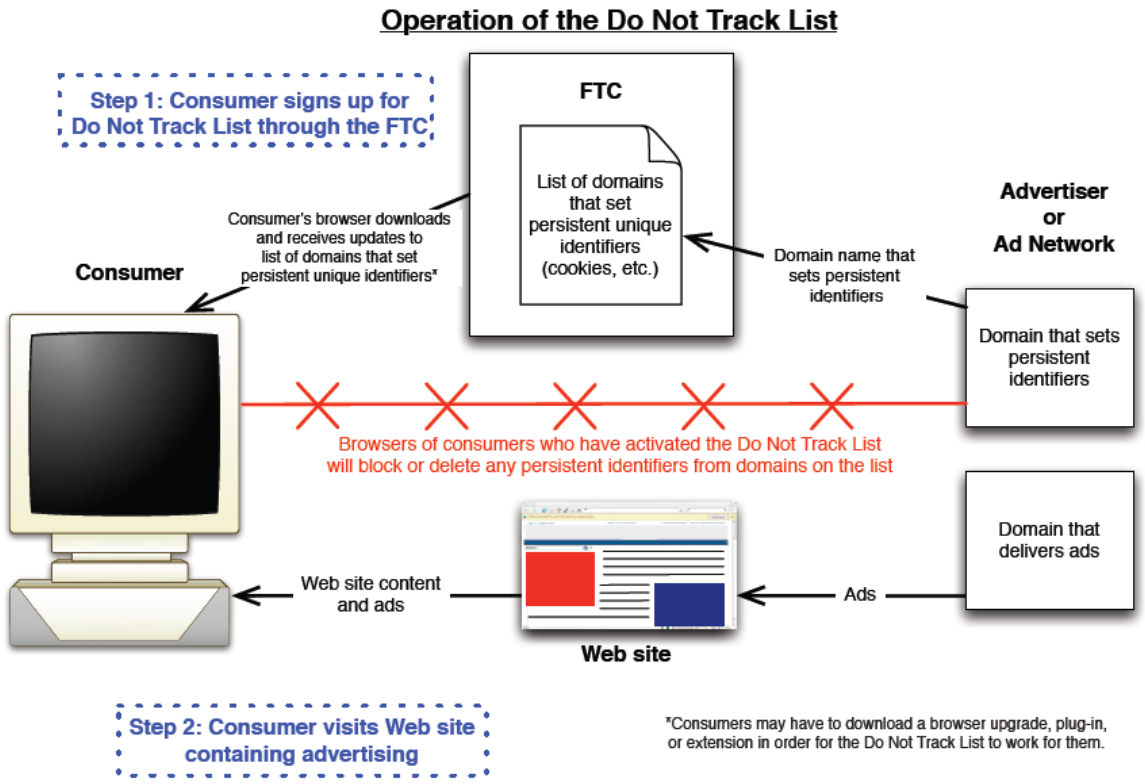

Figure 3: An illustration of how the "Do Not Track List" would work[169]

The coalition of consumer groups advocated for several components to the Do Not Track List, including:

- Any advertising entity that sets a persistent identifier on a user device should be required to provide to the FTC the domain names of the servers or other devices used to place the identifier;
- Companies providing web-based applications should provide functionality that allows users to import or otherwise use the Do Not Track List of domain names, keep the list up-to-date, and block domains on the list from tracking their internet activity;
- Advertisements from servers or other technologies that do not employ persistent identifiers may still be displayed on consumers' computers so that consumers who sign up for the Do Not Track List would still receive advertising;
- The Do Not Track List should be available on the FTC Website for download by consumers who wish to use the list to limit tracking;
- The FTC should educate the public and disseminate information relating to the Do Not Track List broadly to consumers, along with instructions for its use; and
- The FTC should actively encourage all creators of browsing and other relevant technology to incorporate a facility that will enable consumers to use the list.[170]

169 Center for Democracy & Technology, online: http://www.cdt.org/privacy/20071031donottrack.pdf.

170 Electronic copy of a letter submitted to the FTC by the consumer groups is available at http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf.

The proposal also made several other recommendations, such as: providing more robust disclosures to consumers about behavioural tracking; independent auditing of those engaged in behavioural tracking to ensure adherence to privacy standards; providing consumers with access to the personal information advertisers collected about them; prohibiting advertisers from collecting and using personal information about health, financial activities and other sensitive data; and establishing a national "Online Consumer Protection Advisory Committee."

5.3. Initiatives related to the "Do Not Track List" proposal since 2006

5.3.1. The Network Advertising Initiative Code of Conduct for Online Behavioural Advertising

The Network Advertising Initiative (NAI) is an American cooperative of online marketing companies "committed to building consumer awareness and establishing responsible business and data management practices and standards."[171] The NAI published self-regulatory measures for online advertising in 2000 and updated the self-regulatory Code of Conduct for Online Behavioural Advertising in 2008, which addresses new advertising solutions and business models for third party advertising on the internet.[172] The NAI Code defines "online behavioural advertising" to mean "any process used whereby data are collected across multiple web domains owned or operated by different entities to categorize likely consumer interest segments for use in advertising online."[173]

The NAI Code of Conduct stipulates fair information practices for "personally identifiable information" such as transparency, notice, choice, use limitation, transfer and service restrictions, access, reliability and security.[174] NAI members are required to maintain a website to offer explanations of online behavioural advertising and information about and centralized access to consumer choice mechanisms.[175] As well, each member is required to post "clear and conspicuous" notice describing their data collection and use practices on their website.[176] Consumer choice is also a priority, requiring a consumer opt-out mechanism for the use of non-personally identifiable information.[177] The NAI Code of Conduct covers online behavioural advertising, such as the standard process of collecting information about a particular user's surfing habits to deliver targeted third-party advertising to a specific individual.

---

171 Network Advertising Initiative, online: http://networkadvertising.org/about/.

172 Network Advertising Initiative's Self-Regulatory Code for Conduct for Online Behavioral Advertising (2008), online: http://networkadvertising.org/networks/NAI_Principles_2008_Draft_for_Public.pdf.

173 Draft NAI Code of Conduct, *ibid.* at II.1.

174 Draft NAI Code of Conduct, *ibid.* at III.

175 Draft NAI Code of Conduct, *ibid.* at III.1.

176 Draft NAI Code of Conduct, *ibid.* at III.2.a.

177 Draft NAI Code of Conduct, *ibid.* at III.3.a.i.

The NAI Code of Conduct has been vehemently criticized by public interest advocates. The CDT published a response to the NAI Code of Conduct in December 2008, welcoming the development but criticizing the Code for falling short on opt-out requirements, the notice standard, the NAI member accountability model, failing to address ISP behavioural advertising, lack of a choice requirement for multi-side advertising and the data retention principle. As well, the NAI Code failed to provide a long-term plan for user controls.[178]

Similarly, Pam Dixon of the World Privacy Forum published an article discussing the FTC and industry agreement on self-regulation of online advertising.[179] Dixon argues that the NAI has lulled regulators into thinking that self-regulation effectively addresses the interests of consumers in the area of targeted behavioural advertising.

5.3.2. Congressional hearings on privacy, online advertising, behavioural advertising and deep packet inspection

In July 2008, the Senate Committee on Commerce, Science and Transportation convened a full hearing regarding the privacy implications of online advertising. While a number of interests were represented at the hearing, ISPs were notably absent.

The FTC testified that privacy concerns regarding online advertising could be addressed adequately by industry self-regulation adhering to the FTC's proposed guidelines. According to Lydia Parnes, Director of the Bureau of Consumer Protection at the FTC, self-regulation is preferable because it affords the flexibility for innovative and evolving business models. Leslie Harris, President and CEO of CDT testified in favour of stronger guidelines for behavioural advertising, noting that while the practice of behavioural advertising is growing, consumers are increasingly uncomfortable with it and are unable to take meaningful steps to protect their privacy.

Following the Senate hearings, the U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet convened a hearing on behavioural advertising focusing specifically on deep packet inspection (DPI) technologies. While there was disagreement on how to protect user privacy, legislators generally agreed that "consumers should have to actively agree to have their online surfing information tracked by ISPs" – that is, that the only legal way to engage in DPI and behavioural advertising practices was to require opt-in consent by consumers.[180] However, the evidence at the hearings suggested that most companies traditionally provide their customers with notice in a privacy policy or a terms of use agreement that allows the company to use personal information unless the specific user

---

[178] Center for Democracy & Technology, "Response to the 2008 NAI Principles: The Network Advertising Initiative's Self-Regulatory Code of Conduct for Online Behavioral Advertising" (16 December 2008), online: http://www.cdt.org/privacy/20081216_NAIresponse.pdf.

[179] Pam Dixon, "The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation" World Privacy Forum (2 November 2007), online: http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

[180] Ronald W. Del Sesto, Jr. & Jon Frankel, "How Deep Packet Inspection Changed the Privacy Debate" (September 2008), online: http://www.bingham.com/Media.aspx?MediaId=7514.

does not consent to such use. At the moment, standard industry practice remains as opt-out consent by consumers.

These behavioural advertising hearings also brought in technical testimony regarding how DPI works, raising concerns that DPI technology involves the inspection of end-user to end-user information content, decoding and the making of inferences about users' personal interests, private activities, health information and other personal details that many people would not willingly allow access to for advertising purposes.[181]

Following the House hearings, the Subcommittee sent letters to 34 companies inquiring about their online advertising activities and practices. Letters were sent to ISPs and online search engines and the following summarizes their responses:

> … six of the recipients had either trialed or implemented DPI. Typically, these companies updated their privacy policies or terms of use to obtain consumer consent to the practice, i.e., they followed an opt-out regime. But 24 of the recipients either did not track their consumers online activity at all or did so only among the websites they owned or controlled. Three recipients disclosed that they track their users among various websites, not just ones they own or control, but do not engage in DPI. The balance indicated that they have considered various forms of online advertising but do not currently engage in any form of online tracking.[182]

On June 18, 2009, the Communications and Consumer Protection Subcommittees held a joint hearing on behavioural advertising, announcing their intention to introduce legislation related to online advertising and online behavioural advertising in particular in the coming year. In the opening statement, Chair Rick Boucher stated:

> I believe consumers are entitled to some baseline protections in the online space:
>
> - Consumers should be given clear, concise information in an easy-to-find privacy policy about what information a website collects about them, how it is used, how it is stored, how long it is stored, what happens to it when it is no longer stored and whether it is given or sold to third parties.
> - Consumers should be able to opt out of first party use of the information and for its use by third parties or subsidiaries who are part of the company's normal first party marketing operations, or without whom the company could not provide its service.

---

181 *Ibid.* at p. 6.

182 *Ibid.* at p. 7.

- Consumers should be able to opt in to use of the information by third parties for those parties' own marketing purposes.[183]

Several online companies appeared before Congress to defend their policies, such as Google, Yahoo! And Facebook. Ten public interest groups, such as the Center for Digital Democracy, the Electronic Frontier Foundation and the Consumers Union, voiced concerns about the amount of data collected and what might be happening with the data behind the scenes. On September 1, 2009, the advocacy groups released a series of guidelines for legislators considering regulations on behavioural advertising, calling for a clear definition of what constitutes sensitive personal data, greater transparency in companies online behavioural advertising practices, a 24 hour limit on how long companies are allowed to collect and use internet user data for, and giving internet users more control over how the data is used.

5.3.3. Behavioural advertising and tracking in the mobile marketplace

As mobile technology advances and key product launches roll out in the marketplace, more attention has been drawn to the mobile platform, as third party mobile advertisements provide a lucrative new source of revenue for mobile operators. The United States is currently the largest single market for mobile advertising, with eMarketer estimating the total US market for mobile advertising to reach $6.5 billion by 2012. eMarketer projects that worldwide spending on mobile advertising will reach a total of $19 billion in 2012, with the vast majority of this spent on text-messaging campaign, with mobile display advertising and mobile search making up the rest.[184] Mobile marketing represents a vast potential resulting from the operator's intimate knowledge of each subscriber profile and its ability to reach the user via multiple channels and leverage trusted one-on-one relationships.[185]

In January 2009, the CDD and USPIRG filed a joint complaint to the FTC requesting an inquiry and injunctive relief concerning unfair and deceptive mobile marketing practices.[186] This complaint stemmed from growing frustration with the FTC's Town Hall

---

[183] Comments of Congressman Rick Boucher to the Communications, Technology and the Internet and Commerce, Trade and Consumer Protection Subcommittee Joint Hearing on Behavioural Advertising Industry Practices and Consumers' Expectations (18 June 2009), online: http://www.boucher.house.gov/index.php?option=com_content&task=view&id=1724&Itemid=.

[184] Interactive Advertising Bureau, "April 2008 Mobile Marketing" by eMarketer, online: http://www.iab.net/insights_research/947883/1675/256587.

[185] Comverse Hub Value Added Services, "Mobile Advertising", online: http://www.comverse.com/product_families.aspx?domain=137. Comverse is a company offering software and systems for value-added services for voice, messaging, mobile internet and mobile advertising. Comverse published a White Paper, "The Operator's Role in Mobile Advertising", online: http://www.comverse.com/data/uploads/products/White_paper_The_Operators_Role_in_Mobile_Advertising_Final.pdf.pdf which encourages mobile operators to take advantage of key valuable assets they hold, such as subscriber knowledge, their subscriber relationship, real-time triggers, various mobile communication channels and real-time metrics.

[186] Center for Digital Democracy & United States Public Interest Research Group, "Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices"

meeting in May 2008, entitled “Beyond Voice: Mapping the Mobile Marketplace” in which several concerns were raised with consumer data collection, profiling, and behavioral targeting techniques in the mobile marketplace.[187] The joint complaint details several behavioural targeted marketing applications deployed by a number of mobile marketers in the United States. As well, the complaint describes location-based capabilities and targeted advertising with technology on mobile devices and goes on to describe "the many faces of mobile targeting" such as contextual targeting, device targeting, time-based targeting and demographic targeting giving marketers plenty of opportunities to breach consumer privacy.[188]

These technologies also allow marketers to track individual users and analyze mobile analytics in a manner in which certain demographics can be profiled. For example, the complaint states that US English-speaking Hispanics with mobile communication devices outpace other consumer segments in voice and data usage. Marketers are well aware of these data and several marketing initiatives have been implemented to specifically target the Hispanic population. For example, mobile marketing agency HipCricket partnered with Bustos Media and Lotus Media to create a national Hispanic-targeted digital advertising network for radio and television broadcasters.[189] Similarly, targeted advertising campaigns have rolled out that specifically target teenagers.

As well, mobile marketers now have the technological capability to data mine like never before. As stated in the *International Journal of Mobile Marketing*: "Every mobile user has a unique phone number, a known address, and an identified sex, which makes it easy to identify them as a segment. This level of detail has never been available in any previous media."[190]

These mobile marketing practices raise several privacy concerns for consumers and CDD and USPIRG argue that mobile software developers often use unfair and deceptive practices to ensure that their data gathering practices are invisible to the consumer. CDD and USPIRG requested that the FTC require true notice that data is being collected and full disclosure about how that data will be used. Consumer consent must be meaningful. As well, the groups requested that the FTC review industry self-regulation for various mobile marketing standards and protect youth from unfair or deceptive practices.

An additional privacy concern raised with mobile technology is the added dimension of the collection and use of locational data. For example, an American startup called Sense Networks examines the movements of cell phone users tracked by global

---

(submitted to the Federal Trade Commission on 13 January 2009), online: http://www.democraticmedia.org/current_projects/privacy/analysis/mobile_marketing.

187 Federal Trade Commission Town Hall, “Beyond Voice: Mapping the Mobile Marketplace” (May 6-7, 2008), Washington, D.C., online: http://www.ftc.gov/bcp/workshops/mobilemarket/index.shtml.

188 CDD/USPIRG mobile marketing complaint, *supra* note 184 at pp. 17-18.

189 *Ibid.* at pp. 30-31.

190 *Ibid.* at p. 42.

positioning systems by cell towers that catch their signals.[191] Phone companies and advertisers provide Sense with raw data on people's movements and behaviours. Sense then transforms this data into intelligence about what individuals will most likely buy or where they will be when a craving hits: Sense predicts people's preferences by movements. Mobile data, then, adds another dimension to researchers to fine-tune transit systems. As mobile technology pushes ahead, location-specific behaviourally targeted marketing on mobile devices seems to be the next logical step for marketers.

5.3.4. Federal Trade Commission "Self-Regulatory Principles for Online Behavioural Advertising"

There are currently no U.S. federal laws specifically governing behavioral advertising, nor is there a comprehensive federal general privacy law.[192] The United States follows a sectoral model for privacy regulation, where certain sectors or business models of the economy are regulated. E-commerce is largely governed by two laws – the Children's Online Privacy Protection Act of 1999 and the growing "common law" or privacy created by the Federal Trade Commission enforcement actions.[193] However, "[t]he U.S. House Subcommittee on Communications, Technology and the Internet hope to this year introduce legislation related to online advertising, particularly behavioral advertising, and the 2002 Consumer Privacy Protection Act will be the foundation for the new legislation."[194]

In the meantime, self-regulation plays a major role in US privacy protections. In February 2009, the FTC published its staff report on "Self-Regulatory Principles for Online Behavioral Advertising". The guidelines tweaked four of the Fair Information Practices[195] to emphasize different facets particular to behavioural advertising:

1) transparency and consumer control;
2) reasonable security, and limited data retention, for consumer data;
3) affirmative express consent for material changes to existing privacy promises; and

---

191 Stephen Baker, "Mapping a New, Mobile Internet" BusinessWeek (29 February 2009), online: http://www.businessweek.com/print/magazine/content/09_10/b4122042889229.htm.

192 Congressman Bobby L. Rush, (June 18, 2009), online: http://energycommerce.house.gov/Press_111/20090618/rush_open.pdf.

193 15 U.S.C. § 6501-6506.

194 "Behavioral-Ad Restriction Coming?" Privacy Journal, May 2009 Volume 35, Number 7.

195 The FTC Fair Information Practice Principles (FIPs) are a set of guidelines for data collecting entities to make their practices more protective of consumer privacy. The FIPs consist of five core principles: notice, choice, access, security and enforcement. The first four are designed to enhance consumer awareness of data collection and enable consumers to control what their data is used for, to see what data has been collected and to ensure that the data collected is correct and secure. The enforcement principle suggests that some method of enforcement be used either through industry self-regulation or governmental regulation through private remedies or civil/criminal sanctions.

4) affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising.[196]

As well, consent for sensitive data such as health information was also given its own emphasis. The FTC Self-Regulatory Principles for Online Behavioral Advertising has been criticized for failing to include a principle for enforcement or accountability.[197]

In June 2009, the FTC sent a letter to two subcommittees of the House of Representatives with its report on behavioural advertising and consumer privacy protections in this area. Recently, the FTC has become increasingly vocal, expressing concerns about the use of targeting and how company practices are deceptive, providing inadequate notice to consumers and preventing consumers from making informed choices about sharing information.[198] The FTC warns that if the industry does not do a better job at explaining their practices and what they are doing with consumer data and giving consumers a choice, they would advocate for a regulatory approach.

[196] Federal Trade Commission, "FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising" (February 2009), online: http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[197] KnowPrivacy report, *supra* note 10 at p. 12.

[198] Douglas MacMillan, "The FTC Takes On Targeted Web Ads" BusinessWeek (2 August 2009), online: http://www.businessweek.com/technology/content/aug2009/tc2009082_486167.htm.

Timeline of Online Behavioural Advertising Complaints and Regulatory Responses	
2000	EPIC complaint to FTC regarding unfair and deceptive practices of Doublelick
June 2004	FTC report on a “Do Not Email Registry” presented to US Congress
November 2006	CDD/USPIRG complaint to FTC regarding unfair and deceptive online marketing practices
	FTC public hearing “Protecting Consumers in the Next Tech-ade”
April 2007	EPIC/CDD/USPIRG complaint to the FTC regarding the Google/DoubleClick merger
June 2007	BEUC complaint to the European Commissioner regarding the Google/DoubleClick merger
August 2007	CIPPIC complaint to the Canadian Privacy Commissioner and Competition Bureau regarding the Google/DoubleClick merger
November 2007	Consumer groups propose a Do Not Track List in the United States
	FTC Town Hall “Ehavioral Advertising: Tracking, Targeting, and Technology”
April 2008	FTC begins discussion on self-regulatory principles for online behavioural advertising
	British Telecom admits that it trialed Phorm’s technology without customer consent, EU commences infringement proceedings
May 2008	FTC Town Hall “Beyond Voice: Mapping the Mobile Marketplace”
	CIPPIC complaint to the Privacy Commissioner regarding Bell Sympatico’s use of deep packet inspection, complaints against other ISPs to follow
June 2008	NebuAd partners with ISP Charter Communications
	CIPPIC complaint to the Privacy Commissioner regarding Facebook
July 2008	Senate Committee on Commerce, Science and Transportation convened full hearing regarding privacy implications of online advertising
January 2009	CDD/USPIRG complaint to the FTC on unfair and deceptive mobile marketing practices
February 2009	FTC publishes report “Self Regulatory Principles for Online Behavioral Advertising”
March 2009	Google launches internet-based advertising service, European Union Consumer Affairs Commissioner threatens EU intervention
May 2009	NebuAd shuts down
June 2009	The House of Representatives Communications and Consumer Protection Subcommittees hold joint hearings on online behavioural advertising
July 2009	Canadian Privacy Commissioner releases decision regarding Facebook privacy practices

PART 6: A "DO NOT TRACK LIST" FOR CANADA?

6.1. Canadian complaints on online behavioural advertising

While the issue of online behavioural targeted advertising has not received the same level of public debate and political scrutiny as in the United States, the issue has been topical for regulatory agencies and among civil society in Canada. As discussed above, CIPPIC has been very vocal on the issue of online behavioural targeted advertising, launching complaints to the Privacy Commissioner regarding the Google and DoubleClick merger in 2007, the use of deep packet inspection technologies by internet service providers in 2008 and Facebook's privacy practices in 2008. These complaints have highlighted a number of privacy issues, including the potential use and privacy concerns with online targeted advertising.

Additionally, CIPPIC has called on the Office of the Privacy Commissioner of Canada to launch an industry-wide investigation with a view to developing industry guideline before the practice of behavioural targeting is entrenched.[199] Behavioural targeting guidelines would be of great value to both consumers and industry, giving credibility to consumers' trust of the internet and also providing greater certainty for businesses to develop business models and technologies compliant with Canadian privacy laws.

However, these Canadian complaints have not spurred the level of heated public discussion and political scrutiny on online targeted advertising practices as seen in the United States and no regulatory action has been seen in Canada.

6.2. Is there a need for a "Do Not Track List" in Canada?

Online tracking and online targeted behavioural advertising affects Canadian consumers and as discussed above, the practices of online tracking are not limited to American companies. Even where the companies are American, Canadian consumers are affected, as they are often part of the intended targeted audience for advertisements in an age of electronic commerce. Canadian ISPs have already begun implementing technologies that would allow them to offer targeted advertising to their customers based on individual customer internet browsing history.

6.2.1. Criminal Code

Canada's *Criminal Code* prohibits the interception of electronic communications without the consent of at least one party to the communication.[200] It is unlikely that this provision would be used to prosecute online targeted advertisers and consumer profilers, as they would require investigative resources of law enforcement agencies

---

[199] CIPPIC to the Office of the Privacy Commissioner of Canada, "Request for an investigation and development of guidelines re: ISP use of Deep Packet Inspection technology for behavioural targeted marketing purposes" (25 July 2008), online: http://www.cippic.ca/uploads/CIPPIC_RequestforIndGuidelines-DPI-BehTarg_25July08.pdf at p. 11.

[200] *Criminal Code of Canada*, R.S.C. 1985, c. C-46, s. 184.

who often have other priorities. As well, the high criminal burden of proof of beyond a reasonable doubt would be difficult to meet, thus prosecution is very unlikely.

6.2.2. Misleading advertising and deceptive business practices

The *Competition Act* prohibits promoting the supply or use of a product or any business interest by making a representation to the public that is false or misleading in any respect.[201] Omission of information can constitute a misleading representation.[202] The Competition Bureau has used these provisions to pursue egregious cases of consumer fraud, but they have not yet held companies accountable for misleading representations regarding consumer privacy.

6.2.3. Privacy and data protection legislation

Canadians often pride themselves in having a legislative framework for private sector data practices in the form of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which governs the collection, use and disclosure of personal information by private sector organizations in the course of commercial activities.[203] Under PIPEDA, organizations cannot collect, use or disclose personal information in the context of commercial activities without the individual's knowledge and consent, except as specified. "Personal information" is defined as any "information about an identifiable individual."[204] This legal definition is notable, as there is no equivalent data protection legislation in the United States, where the term "personally identifiable information" is often used in privacy discussions.

The Privacy Commissioner has previously found that an IP address can be considered personal information if it can be associated with an identifiable individual.[205] Therefore, the use of cookies may mean that the website must comply with the privacy principles in *PIPEDA* if the cookie is used to collect individual's IP address in a manner that can identify the individual.

Furthermore, the Privacy Commissioner has released a finding with respect to informed consent and transparency for the collection of personal information and to use and disclosure of this information by third parties for secondary marketing purposes in a complaint against Ticketmaster Canada.[206] The complainant alleged that customers did not have fair opportunities to provide informed consent to its routine collection of their

---

201 R.S.C. 1985, c. C-24, ss. 52 and 74.01 (criminal and civil provisions).

202 *Misleading Advertising Guidelines* (2001), online: http://strategis.ic.gc.ca/epic/internet/incb-bc.nsf/en/ct01299e.html#g. See also *Application of the Competition Act to Representations on the Internet*, Information Bulletin (18 February 2003), online: http://strategis.ic.gc.ca/epic/internet/incb-bc.nsf/en/ct02500e.html.

203 2000, c.5, online: http://laws.justice.gc.ca/en/P-8.6/.

204 *Ibid.* at s-s. 2(1).

205 PIPEDA Case Summary #2005-319, "ISP's anti-spam measures questioned" (3 November 2005), online: http://www.privcom.gc.ca/cf-dc/2005/319_20051103_e.cfm.

206 Commissioner's Findings, PIPEDA Case Summary #2008-388, "Ticketmaster Canada Limited revised its policies and practices with respect to PIPEDA to protect customers' personal information", online: http://www.priv.gc.ca/cf-dc-2008/388_20080212_e.cfm.

personal information, nor to its disclosure and use by third parties for secondary marketing purposes because Ticketmaster collected personal information as a condition of service and without providing a clear opt-out option to customers who did not want their personal information shared for promotional or marketing purposes. To resolve the complaint, Ticketmaster changed its policies, allowing customers to choose whether or not they want to opt-in to receiving marketing material from Ticketmaster and its affiliates. The Assistant Commissioner stated four guidelines that online companies operating in Canada must observe in order to ensure compliance with *PIPEDA*:

> 1) If businesses collect their customers personal information with the intent of disclosing it to third parties for use in marketing and other secondary purposes, their customers must be explicitly informed and be provided a clear opt-in or opt-out opportunity to consent to the disclosure and use before payment is made. The customers' choice to opt in or opt out of information sharing must neither advantage nor disadvantage them with respect to other customers obtaining or seeking to obtain the same service.
>
> 2) Businesses are responsible for protecting their customer's personal information, by contractual or other means, which has been transferred to a third party for processing. The level of protection must be comparable with that provided by the business that collected the information.
>
> 3) Regardless of whether customer requests are issued on paper, in person, by telephone or via a web site, businesses must effectively communicate to customers in the same consistent manner their practices and policies regarding personal information collection, disclosure and use.
>
> 4) A business's privacy policy must be easily accessible by any individual, and organized and written in such a way that knowledge of any of the business's personal information management practices can be acquired without unreasonable effort.[207]

On the issue of online behavioural targeted advertising, the Privacy Commissioner has noted that this is an important emerging issue on the internet but has not made any findings under PIPEDA respecting online behavioural targeted advertising practices.

6.2.4. Proposed anti-spam legislation

The Canadian Parliament is currently considering anti-spam legislation in the form of Bill C-27, the *Electronic Commerce Protection Act* (ECPA).[208] Bill C-27 is the culmination of

---

207 *Ibid*.

208 Bill C-27, *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the*

a process that began with the Anti-Spam Action Plan for Canada in 2004 to deal with the issue of unsolicited commercial email, or "spam." The bill involves several agencies in the regulation of spam, including the Competition Bureau, the Privacy Commissioner, and the CRTC. Bill C-27 provides a regulatory scheme that includes administrative monetary penalties for spam and related threats from unsolicited electronic contact, including identity theft, phishing, spyware, viruses and botnets. It also grants an additional right of civil action to businesses and consumers targeted by the perpetrators of these activities.

Many businesses lobbied the government to derail Bill C-27 with concerns that the bill will greatly affect small businesses looking to promote their products over the internet and impair their ability to email consumers. Businesses lobbied for various exceptions, including a referral exception, and marketers proposed loopholes to make it easier for them to send unsolicited emails. Consumer groups such as PIAC were supportive of the bill, calling on the government to refrain from adding exceptions to dilute the anti-spam legislation. At the time of writing this report, the Bill had nearly made it through the House of Commons Standing Committee on Industry, Science and Technology with a limited number of changes.

6.2.5. Industry self-regulation

While the United States has the Network Advertising Initiative's Self-Regulatory Code of Conduct for Online Behavioural Advertising, the Canadian Marketing Association has not conducted any studies, white papers, Code of Ethics, or best practice guidelines pertaining to behavioural marketing for Canadian businesses. While the Canadian Marketing Association Code of Ethics has a section respecting the collection, use and disclosure of personal information of children and teenagers between, the CMA has not expanded these guidelines to fit modern advertising technologies such as online behavioural targeted marketing.

Thus, Canadian consumers are being tracked online and the only mechanism of recourse for Canadian consumers are through the complaint mechanisms of the Competition Bureau in the event of misleading advertisements and the Privacy Commissioner in the event of concerns with the collection, use or disclosure of their personal information. These mechanisms place the onus on consumers to take the time to file a proper complaint. This is particularly onerous given that few websites very clearly disclose their practices and notify consumers of the tracking technologies they use, and even where their practices are disclosed in the form of terms of service or a privacy policy, these practices are vaguely described. As a result, most consumers are not aware of the full extent of tracking and consumer surveillance on the internet. It would be difficult for the consumer to prove that the tracking is being done. Whether their continued use of these services can constitute informed consent to consumer

---

Telecommunications Act, Second Session, 40th Parliament, 57-58 Elizabeth II, introduced for First Reading on 24 April 2009. The Bill passed Second Reading on 8 May 2009 and was referred to the Standing Committee on Industry, Science and Technology on the same date.

surveillance is in question. Added to this, most consumers rarely have the time, energy and resources to lodge formal complaints with regulatory agencies, and even if they do, they lack sufficient information about their rights to take action. Furthermore, complaint mechanisms are not effective to help consumers opt out of tracking on the internet or prevent companies from building profiles about them.

6.3. Major barriers to implementing a "Do Not Track List" in Canada

6.3.1. According to the experts

PIAC contacted academic and industry experts to engage them in a discussion regarding the feasibility of a Do Not Track List in Canada. Three experts responded to our survey questions: Valerie Steeves, a professor with the Department of Criminology at the University of Ottawa, focusing on privacy and technology and Chair of the National Privacy Coalition; Jim Nehf, a law professor at Indiana University School of Law teaching consumer law and specializing in consumer privacy law; and Drew McArthur, Vice President Corporate Affairs and Compliance Officer for TELUS. The questionnaire and responses received are included in Appendix B.

6.3.2. Legal barriers

The challenges of regulating data collection, use and disclosure of businesses are significant, as technology has always been ahead of the law. Internet consumer tracking technologies have already been developed and heavily invested in on the assumption that these practices were legal. Companies have built a large industry of online behavioural targeted advertising on the possibilities of collecting, using, retaining and disclosing personal information and details about individual online activities without the consumer's knowledge or consent.

Consumers are not aware of the type and amount of personal information collected by the websites they visit and they are not aware of the extent of tracking that companies and third party advertisers are engaging in when they surf the internet. As discussed above, complaints-based approaches are unlikely to be effective. Thus there is an asymmetry in power between the consumer and the companies profiling them. Even if consumers were to put pressure on governments to regulate in the field of online behavioural targeted advertising, and as noted by Professor Nehf, prospective legislation or regulatory efforts would be subject to strong opposition and political pressure to create loopholes and exceptions. If experience is indicative of future trends, the previous lobbying efforts against the Do Not Call List and Bill C-27 by industry and businesses suggest that any regulatory effort against online targeted marketing would meet similar opposition. As well, Nehf notes that governments are increasingly relying on data brokers to provide information about individuals that is either too expensive or illegal for governments to collect and organize, making opposition entrenched and difficult to overcome.

6.3.3. Operational and technological barriers

To be successful, a Do Not Track List would have to identify individuals in a unique way – either by name or a unique identifier. IP addresses could be used for some tracking platforms, such as targeted advertising while surfing the internet, but would not address the problem completely, as users often have multiple IP addresses. An opt-in system might solve this problem, where a user could register an IP address if they wish to be tracked and to receive targeted advertising. However, as Professor Steeves notes, this policy will not likely be successful, because "the government has privileged e-commerce over privacy for the past 15 years."

McArthur suggested that the only way enforcement could be performed would be through a complaint investigation mechanism, similar to the way PIPEDA and the Do Not Call List currently operate. McArthur suggested that enforcement already exists in Canada through provincial private sector privacy legislation or PIPEDA, thus unauthorized collection and use of information is contrary to the law and therefore inappropriate and a Do Not Track List would not provide any further benefits to protecting consumers. Steeves suggests that a Do Not Track List should be regulated and enforced by complaints to the Privacy Commissioner. Both Steeves and Nehf suggested heavy fines levied for tracking without permission.

Nehf also emphasized that the data collection industry is too diverse and opaque for self-regulation to be effective. If consumers are tracked and profiled, they have no way of knowing who collected the data and passed it on to another company. Private enforcement by individuals will be rare, thus legal standing to privacy and consumer organizations would help, with legal fees and other awards given for successful legal actions.

6.3.4. Funding issues: who will bear the cost?

As per PIAC's survey, 21% of respondents stated that the federal government should bear the most responsibility for the costs of creating and maintaining a national Do Not Track List, compared to 20% of respondents who chose internet service providers and 16% who chose consumers who sign up for the service. McArthur argued that the telecommunications carrier should not pay for a Do Not Track List, as they should not have borne the cost of the Do Not Call List, since all the telecom carriers were implementing Do Not Call Lists of their own that were working well.

As noted by Nehf, the industry will have little difficulty in providing cost estimates outlining compliance costs and the loss of consumer "benefits" through tracking and profiling. On the other side, privacy advocates will have difficulty quantifying the consumer benefits of a Do Not Track List because these benefits are not easily convertible to dollar values. The usual result of this is no political action.

6.3.5. Will a "Do Not Track List" gain consumer confidence?

Professor Steeves voiced several concerns, as she is doubtful that companies would respect a Do Not Track List. Steeves suggested that companies will likely offer "benefits" to consumers who are tracked and restricting services to consumers who will not consent to being tracked. Clear policy guidelines are needed to ensure that services cannot be restricted to those who do not consent to being tracked and consumers should not pay for the cost of market surveillance of others.

Nehf stated that a Do Not Track List would be a step to reversing the privacy invasions that have happened as a result of modern technology. The law should make it illegal for companies to track our activities.

However, a complaints-based Do Not Track List might not attract consumer confidence, given the track record of the Do Not Call List in Canada, especially if a Do Not Track List is full of exceptions and loopholes for industry marketers. The Do Not Track List may also suffer from jurisdictional difficulties, as regulators might not extend enforcement against non-Canadian companies such as Google and DoubleClick. This would severely reduce the effectiveness of a Do Not Track List, given that much of the development and implementation of tracking technologies is taking place in the United States but enable the tracking of Canadian consumers.

CONCLUSION & RECOMMENDATIONS

As demonstrated by PIAC's surveys and other similar surveys conducted in the United States, consumers are not aware of tracking on the internet or the technical tools used by companies to track their behaviour online. While consumers may be somewhat familiar with more simplistic tracking technologies like cookies, they are not aware of the extent to which their personal information is collected and used to serve behaviourally targeted advertising to appeal to their consumer profile. Current industry practice is automatic consumer tracking. Any notice that might take place would be stated in vague terms hidden in the terms of use or privacy policies.

Consumers want the ability to control their personal information online – not only when and how it is collected, but also how it is used and shared with other parties. Consumer consent is only meaningful when proper notice is present, thus transparency in online behavioural targeted advertising practices is very important. In order to obtain informed consent to their practices, websites must clearly and openly notify their users of the tracking tools used by their websites and affiliates to track their behaviours online. In particular, consumers must know:

1) what personal information about them is collected, and especially what sensitive personal information is collected (e.g. health and financial information);
2) how this information will be used for online behavioural targeted advertising;
3) how long this information will be retained by the website operator and/or the parties with which they share the information; and
4) to whom this information will be disclosed, including affiliates and third party marketers and market researchers. Definitions should be provided for "affiliates," "third party" and "partners."

Studies by the United States Congress and the British All Party Parliamentary Communications Group have put forward strong recommendations for opt-in consent mechanisms for behavioural targeted advertising, especially for the use of deep packet inspection systems by ISPs. This means that behavioural advertising and online tracking would not be performed unless the consumer explicitly consented to the practice. The consumers in PIAC's survey about a "Do Not Track List" also voiced a strong desire for an opt-in consent model. However, the commercial sector and the online behavioural advertising industry appear committed to the opt-out consent model. The opt-out consent model takes advantage of consumer tendencies to trust businesses and leaves most consumers powerless. Opt-out regimes are often unfriendly to consumers, particularly for consumers who are not technically savvy, and rarely offer a whole, permanent solution for the consumer as opt-out may only be possible for the receipt of targeted advertising and not the collection of personal information for marketing research.

Consumer education through proper notice is only part of the solution. At the moment, there is a great power imbalance between the online advertising industry and consumers, as online behavioural targeted marketing has become the norm and

industry standard without any oversight by regulatory bodies. These practices have evolved without proper consideration to protect consumer autonomy and privacy and only with the goal of advertising revenues in mind.

Canadian consumers surveyed by PIAC expressed discomfort with online tracking for the purpose of targeted and behavioural advertising. The majority of survey respondents supported the creation of a "Do Not Track List," which would be a service wherein consumers who sign up for the list would not have information about their online activities collected, used or disclosed. However, it would be very difficult to design and deploy a "Do Not Track List" without assigning users a unique identifier. Furthermore, efforts to establish a "Do Not Track List" would face opposition and lobbying by industry to create loopholes and exceptions for businesses. Implementing a "Do Not Track List" in Canada would give Canadian consumers better control over their personal information while they surf the internet. However, while a "Do Not Track List" would certainly be a step to better protection for consumers from online tracking, it cannot be expected to provide holistic or foolproof consumer protection, especially given the logistical and technical barriers to effective implementation.

Voluntary industry codes currently do not exist in Canada for online behavioural targeted advertising, and even if they did, they would likely be ineffective because compliance would be voluntary and businesses have no incentive to comply given the value and potential revenue to be gleaned from using consumers' personal information. A voluntary industry code would not appropriately address the power imbalance between the advertising industry and consumers and would not likely include an effective enforcement regime or consumer complaint mechanism.

Currently, the only legislation in place that would appropriately deal with the issue of online behavioural targeted advertising is the *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA provides consumers with a complaint mechanism wherein the Privacy Commissioner will investigate and make findings with respect to the data practices of private sector organizations. However, the Privacy Commissioner has not yet used PIPEDA to specifically address the issue of online behavioural targeted advertising practices. Moreover, it is unreasonable to expect consumers to complain about the practice when they are unaware of the extent to which their personal information is collected, used and disclosed for the purpose of online behavioural targeted advertising.

Several jurisdictions have begun to study the issue of online behavioural targeted advertising, including the United States and the European Union. It is now Canada's turn to examine this issue in depth, with a mind to ensuring that Canada's regulatory framework remains fit to effectively enforce privacy and data protection for Canadian consumers. Furthermore, a review of the current regulatory framework would provide legal clarity and certainty for the online behavioural targeted advertising industry as companies continue to develop their technologies.

The Privacy Commissioner should review the existing legislation and set out guidelines for how website operators can deploy their behavioural advertisement technology in order to comply with the requirements of PIPEDA and protect the privacy of Canadians. Furthermore, the Government should review the existing privacy legislation applying to behavioural advertisement and bring forward new rules as necessary, in particular to ensure that these systems are only operated on an explicit, informed, opt-in basis and that an effective enforcement mechanism with fines exists to punish marketers who operate outside of the rules. Special consideration and study should be paid to the issue to how behavioural advertising aimed at children and young people should be regulated. Online behavioural advertising targeting minors must be prohibited.

While a “Do Not Track List” would likely encounter considerable industry objection and operational and technical barriers, regulators are in a position to set down clear guidelines for online behavioural targeted advertising practices. Given the prevalence of personal information collection, use and disclosure for the purposes of behavioural targeted advertising on the internet, only clear, enforceable rules can make a significant impact to protect consumers from unwanted online surveillance and behavioural targeted advertisements. Enforceable guidelines would better fit within the regulatory framework and would likely provide consumers with more effective and holistic privacy protection than a “Do Not Track List.”

APPENDIX A – ENVIRONICS SURVEY RESULTS

Below is a copy of the survey results, as conducted by Environics and designed by PIAC, examining Canadian attitudes toward the “Do Not Track List."

TABLE OF CONTENTS

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

QS. INTERNET ACCESS

		REGION					SUB-REGION							COMMUNITY SIZE				EMPLOYMENT				
	TOTAL	Atla-ntic	QC	ON	Prai-ries	BC	Tor.	Mtl	Van.	MB	SK	AB	Can. Excl. QC	1M+	100K-1M	5K-100K	Under 5K	Full Time	Part Time	Home-maker	Unemp loyed	Re-tired
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)	(V)
TOTAL WEIGHTED	2002	148	487	767	335	265	322	234	137	71	60	204	1515	810	356	568	269	889	190	82	118	403
UNWEIGHTED TOTAL	2002	251	501	500	500	250	205	232	125	133	117	250	1501	705	367	571	359	846	165	87	103	520
NET: Any	82%	84% C	76%	83% C	87% C	84% C	87%	83%	83%	86%	86%	88%	84%	85% Q	86% Q	81% Q	72%	95% TUV	90% TUV	74% V	75% V	50%
Home	77%	80% C	70%	79% C	82% C	78% C	82%	76%	76%	84%	75%	83%	80%	80% PQ	84% PQ	75% Q	65%	87% TUV	84% UV	74% V	71% V	50%
Work	53%	53%	50%	53%	62% CDF	48%	63% IM	60%	51%	54%	60%	66% IM	54%	60% PQ	58% PQ	46%	41%	78% STUV	55% TUV	14%	30% TV	7%
At School	23%	22%	19%	24%	27% C	21%	32% IM	24%	20%	28%	24%	27%	24%	27% PQ	23%	18%	18%	20% TV	45% RTUV	11%	21% V	5%
None of the above	18%	16%	24% BDEF	17%	13%	16%	13%	17%	17%	14%	14%	12%	16%	15%	14%	19%	28% NOP	5%	10%	26% RS	25% RS	50% RSTU

Comparison Groups: BCDEF/GHIJKLM/NOPQ/RSTUV
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

QS. INTERNET ACCESS

		FAMILY INCOME				EDUCATION					LANGUAGE			GENDER		AGE				KIDS <18	
	TOTAL	Under $20K	$20K Under $40K	$40K Under $80K	$80K More	Less H.S.	H.S.	Comm. Coll.	Some Univ.	Univ. Deg.	Eng.	Fre.	Other	M	F	18-29	30-44	45-59	60+	Yes	No
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)
TOTAL WEIGHTED	2002	178	309	472	507	237	335	578	203	598	1298	512	236	967	1035	396	554	572	481	532	1470
UNWEIGHTED TOTAL	2002	183	317	475	486	278	346	549	196	579	1299	542	200	999	1003	186	511	674	631	462	1540
NET: Any	82%	56%	73%	89%	97%	51%	74%	87%	91%	93%	85%	75%	81%	84%	81%	94%	94%	87%	53%	93%	78%
			B	BC	BCD		F	FG	FG	FGH	L					RS	RS	S		U	
Home	77%	54%	67%	81%	95%	47%	68%	82%	87%	88%	81%	70%	76%	80%	75%	89%	89%	80%	52%	88%	74%
			B	BC	BCD		F	FG	FG	FGH	L			O		RS	RS	S		U	
Work	53%	13%	41%	58%	79%	19%	40%	54%	61%	71%	54%	49%	52%	56%	50%	62%	73%	59%	16%	68%	48%
			B	BC	BCD		F	FG	FG	FGHI	L			O		S	PRS	S		U	
At School	23%	21%	23%	18%	32%	16%	17%	21%	31%	28%	23%	19%	31%	25%	21%	52%	25%	15%	5%	30%	20%
					BCD			F	FGH	FGH	L		KL	O		QRS	RS	S		U	
None of the above	18%	44%	27%	11%	3%	49%	26%	13%	9%	7%	15%	25%	19%	16%	19%	6%	6%	13%	47%	7%	22%
		CDE	DE	E		GHIJ	HIJ	J				K						PQ	PQR		T

Comparison Groups: BCDE/FGHIJ/KLM/NO/PQRS/TU
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q1. MANY INTERNET WEBSITES USE TECHNOLOGY SUCH AS PERSISTENT "COOKIES" OR "WEB BEACONS" TO TRACK PEOPLES' ONLINE ACTIVITIES. HOW FAMILIAR ARE YOU WITH THE EXISTENCE OF THESE TRACKING DEVICES AND TECHNIQUES?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		REGION					SUB-REGION							COMMUNITY SIZE				EMPLOYMENT				
	TOTAL	Atla-ntic	QC	ON	Prai-ries	BC	Tor.	Mtl	Van.	MB	SK	AB	Can. Excl. QC	1M+	100K-1M	5K-100K	Under 5K	Full Time	Part Time	Home-maker	Unemp loyed	Re-tired
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)	(V)
TOTAL	1647	125	370	640	291	222	279	193	114	61	51	179	1277	692	305	457	193	841	171	60	88	203
UNWEIGHTED TOTAL	1570	194	358	405	410	203	173	181	101	105	92	213	1212	579	305	439	247	790	141	62	74	262
Very familar	20%	19% C	12%	22% C	18% C	27% CE	23% HK	12%	26% HK	16%	11%	20% H	22% HK	20% Q	25% Q	19% Q	10%	21% V	22% V	13%	24% V	12%
Somwehat familiar	30%	43% C	11%	34% C	39% C	33% C	38% H	13%	31% H	32% H	50% HIJM	38% H	36% H	30%	34%	28%	32%	32%	31%	26%	29%	27%
Not very familiar	19%	10%	28% BDF	16%	22% BDF	13%	14%	27% GIM	14%	30% GIM	20%	20%	16%	19%	20%	19%	21%	19%	18%	28%	23%	16%
Not at all familiar	31%	28%	49% BDEF	27%	21%	27%	24%	48% IJKLMG	29%	21%	19%	21%	26%	31% O	21%	35% O	37% O	29%	29%	33%	24%	45% RSU
Refused	*%	-	-	*%	-	-	-	-	-	-	-	-	*%	-	*%	-	-	-	-	-	-	1%
DK/NA	*%	-	-	-	*%	-	-	-	-	1%	-	-	*%	-	-	*%	-	*%	-	-	-	-

Comparison Groups: BCDEF/GHIJKLM/NOPQ/RSTUV
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q1. MANY INTERNET WEBSITES USE TECHNOLOGY SUCH AS PERSISTENT "COOKIES" OR "WEB BEACONS" TO TRACK PEOPLES' ONLINE ACTIVITIES. HOW FAMILIAR ARE YOU WITH THE EXISTENCE OF THESE TRACKING DEVICES AND TECHNIQUES?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		FAMILY INCOME				EDUCATION					LANGUAGE			GENDER		AGE				KIDS <18	
	TOTAL	Under $20K	$20K Under $40K	$40K Under $80K	$80K More	Less H.S.	H.S.	Comm. Coll.	Some Univ.	Univ. Deg.	Eng.	Fre.	Other	M	F	18-29	30-44	45-59	60+	Yes	No
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)
TOTAL	1647	100	224	419	494	120	249	502	186	554	1106	385	192	810	837	373	518	499	256	493	1154
UNWEIGHTED TOTAL	1570	88	210	411	470	123	244	467	175	525	1064	384	151	796	774	175	477	583	335	429	1141
Very familar	20%	19%	15%	16%	22% CD	16%	10%	20% G	20% G	24% G	22% L	12%	24% L	28% O	12%	21% S	24% RS	17%	13%	23%	18%
Somwehat familiar	30%	19%	33% B	30%	35% B	19%	25%	29% F	33% F	36% FGH	36% L	14%	29% L	32%	29%	31%	32%	29%	29%	31%	30%
Not very familiar	19%	19%	23%	20%	19%	19%	24%	17%	16%	19%	17%	26% K	19%	16%	22% N	26% RS	19%	15%	17%	21%	18%
Not at all familiar	31%	42% E	29%	34% E	24%	46% HIJ	41% IJ	34% J	30% J	21%	25%	48% KM	28%	25%	37% N	23%	25%	38% PQ	41% PQ	25%	33% T
Refused	*%	-	-	-	-	-	-	-	1%	-	*%	-	-	-	*%	-	-	-	1%	-	*%
DK/NA	*%	-	-	-	-	-	-	*%	-	-	*%	-	-	-	*%	-	*%	-	-	*%	-

Comparison Groups: BCDE/FGHIJ/KLM/NO/PQRS/TU
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q2. WHEN YOU ARE SURFING THE INTERNET, YOU MAY SEE POP-UP OR BANNER ADS. OFTEN TIMES THESE ADS ARE TARGETED AT YOU AS A RESULT OF YOUR ONLINE ACTIVITIES AND PREFERENCES BEING TRACKED. HOW COMFORTABLE ARE YOU WITH YOUR ONLINE ACTIVITY BEING TRACKED FOR THIS PURPOSE?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		REGION					SUB-REGION							COMMUNITY SIZE				EMPLOYMENT				
	TOTAL	Atlantic	QC	ON	Prairies	BC	Tor.	Mtl	Van.	MB	SK	AB	Can. Excl. QC	1M+	100K-1M	5K-100K	Under 5K	Full Time	Part Time	Home-maker	Unemployed	Retired
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)	(V)
TOTAL	1647	125	370	640	291	222	279	193	114	61	51	179	1277	692	305	457	193	841	171	60	88	203
UNWEIGHTED TOTAL	1570	194	358	405	410	203	173	181	101	105	92	213	1212	579	305	439	247	790	141	62	74	262
Very comfortable	8%	10% E	10% E	7% E	4%	8%	8% K	10% KL	7%	5%	3%	4%	7% K	7%	8%	8%	6%	9% V	5%	6%	10%	4%
Somewhat comfortable	17%	20%	13%	20% C	19% C	14%	21% H	11%	16%	19%	18%	20% H	19% H	18%	16%	18%	18%	18% V	16%	18%	21%	13%
Not very comfortable	25%	26%	25%	23%	27%	26%	25%	27%	29%	34%	20%	26%	25%	27%	23%	25%	21%	26%	31%	29%	23%	23%
Not at all comfortable	49%	43%	51%	49%	49%	49%	45%	50%	43%	42%	59% IJ	48%	48%	46%	53%	48%	54%	47%	48%	46%	45%	56% R
Refused	1%	1%	-	1%	1%	2%	*%	-	3%	-	-	2%	1%	1%	1%	1%	2%	1%	-	1%	1%	2%
DK/NA	*%	-	1%	*%	-	1%	-	1%	1%	-	-	-	*%	*%	*%	1%	-	*%	-	-	-	2% R

Comparison Groups: BCDEF/GHIJKLM/NOPQ/RSTUV
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q2. WHEN YOU ARE SURFING THE INTERNET, YOU MAY SEE POP-UP OR BANNER ADS. OFTEN TIMES THESE ADS ARE TARGETED AT YOU AS A RESULT OF YOUR ONLINE ACTIVITIES AND PREFERENCES BEING TRACKED. HOW COMFORTABLE ARE YOU WITH YOUR ONLINE ACTIVITY BEING TRACKED FOR THIS PURPOSE?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		FAMILY INCOME				EDUCATION					LANGUAGE			GENDER		AGE				KIDS <18	
	TOTAL	Under $20K	$20K Under $40K	$40K Under $80K	$80K More	Less H.S.	H.S.	Comm. Coll.	Some Univ.	Univ. Deg.	Eng.	Fre.	Other	M	F	18-29	30-44	45-59	60+	Yes	No
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)
TOTAL	1647	100	224	419	494	120	249	502	186	554	1106	385	192	810	837	373	518	499	256	493	1154
UNWEIGHTED TOTAL	1570	88	210	411	470	123	244	467	175	525	1064	384	151	796	774	175	477	583	335	429	1141
Very comfortable	8%	3%	9%	10% B	8%	7%	10% J	9%	7%	6%	7%	9%	7%	9%	7%	10% S	9% S	6%	4%	10%	7%
Somewhat comfortable	17%	19%	17%	17%	22%	17%	18%	17%	12%	20% I	19% L	13%	17%	20% O	15%	22% RS	20% RS	13%	14%	21% U	16%
Not very comfortable	25%	31%	23%	28%	22%	19%	27%	22%	23%	28%	25%	26%	23%	24%	26%	24%	27%	23%	23%	27%	24%
Not at all comfortable	49%	43%	51%	45%	47%	54%	44%	51%	56% GJ	45%	48%	52%	51%	45%	52% N	43%	42%	56% PQ	55% PQ	42%	52% T
Refused	1%	2%	*%	1%	1%	3%	*%	1%	1%	1%	1%	-	1%	1% O	*%	1%	1%	*%	3% R	*%	1%
DK/NA	*%	3%	-	*%	*%	1%	*%	*%	-	1%	*%	*%	2%	1%	*%	1%	-	*%	1%	-	1%

Comparison Groups: BCDE/FGHIJ/KLM/NO/PQRS/TU
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q3. IN GENERAL HOW COMFORTABLE ARE YOU WITH COMPANIES AND ORGANIZATIONS YOU DEAL WITH SHARING INFORMATION ABOUT YOUR CONSUMER BEHAVIOUR WITH OTHER COMPANIES AND ORGANIZATIONS SO THAT THEY CAN TARGET THEIR ADVERTISING AT YOU?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		REGION					SUB-REGION							COMMUNITY SIZE				EMPLOYMENT				
	TOTAL	Atla-ntic	QC	ON	Prai-ries	BC	Tor.	Mtl	Van.	MB	SK	AB	Can. Excl. QC	1M+	100K-1M	5K-100K	Under 5K	Full Time	Part Time	Home-maker	Unemp loyed	Re-tired
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)	(V)
TOTAL	1647	125	370	640	291	222	279	193	114	61	51	179	1277	692	305	457	193	841	171	60	88	203
UNWEIGHTED TOTAL	1570	194	358	405	410	203	173	181	101	105	92	213	1212	579	305	439	247	790	141	62	74	262
Very comfortable	4%	3%	6% EF	4% E	1%	2%	5% L	5% KL	2%	2%	1%	1%	3%	4% Q	5% Q	4%	1%	5% S	1%	5%	7% S	2%
Somewhat comfortable	18%	21%	18%	18%	17%	16%	18% J	24% JK	19%	9%	12%	21% J	18% J	20%	15%	18%	15%	18% V	22% V	24% V	20% V	8%
Not very comfortable	25%	25%	25%	27%	23%	23%	32% HI	22%	20%	20%	24%	23%	25%	26%	25%	24%	25%	25%	29%	28%	23%	20%
Not at all comfortable	53%	51%	50%	50%	58% CD	58%	44%	49%	57%	69% GHLM	62% G	54%	53% G	50%	54%	55%	57%	52%	46%	43%	49%	67% RSTU
Refused	*%	-	*%	1%	*%	-	1%	-	-	-	-	*%	*%	*%	*%	-	1%	*%	-	-	1%	1%
DK/NA	*%	-	*%	*%	*%	1%	-	1%	2%	-	-	*%	*%	*%	1%	-	*%	*%	1%	-	-	1%

Comparison Groups: BCDEF/GHIJKLM/NOPQ/RSTUV
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q3. IN GENERAL HOW COMFORTABLE ARE YOU WITH COMPANIES AND ORGANIZATIONS YOU DEAL WITH SHARING INFORMATION ABOUT YOUR CONSUMER BEHAVIOUR WITH OTHER COMPANIES AND ORGANIZATIONS SO THAT THEY CAN TARGET THEIR ADVERTISING AT YOU?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		FAMILY INCOME				EDUCATION					LANGUAGE			GENDER		AGE				KIDS <18	
	TOTAL	Under $20K	$20K Under $40K	$40K Under $80K	$80K More	Less H.S.	H.S.	Comm. Coll.	Some Univ.	Univ. Deg.	Eng.	Fre.	Other	M	F	18-29	30-44	45-59	60+	Yes	No
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)
TOTAL	1647	100	224	419	494	120	249	502	186	554	1106	385	192	810	837	373	518	499	256	493	1154
UNWEIGHTED TOTAL	1570	88	210	411	470	123	244	467	175	525	1064	384	151	796	774	175	477	583	335	429	1141
Very comfortable	4%	5%	7%	4%	3%	5%	7% HJ	3%	3%	3%	3%	5%	10% K	4%	3%	5%	3%	4%	3%	5%	3%
Somewhat comfortable	18%	16%	20%	21%	20%	15%	22%	19%	15%	17%	18%	16%	21%	21% O	15%	25% RS	22% RS	12%	11%	21% U	16%
Not very comfortable	25%	19%	29%	24%	28%	26%	20%	24%	29%	27% G	24%	27%	28%	24%	26%	27%	26%	24%	22%	29% U	23%
Not at all comfortable	53%	57% C	43%	51%	49%	53%	49%	54%	52%	52%	55% M	52% M	41%	50%	55%	42%	48%	60% PQ	63% PQ	44%	57% T
Refused	*%	*%	1%	-	-	2%	*%	*%	-	-	*%	*%	-	1%	-	-	*%	1%	*%	-	*%
DK/NA	*%	2%	1%	*%	*%	-	2%	-	1%	-	*%	*%	1%	1%	*%	1%	*%	-	1%	1%	*%

Comparison Groups: BCDE/FGHIJ/KLM/NO/PQRS/TU
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q4. THERE ARE SEVERAL WAYS IN WHICH INFORMATION ABOUT YOUR INTERNET ACTIVITIES COULD BE USED. WHICH OF THE FOLLOWING WOULD YOU BE MOST LIKELY TO CONSENT TO?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		REGION					SUB-REGION							COMMUNITY SIZE				EMPLOYMENT				
	TOTAL	Atla-ntic	QC	ON	Prai-ries	BC	Tor.	Mtl	Van.	MB	SK	AB	Can. Excl. QC	1M+	100K-1M	5K-100K	Under 5K	Full Time	Part Time	Home-maker	Unemp loyed	Re-tired
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)	(V)
TOTAL	1647	125	370	640	291	222	279	193	114	61	51	179	1277	692	305	457	193	841	171	60	88	203
UNWEIGHTED TOTAL	1570	194	358	405	410	203	173	181	101	105	92	213	1212	579	305	439	247	790	141	62	74	262
Customer service purposes by a company or organization you deal with	47%	50%	41%	52% CF	45%	42%	60% HIKLM	42%	43%	52%	40%	44%	49%	50%	46%	43%	46%	48% V	50% V	47%	40%	33%
Targeted advertising by a company or organization you deal with	22%	17%	26% BD	19%	26% BD	22%	17%	26%	20%	23%	31% G	25%	21%	21%	20%	22%	27%	23%	23%	24%	26%	17%
Market research studies by companies or organizations you have not dealt with	11%	15% E	11%	11%	8%	11%	9%	12%	13%	9%	5%	9%	11%	10%	14% Q	12% Q	6%	11%	11%	10%	9%	13%
Targeted advertising by companies or organizations you have not dealt with	6%	5%	5%	7%	8%	5%	6%	5%	4%	5%	10%	8%	7%	6%	7%	6%	4%	6%	7%	5%	10%	9%
None	12%	11%	18% DE	9%	9%	17% DE	7%	16% G	16% G	8%	10%	10%	11%	11%	10%	14%	14%	11%	7%	11%	10%	23% RSTU
Refused	1%	1%	-	1%	1%	2%	-	-	2%	3%	-	1%	1%	*%	1%	1%	*%	1%	-	1%	-	3% R
DK/NA	1%	1%	1%	1%	3%	1%	1%	1%	2%	1%	5%	3%	2%	1%	1%	2%	2%	1%	2%	2%	4%	3% R

Comparison Groups: BCDEF/GHIJKLM/NOPQ/RSTUV
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q4. THERE ARE SEVERAL WAYS IN WHICH INFORMATION ABOUT YOUR INTERNET ACTIVITIES COULD BE USED. WHICH OF THE FOLLOWING WOULD YOU BE MOST LIKELY TO CONSENT TO?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		FAMILY INCOME				EDUCATION					LANGUAGE			GENDER		AGE				KIDS <18	
	TOTAL	Under $20K	$20K Under $40K	$40K Under $80K	$80K More	Less H.S.	H.S.	Comm. Coll.	Some Univ.	Univ. Deg.	Eng.	Fre.	Other	M	F	18-29	30-44	45-59	60+	Yes	No
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)
TOTAL	1647	100	224	419	494	120	249	502	186	554	1106	385	192	810	837	373	518	499	256	493	1154
UNWEIGHTED TOTAL	1570	88	210	411	470	123	244	467	175	525	1064	384	151	796	774	175	477	583	335	429	1141
Customer service purposes by a company or organization you deal with	47%	35%	47%	54% B	47%	46%	51%	48%	45%	45%	50% LM	42%	39%	44%	49% N	45%	51% S	48% S	39%	49%	46%
Targeted advertising by a company or organization you deal with	22%	30%	19%	20%	26%	20%	20%	23%	22%	21%	21%	25%	22%	21%	22%	24%	24% S	21%	16%	26% U	20%
Market research studies by companies or organizations you have not dealt with	11%	15%	13%	8%	8%	11%	9%	9%	12%	13%	10%	11%	14%	12%	9%	14% Q	8%	11%	10%	9%	12%
Targeted advertising by companies or organizations you have not dealt with	6%	6%	5%	6%	7%	4%	6%	4%	6%	9% H	6%	5%	10%	8% O	5%	8%	5%	5%	8%	5%	6%
None	12%	7%	13%	11%	10%	14%	8%	15% G	11%	12%	11%	17% KM	10%	12%	13%	8%	10%	14% P	21% PQR	9%	13% T
Refused	1%	2%	1%	*%	1%	2%	2%	1%	1%	*%	1%	-	1%	1%	1%	*%	1%	*%	3% R	*%	1%
DK/NA	1%	5%	2%	*%	1%	3%	3% HJ	1%	1%	*%	1%	1%	4%	2%	1%	2%	1%	1%	3% QR	2%	1%

Comparison Groups: BCDE/FGHIJ/KLM/NO/PQRS/TU
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q5. THERE ARE A NUMBER OF TYPES OF ORGANIZATIONS THAT MIGHT TRACK INTERNET ACTIVITY AND TARGET ADVERTISING. WHICH ONE OF THE FOLLOWING WOULD YOU BE MOST COMFORTABLE WITH ALLOWING TO TRACK YOUR INTERNET ACTIVITY AND TO TARGET ONLINE ADVERTISING AT YOU?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		REGION					SUB-REGION							COMMUNITY SIZE				EMPLOYMENT				
	TOTAL	Atla-ntic	QC	ON	Prai-ries	BC	Tor.	Mtl	Van.	MB	SK	AB	Can. Excl. QC	1M+	100K-1M	5K-100K	Under 5K	Full Time	Part Time	Home-maker	Unemp loyed	Re-tired
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)	(V)
TOTAL	1647	125	370	640	291	222	279	193	114	61	51	179	1277	692	305	457	193	841	171	60	88	203
UNWEIGHTED TOTAL	1570	194	358	405	410	203	173	181	101	105	92	213	1212	579	305	439	247	790	141	62	74	262
Companies and organizations with websites you visit regularly	41%	42% C	30%	46% C	45% C	40% C	45% H	30%	37%	51% H	52% H	41% H	44% H	39%	43%	42%	44%	42% V	44% V	36%	38%	33%
Government agencies	28%	31%	35% DEF	25%	27%	22%	25%	36% GJM	28%	21%	24%	30%	26%	30%	28%	25%	28%	29%	28%	25%	27%	27%
Market researchers and data brokers	9%	10%	10%	10%	8%	7%	12%	11%	6%	7%	8%	9%	9%	10% Q	11% Q	9%	5%	9%	11%	13%	10%	6%
Other/Combination	1%	-	2% D	*%	-	1%	-	1%	2%	-	-	-	*%	1%	1%	*%	2%	1%	2%	4%	-	*%
None	20%	16%	22%	17%	18%	28% BDE	16%	21%	26% K	21%	12%	18%	19%	19%	17%	22%	20%	18%	12%	21%	21%	31% RS
Refused	1%	1%	-	1%	*%	1%	1%	-	2%	-	-	*%	1%	1%	*%	1%	-	*%	1%	1%	1%	1%
DK/NA	1%	1%	1%	1%	1%	1%	1%	1%	-	1%	4%	1%	1%	1%	1%	1%	1%	*%	3%	-	2%	3%

Comparison Groups: BCDEF/GHIJKLM/NOPQ/RSTUV
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q5. THERE ARE A NUMBER OF TYPES OF ORGANIZATIONS THAT MIGHT TRACK INTERNET ACTIVITY AND TARGET ADVERTISING. WHICH ONE OF THE FOLLOWING WOULD YOU BE MOST COMFORTABLE WITH ALLOWING TO TRACK YOUR INTERNET ACTIVITY AND TO TARGET ONLINE ADVERTISING AT YOU?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		FAMILY INCOME				EDUCATION					LANGUAGE			GENDER		AGE				KIDS <18	
	TOTAL	Under $20K	$20K Under $40K	$40K Under $80K	$80K More	Less H.S.	H.S.	Comm. Coll.	Some Univ.	Univ. Deg.	Eng.	Fre.	Other	M	F	18-29	30-44	45-59	60+	Yes	No
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)
TOTAL	1647	100	224	419	494	120	249	502	186	554	1106	385	192	810	837	373	518	499	256	493	1154
UNWEIGHTED TOTAL	1570	88	210	411	470	123	244	467	175	525	1064	384	151	796	774	175	477	583	335	429	1141
Companies and organizations with websites you visit regularly	41%	50%	43%	44%	44%	45%	42%	40%	44%	41%	46% LM	32%	33%	41%	41%	44% S	44% S	41% S	31%	44%	40%
Government agencies	28%	24%	26%	31%	27%	27%	28%	26%	25%	30%	24%	34% K	37% K	29%	27%	29%	31% R	23%	28%	30%	27%
Market researchers and data brokers	9%	11%	8%	9%	11%	8%	11%	9%	11%	8%	9%	10%	7%	10%	8%	14% QRS	8%	8%	7%	9%	9%
Other/Combination	1%	2%	2%	*%	*%	-	1%	1%	-	*%	*%	2% K	1%	1%	1%	1%	1%	1%	*%	1%	1%
None	20%	13%	19%	14%	17%	19%	14%	23% G	18%	20%	19%	21%	15%	18%	21%	10%	15%	25% PQ	30% PQ	15%	22% T
Refused	1%	1%	1%	1%	*%	1%	1%	1%	1%	*%	*%	-	3%	1%	1%	-	*%	1%	2% Q	*%	1%
DK/NA	1%	-	2%	1%	1%	-	2%	*%	1%	1%	1%	1%	3%	1%	1%	1%	*%	1%	2%	1%	1%

Comparison Groups: BCDE/FGHIJ/KLM/NO/PQRS/TU
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q6. SOME PEOPLE HAVE SUGGESTED CREATING A NATIONAL "DO NOT TRACK" LIST. PEOPLE CHOOSING TO BE ON THE "DO NOT TRACK" LIST WOULD NOT HAVE INFORMATION ABOUT THEIR ONLINE ACTIVITIES COLLECTED, USED OR DISCLOSED. WOULD YOU __ THE CREATION OF THIS TYPE OF NATIONAL "DO NOT TRACK" LIST?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		REGION					SUB-REGION							COMMUNITY SIZE				EMPLOYMENT				
	TOTAL	Atlantic	QC	ON	Prairies	BC	Tor.	Mtl	Van.	MB	SK	AB	Can. Excl. QC	1M+	100K-1M	5K-100K	Under 5K	Full Time	Part Time	Home-maker	Unemployed	Retired
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)	(V)
TOTAL	1647	125	370	640	291	222	279	193	114	61	51	179	1277	692	305	457	193	841	171	60	88	203
UNWEIGHTED TOTAL	1570	194	358	405	410	203	173	181	101	105	92	213	1212	579	305	439	247	790	141	62	74	262
Strongly support	54%	45%	51%	56% B	55%	55%	51%	54%	56%	58%	58%	53%	55%	53%	60% P	52%	51%	56%	51%	52%	43%	58%
Somewhat support	27%	27%	26%	28%	26%	27%	32%	28%	25%	25%	26%	26%	27%	28%	24%	28%	23%	26% V	32% V	25%	29%	20%
Somewhat oppose	8%	14% CDF	8%	6%	10% D	7%	8%	7%	7%	8%	8%	11%	8%	9%	6%	7%	8%	7%	9%	9%	17% RV	6%
Strongly oppose	10%	10%	14% DE	8%	8%	10%	7%	10%	10%	10%	6%	7%	8%	8%	9%	11%	15% N	8%	7%	15%	8%	14% R
Refused	1%	1%	-	2%	1%	1%	2%	-	2%	-	-	1%	1%	1%	-	1%	*%	1%	*%	-	2%	1%
DK/NA	1%	2% D	1%	*%	1%	-	-	1%	-	-	1%	2%	1%	*%	1%	1%	2%	1%	*%	-	1%	1%

Comparison Groups: BCDEF/GHIJKLM/NOPQ/RSTUV
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q6. SOME PEOPLE HAVE SUGGESTED CREATING A NATIONAL "DO NOT TRACK" LIST. PEOPLE CHOOSING TO BE ON THE "DO NOT TRACK" LIST WOULD NOT HAVE INFORMATION ABOUT THEIR ONLINE ACTIVITIES COLLECTED, USED OR DISCLOSED. WOULD YOU __ THE CREATION OF THIS TYPE OF NATIONAL "DO NOT TRACK" LIST?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		FAMILY INCOME				EDUCATION					LANGUAGE			GENDER		AGE				KIDS <18	
	TOTAL	Under $20K	$20K Under $40K	$40K Under $80K	$80K More	Less H.S.	H.S.	Comm. Coll.	Some Univ.	Univ. Deg.	Eng.	Fre.	Other	M	F	18-29	30-44	45-59	60+	Yes	No
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)
TOTAL	1647	100	224	419	494	120	249	502	186	554	1106	385	192	810	837	373	518	499	256	493	1154
UNWEIGHTED TOTAL	1570	88	210	411	470	123	244	467	175	525	1064	384	151	796	774	175	477	583	335	429	1141
Strongly support	54%	43%	48%	53%	57% BC	36%	50% F	57% F	49% F	58% F	54%	51%	51%	53%	55%	46%	52%	60% PQ	56%	49%	56% T
Somewhat support	27%	31%	26%	30%	29%	28%	26%	26%	32%	27%	28%	27%	25%	26%	28%	29%	31% RS	23%	22%	31%	25%
Somewhat oppose	8%	14% E	12% E	8% E	5%	11%	12% J	7%	8%	6%	8%	7%	11%	9%	7%	14% QRS	6%	6%	6%	9%	7%
Strongly oppose	10%	11%	12%	8%	8%	22% GHIJ	12%	8%	9%	7%	8%	14% K	11%	10%	9%	9%	9%	9%	14% QR	11%	9%
Refused	1%	1%	1%	1%	-	2%	-	*%	*%	2% H	1%	-	1%	1%	1%	1%	1%	1%	1%	1%	1%
DK/NA	1%	*%	*%	1%	*%	1%	1%	1%	1%	-	1%	1%	*%	1%	1%	1%	1%	1%	1%	1%	1%

Comparison Groups: BCDE/FGHIJ/KLM/NO/PQRS/TU
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q7. IF THERE WAS A NATIONAL "DO NOT TRACK" LIST, HOW LIKELY WOULD YOU BE TO SIGN UP FOR IT?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		REGION					SUB-REGION							COMMUNITY SIZE				EMPLOYMENT				
	TOTAL	Atla-ntic	QC	ON	Prai-ries	BC	Tor.	Mtl	Van.	MB	SK	AB	Can. Excl. QC	1M+	100K-1M	5K-100K	Under 5K	Full Time	Part Time	Home-maker	Unemp loyed	Re-tired
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)	(V)
TOTAL	1647	125	370	640	291	222	279	193	114	61	51	179	1277	692	305	457	193	841	171	60	88	203
UNWEIGHTED TOTAL	1570	194	358	405	410	203	173	181	101	105	92	213	1212	579	305	439	247	790	141	62	74	262
Definitely	33%	32%	30%	35%	34%	33%	29%	34%	34%	36%	37%	33%	34%	32%	40% NP	31%	33%	36%	28%	33%	29%	35%
Probably	37%	39%	37%	39%	36%	34%	44%	36%	32%	39%	38%	34%	37%	38%	35%	40% Q	31%	36%	48% RV	42%	36%	32%
Probably not	17%	16%	15%	16%	17%	20%	19%	14%	20%	16%	14%	19%	17%	18%	13%	16%	19%	16%	16%	10%	21%	16%
Definitely not	12%	13%	17% DE	9%	12%	12%	8%	15%	14%	9%	10%	13%	10%	12%	11%	11%	16%	11%	7%	15%	12%	16% S
Refused	*%	-	-	-	*%	-	-	-	-	-	-	*%	*%	-	-	*%	-	-	-	-	-	-
DK/NA	1%	1%	1%	1%	*%	*%	-	1%	-	-	*%	1%	1%	*%	*%	1%	*%	1%	*%	-	2%	1%

Comparison Groups: BCDEF/GHIJKLM/NOPQ/RSTUV
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q7. IF THERE WAS A NATIONAL "DO NOT TRACK" LIST, HOW LIKELY WOULD YOU BE TO SIGN UP FOR IT?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		FAMILY INCOME				EDUCATION					LANGUAGE			GENDER		AGE				KIDS <18	
	TOTAL	Under $20K	$20K Under $40K	$40K Under $80K	$80K More	Less H.S.	H.S.	Comm. Coll.	Some Univ.	Univ. Deg.	Eng.	Fre.	Other	M	F	18-29	30-44	45-59	60+	Yes	No
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)
TOTAL	1647	100	224	419	494	120	249	502	186	554	1106	385	192	810	837	373	518	499	256	493	1154
UNWEIGHTED TOTAL	1570	88	210	411	470	123	244	467	175	525	1064	384	151	796	774	175	477	583	335	429	1141
Definitely	33%	19%	28%	34% B	34% B	24%	28%	39% FG	33%	34%	34%	32%	31%	32%	35%	23%	35% P	39% P	33% P	30%	35%
Probably	37%	46%	38%	38%	40%	24%	38% F	36% F	40% F	40% F	38%	37%	31%	35%	39%	45% QRS	36%	35%	34%	39%	36%
Probably not	17%	20%	15%	17%	15%	26% HJ	17%	15%	18%	16%	16%	15%	22%	19%	15%	17%	18%	15%	18%	16%	17%
Definitely not	12%	13%	18% E	12%	9%	25% HIJ	16% J	10%	9%	9%	11%	16% K	15%	14%	11%	16%	10%	10%	14%	14%	11%
Refused	*%	1%	-	-	-	-	-	-	-	*%	*%	-	-	-	*%	-	-	*%	-	-	*%
DK/NA	1%	1%	1%	*%	1%	1%	*%	1%	-	1%	1%	*%	1%	1%	1%	-	*%	1%	1%	*%	1%

Comparison Groups: BCDE/FGHIJ/KLM/NO/PQRS/TU
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q8. IF YOU SIGNED UP FOR THIS "DO NOT TRACK" SERVICE, WOULD YOU WANT TO BE ABLE TO SPECIFY EXCEPTIONS FOR SPECIFIC COMPANIES OR ORGANIZATIONS?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		REGION					SUB-REGION							COMMUNITY SIZE				EMPLOYMENT				
	TOTAL	Atla-ntic	QC	ON	Prai-ries	BC	Tor.	Mtl	Van.	MB	SK	AB	Can. Excl. QC	1M+	100K-1M	5K-100K	Under 5K	Full Time	Part Time	Home-maker	Unemp loyed	Re-tired
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)	(V)
TOTAL	1647	125	370	640	291	222	279	193	114	61	51	179	1277	692	305	457	193	841	171	60	88	203
UNWEIGHTED TOTAL	1570	194	358	405	410	203	173	181	101	105	92	213	1212	579	305	439	247	790	141	62	74	262
Yes	58%	57%	53%	63% C	58%	54%	66% I	56%	50%	56%	55%	60%	60%	60%	63% P	54%	55%	62% V	61% V	61% V	63% V	37%
No	34%	39% D	38% D	29%	37% D	40% D	22%	36% G	45% GM	43% G	41% G	35% G	33% G	32%	31%	40% NO	36%	33%	29%	31%	29%	52% RSTU
Maybe/it depends	6%	4%	8%	7%	4%	5%	9% J	8% J	4%	2%	3%	5%	5%	7%	4%	5%	6%	5%	7%	8%	5%	7%
Refused	*%	-	*%	1%	-	1%	1%	-	-	-	-	-	1%	*%	1%	*%	1%	-	-	-	1%	2%
DK/NA	1%	*%	2%	1%	*%	1%	2%	*%	1%	-	1%	*%	1%	1%	1%	1%	2%	1%	3%	-	1%	2%

Comparison Groups: BCDEF/GHIJKLM/NOPQ/RSTUV
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q8. IF YOU SIGNED UP FOR THIS "DO NOT TRACK" SERVICE, WOULD YOU WANT TO BE ABLE TO SPECIFY EXCEPTIONS FOR SPECIFIC COMPANIES OR ORGANIZATIONS?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		FAMILY INCOME				EDUCATION					LANGUAGE			GENDER		AGE				KIDS <18	
	TOTAL	Under $20K	$20K Under $40K	$40K Under $80K	$80K More	Less H.S.	H.S.	Comm. Coll.	Some Univ.	Univ. Deg.	Eng.	Fre.	Other	M	F	18-29	30-44	45-59	60+	Yes	No
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)
TOTAL	1647	100	224	419	494	120	249	502	186	554	1106	385	192	810	837	373	518	499	256	493	1154
UNWEIGHTED TOTAL	1570	88	210	411	470	123	244	467	175	525	1064	384	151	796	774	175	477	583	335	429	1141
Yes	58%	59%	58%	59%	65%	43%	49%	60% FG	68% FG	61% FG	59%	54%	61%	58%	58%	66% RS	62% RS	54% S	46%	65% U	55%
No	34%	31%	35%	34%	30%	49% HIJ	39% I	33%	27%	33%	35%	37%	30%	35%	34%	28%	32%	37% P	44% PQ	28%	37% T
Maybe/it depends	6%	7%	5%	6%	4%	2%	10% FIJ	6% F	4%	5%	5%	7%	7%	5%	7%	6%	5%	7%	6%	6%	6%
Refused	*%	2%	-	-	-	1%	*%	*%	1%	*%	*%	*%	1%	*%	*%	-	-	-	3%	-	1%
DK/NA	1%	1%	2%	1%	1%	5% H	1%	*%	1%	1%	1%	1%	2%	1%	1%	1%	1%	1%	1%	1%	1%

Comparison Groups: BCDE/FGHIJ/KLM/NO/PQRS/TU
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q9. WHICH OF THE FOLLOWING OPTIONS WOULD YOU PREFER TO USE IF YOU WERE GOING TO CONSENT TO THE TRACKING OF YOUR ONLINE ACTIVITY ON A PARTICULAR WEBSITE?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		REGION					SUB-REGION							COMMUNITY SIZE				EMPLOYMENT				
	TOTAL	Atla-ntic	QC	ON	Prai-ries	BC	Tor.	Mtl	Van.	MB	SK	AB	Can. Excl. QC	1M+	100K-1M	5K-100K	Under 5K	Full Time	Part Time	Home-maker	Unemp loyed	Re-tired
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)	(V)
TOTAL	1647	125	370	640	291	222	279	193	114	61	51	179	1277	692	305	457	193	841	171	60	88	203
UNWEIGHTED TOTAL	1570	194	358	405	410	203	173	181	101	105	92	213	1212	579	305	439	247	790	141	62	74	262
Checking an 'opt-in' box on the website (this means that the website does not track you unless you check the box)	75%	79% C	57%	79% C	81% C	83% C	78% H	60%	84% H	81% H	81% H	81% H	80% H	75%	76%	76%	71%	76%	77%	77%	66%	70%
Checking an 'opt-out' box on the website (this means that the website will track you until you check the box)	19%	16%	33% BDEF	16%	14%	13%	20%	33% IJKLM G	12%	13%	15%	15%	15%	21%	19%	17%	19%	20%	21%	16%	22%	17%
Neither, there should be no tracking at all	4%	2%	8% BDEF	2%	3%	3%	1%	6% G	2%	6%	3%	3%	3%	3%	4%	4%	6%	3%	1%	4%	6%	7% RS
Other	*%	*%	1%	-	-	-	-	1%	-	-	-	-	*%	*%	*%	*%	*%	*%	-	-	-	1%
Refused	1%	1%	-	1%	*%	1%	1%	-	1%	-	1%	*%	1%	1%	1%	*%	2%	*%	-	1%	1%	3% R
DK/NA	1%	1%	1%	2%	1%	1%	1%	1%	1%	-	-	1%	1%	1%	1%	2%	2%	1%	1%	2%	5%	3% R

Comparison Groups: BCDEF/GHIJKLM/NOPQ/RSTUV
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q9. WHICH OF THE FOLLOWING OPTIONS WOULD YOU PREFER TO USE IF YOU WERE GOING TO CONSENT TO THE TRACKING OF YOUR ONLINE ACTIVITY ON A PARTICULAR WEBSITE?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		FAMILY INCOME				EDUCATION					LANGUAGE			GENDER		AGE				KIDS <18	
	TOTAL	Under $20K	$20K Under $40K	$40K Under $80K	$80K More	Less H.S.	H.S.	Comm. Coll.	Some Univ.	Univ. Deg.	Eng.	Fre.	Other	M	F	18-29	30-44	45-59	60+	Yes	No
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)
TOTAL	1647	100	224	419	494	120	249	502	186	554	1106	385	192	810	837	373	518	499	256	493	1154
UNWEIGHTED TOTAL	1570	88	210	411	470	123	244	467	175	525	1064	384	151	796	774	175	477	583	335	429	1141
Checking an 'opt-in' box on the website (this means that the website does not track you unless you check the box)	75%	69%	77%	75%	77%	74%	68%	77% G	73%	78% G	80% L	61%	73% L	73%	77%	75% S	78% S	77% S	66%	76%	74%
Checking an 'opt-out' box on the website (this means that the website will track you until you check the box)	19%	23%	17%	22%	18%	14%	25% FHJ	18%	22%	18%	16%	30% KM	19%	21%	17%	21%	18%	17%	22%	20%	19%
Neither, there should be no tracking at all	4%	2%	4%	2%	3%	10% GHJ	3%	4%	5%	3%	3%	7% K	4%	4%	4%	3%	2%	5% Q	7% PQ	2%	4%
Other	*%	-	-	-	*%	-	*%	-	-	*%	*%	1%	-	*%	*%	-	*%	*%	1%	-	*%
Refused	1%	3%	1%	-	*%	1%	1%	1%	-	*%	1%	-	1%	1%	*%	*%	-	*%	3% PR	*%	1%
DK/NA	1%	3%	1%	1%	1%	-	3%	1%	1%	2%	1%	*%	3%	1%	1%	1%	1%	1%	2%	1%	1%

Comparison Groups: BCDE/FGHIJ/KLM/NO/PQRS/TU
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q10. WHICH ONE OF THE FOLLOWING SHOULD BEAR THE MOST RESPONSIBILITY FOR THE COSTS OF CREATING AND MAINTAINING A NATIONAL "DO NOT TRACK" LIST?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		REGION					SUB-REGION							COMMUNITY SIZE				EMPLOYMENT				
	TOTAL	Atla-ntic	QC	ON	Prai-ries	BC	Tor.	Mtl	Van.	MB	SK	AB	Can. Excl. QC	1M+	100K-1M	5K-100K	Under 5K	Full Time	Part Time	Home-maker	Unemp loyed	Re-tired
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)	(V)
TOTAL	1647	125	370	640	291	222	279	193	114	61	51	179	1277	692	305	457	193	841	171	60	88	203
UNWEIGHTED TOTAL	1570	194	358	405	410	203	173	181	101	105	92	213	1212	579	305	439	247	790	141	62	74	262
Online marketers, data brokers, and other groups who track online behaviour	39%	38%	30%	40% C	49% BCDF	36%	40%	34%	33%	38%	46%	54% GHIJM	41%	39%	46% PQ	36%	34%	39% S	28%	56% RSUV	34%	41% S
The federal government	21%	19%	26% DEF	20%	18%	18%	21%	24%	21%	16%	23%	17%	19%	22%	22%	21%	17%	21% T	27% TV	11%	23%	17%
Internet Service Providers	20%	27% E	21% E	20%	15%	22% E	19%	22% KL	19%	23% K	10%	13%	20% KL	19%	18%	21%	24%	21%	21%	12%	17%	20%
Consumers who sign up for the service	16%	13%	16%	18%	15%	16%	18%	16%	14%	21%	17%	13%	16%	16%	13%	18%	20%	17%	21%	14%	16%	13%
Other	1%	-	2% E	-	*%	2%	-	3%	4%	-	-	*%	*%	1%	-	*%	1%	1%	*%	-	-	1%
No one	1%	-	2%	1%	1%	1%	1%	1%	3%	1%	-	1%	1%	1%	*%	1%	1%	1%	1%	2%	1%	3%
Refused	1%	-	-	1%	*%	1%	1%	-	2%	-	-	*%	1%	1%	1%	-	*%	*%	-	-	2%	3% R
DK/NA	2%	3%	2%	1%	1%	4%	1%	1%	4% L	1%	4%	*%	2% L	1% O	*%	3% O	3% O	1%	3%	4%	6% R	3%

Comparison Groups: BCDEF/GHIJKLM/NOPQ/RSTUV
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

Public Interest Advocacy Centre - Canadians Attitudes Toward 'Do Not Track' - April 2009

Q10. WHICH ONE OF THE FOLLOWING SHOULD BEAR THE MOST RESPONSIBILITY FOR THE COSTS OF CREATING AND MAINTAINING A NATIONAL "DO NOT TRACK" LIST?

SUBSAMPLE: THOSE WITH INTERNET ACCESS

		FAMILY INCOME				EDUCATION					LANGUAGE			GENDER		AGE				KIDS <18	
	TOTAL	Under $20K	$20K Under $40K	$40K Under $80K	$80K More	Less H.S.	H.S.	Comm. Coll.	Some Univ.	Univ. Deg.	Eng.	Fre.	Other	M	F	18-29	30-44	45-59	60+	Yes	No
	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)	(M)	(N)	(O)	(P)	(Q)	(R)	(S)	(T)	(U)
TOTAL	1647	100	224	419	494	120	249	502	186	554	1106	385	192	810	837	373	518	499	256	493	1154
UNWEIGHTED TOTAL	1570	88	210	411	470	123	244	467	175	525	1064	384	151	796	774	175	477	583	335	429	1141
Online marketers, data brokers, and other groups who track online behaviour	39%	29%	29%	37%	46% BCD	28%	29%	35%	45% FGH	47% FGH	44% LM	30%	30%	40%	38%	36%	41%	38%	40%	36%	40%
The federal government	21%	24%	23%	22%	16%	25%	24%	21%	21%	19%	18%	28% K	27% K	22%	19%	28% QRS	19%	18%	19%	23%	20%
Internet Service Providers	20%	21%	22%	24% E	16%	27%	19%	22%	16%	18%	20%	20%	20%	20%	20%	16%	19%	25% PQ	20%	19%	20%
Consumers who sign up for the service	16%	19%	21%	14%	19%	16%	21% J	17%	15%	14%	15%	18%	19%	15%	18%	18%	18%	15%	14%	17%	16%
Other	1%	-	*%	1%	1%	1%	-	1%	1%	1%	*%	1%	*%	*%	1%	-	1%	1%	1%	1%	1%
No one	1%	1%	1%	1%	1%	2%	1%	1%	1%	1%	1%	2%	1%	1%	1%	-	1%	2%	2%	1%	1%
Refused	1%	1%	1%	*%	-	-	1%	*%	1%	*%	1%	-	-	1%	1%	-	-	1%	2%	*%	1%
DK/NA	2%	4%	3%	1%	1%	2%	4% J	3%	-	1%	2%	1%	2%	2%	2%	2%	1%	2%	2%	2%	2%

Comparison Groups: BCDE/FGHIJ/KLM/NO/PQRS/TU
Independent T-Test for Means, Independent Z-Test for Percentages
Upper case letters indicate significance at the 95% level.

APPENDIX B – EXPERT QUESTIONNAIRE RESULTS

Questionnaire

Please answer, if applicable, the following questions:

1. How do you expect the introduction of a “Do Not Track List” to affect the growth or operation of products and services providers on electronic platforms?

2. What are the biggest technological challenges in enforcing a “Do Not Track List”?

3. Are there other barriers to implementing or enforcing a “Do Not Track List” in Canada?

4. What would be the estimated costs of having a “Do Not Track List” in the Canadian e-commerce industry?

5. Should the “Do Not Track List” be regulated or self-regulatory? How should the “Do Not Track List” be enforced?

6. Do you view the use of personal information obtained from user social profiles from popular networking sites for targeted marketing purposes as intrusive behaviors?

7. Should users of social networking sites or other online services assume any risk (i.e. financial, personal, privacy, etc.) of providing any personal, including sensitive, information to the service provider?

8. Do you believe that educating consumers and increasing their awareness of the technologies used to track their online activities, the means of obtaining their personal information, and the use of such information, are sufficient to protect consumer interests and their privacy rights?

9. Evaluate the potential effectiveness and benefits of a “Do Not Track List” as means of protecting consumers’ privacy rights.

10. If you believe there are other important factors to consider in the introduction of a “Do Not Track List” in Canada that is not mentioned above, please briefly explain them.

End of Questionnaire
Thank you!

Drew McArthur Response to Questionnaire

1. How do you expect the introduction of a “Do Not Track List” to affect the growth or operation of products and services providers on electronic platforms?

   Depending upon your view of what behavioural marketing messages are (some providers have been tracking user preference for a long time to provide product recommendations which used to be known as “database marketing”) marketers would consider this a large inconvenience. They would likely argue that they are providing the user with a better experience through the use of such tools as database marketing, and would see their ability to better target their audience as being limited or threatened by a “Do Not Track List”.

2. What are the biggest technological challenges in enforcing a “Do Not Track List”?

   It seems to me that the only way enforcement could be performed is in a similar to way to PIPEDA and the Do Not Call list. That is through complaint investigation. Web crawlers might be able to detect the collection or tracking of information, but how would an agency know which consumers who use a particular website had not consented to the use of tracking technology?

3. Are there other barriers to implementing or enforcing a “Do Not Track List” in Canada?

   Without thinking through all the implications, there may be many logistical barriers to implementing a do not track list. Canada already has legislation in place that requires organizations to inform users of the purposes for the collection and use of their information, so in essence, we have legislation that allows consumers to take action against unauthorized collection of information.

4. What would be the estimated costs of having a “Do Not Track List” in the Canadian e-commerce industry?

   More importantly, who would be the appropriate party to pay for a Do Not Track List. I will argue that having the telecommunications carriers pay for the Do Not Call List was the wrong group, since all the paying telecom carriers already had implemented Do Not Call Lists of their own which were working well. It is inappropriate, in my view, to have a reputable industry group pay for the poor practices of other organizations.

5. Should the “Do Not Track List” be regulated or self-regulatory? How should the “Do Not Track List” be enforced?

   As noted above, the enforcement already exists in Canada, through either provincial private sector privacy legislation (PIPA in Alberta and BC) or PIPEDA.

6. Do you view the use of personal information obtained from user social profiles from popular networking sites for targeted marketing purposes as intrusive behaviors?

   I believe the unauthorized collection and use of information from social profiles to be contrary to PIPEDA, and therefore inappropriate.

7. Should users of social networking sites or other online services assume any risk (i.e. financial, personal, privacy, etc.) of providing any personal, including sensitive, information to the service provider?

   Users should be aware of the consequences of providing their personal information in any circumstance, and the provision of such information should be governed by privacy legislation. Education of users is one of the mandates of the Federal and Provincial Privacy Commissioners, and there are a number of educational support tools made available regarding social networking sites.

8. Do you believe that educating consumers and increasing their awareness of the technologies used to track their online activities, the means of obtaining their personal information, and the use of such information, are sufficient to protect consumer interests and their privacy rights?

   Education is only one element of an appropriate regime for the collection and use of personal information. Federal and provincial privacy legislation already provide for education and enforcement schemes to protect Canadians.

9. Evaluate the potential effectiveness and benefits of a “Do Not Track List” as means of protecting consumers’ privacy rights.

   I think this is already accomplished by PIPEDA, and I do not see a Do Not Track List as providing any further benefits to protecting consumers.

10. If you believe there are other important factors to consider in the introduction of a “Do Not Track List” in Canada that is not mentioned above, please briefly explain them.

    I believe I have addressed the key issues, and would recommend a discussion with Canada’s privacy commissioners prior to undertaking the development of such a list. As we have noted with the Do Not Call List, there are a number of unanticipated logistical issues, and in my view, these would be best worked through in concert with the existing privacy legislation.

End of Questionnaire

Valerie Steeves Response to Questionnaire

1. How do you expect the introduction of a “Do Not Track List” to affect the growth or operation of products and services providers on electronic platforms?

   I don’t think it will. The direct sales and marketing approach will continue, even if people opt out of the more aggressive forms of online marketing that are based on seamless and continuous surveillance. I also don’t think it should matter. The practices of online tracking are invasive and manipulative and should be curtailed on that basis.

2. What are the biggest technological challenges in enforcing a “Do Not Track List”?

   The fact people have multiple IP addresses. I’d much prefer an opt-in system where I could register an IP address if I want to be tracked. Easier to do technically and a lot more privacy protective. But I also think this isn’t likely to fly at a policy level because the government has privileged e-commerce over privacy for the past 15 years.

3. Are there other barriers to implementing or enforcing a “Do Not Track List” in Canada?

   Frankly, I don’t think companies will respect it. I also think they’ll offer “benefits” to those who are tracked, and pretty soon, switch to restricting services to those who won’t consent to being tracked. We see the same thing with shopper cards – I pay extra to cover the costs of collecting others’ info and giving them “rewards”. So we’ll need clear policy guidelines that make it clear you can’t punish people for registering on the list, including making those people pay for the costs of market surveillance of others.

4. What would be the estimated costs of having a “Do Not Track List” in the Canadian e-commerce industry?

   Don’t know.

5. Should the “Do Not Track List” be regulated or self-regulatory? How should the “Do Not Track List” be enforced?

   Regulated. Enforced by complaints to the Privacy Commissioner AND fines for tracking without permission.

6. Do you view the use of personal information obtained from user social profiles from popular networking sites for targeted marketing purposes as intrusive behaviors?

   You bet.

7. Should users of social networking sites or other online services assume any risk (i.e. financial, personal, privacy, etc.) of providing any personal, including sensitive, information to the service provider?

   No. The obligation NOT to collect should be placed on corporations, especially because these sites do not present themselves as market research labs but places where you can “be yourself” and “connect with friends”.

8. Do you believe that educating consumers and increasing their awareness of the technologies used to track their online activities, the means of obtaining their personal information, and the use of such information, are sufficient to protect consumer interests and their privacy rights?

   No. We need laws to restrict collection. Responsibilizing individuals will do nothing to curb invasive practices and provide a false sense of legitimacy to socially destructive forms of surveillance.

9. Evaluate the potential effectiveness and benefits of a “Do Not Track List” as means of protecting consumers’ privacy rights.

   Better than nothing. Not good enough because it does nothing to bring corporate practices into line with what’s good for a democracy. We should use PIPEDA to limit purposes for collection, and make it clear that companies can’t watch everything just because they might be able to benefit from it. Let’s face it – this has nothing to do with customer convenience or service and everything to do with mining the social world and reconstructing it for the purposes of manipulating people’s behaviours. If you have a product to sell, let me opt in to learning about it. Watching me while I play, talk, work and surf so you can change my behaviour to make a sale is offensive at a core level and we should be restricting this kind of marketing. It’s also absolutely crucial that we stop the ways in which corporate marketing fractures online public spaces for debate and discussion. Structuring my online environment by limiting what I see to what the service provider guesses I “want” to see (or what they want me to see so I’ll behave accordingly) is at its core incredibly undemocratic and weakens the public sphere.

10. If you believe there are other important factors to consider in the introduction of a “Do Not Track List” in Canada that is not mentioned above, please briefly explain them.

End of Questionnaire

Jim Nehf Response to Questionnaire

1. How do you expect the introduction of a “Do Not Track List” to affect the growth or operation of products and services providers on electronic platforms?

   I do not have sufficient background or experience to address this question.

2. What are the biggest technological challenges in enforcing a “Do Not Track List”?

   Not being a technology expert, this is difficult to answer. However, to be successful a DNT list must identify individuals in some unique way. Unlike a Do Not Call list, which applies to unique telephone numbers, a DNT list must identify people by names or some other identifier. Names are not unique and can have many variations, and the use of identifiers such as Social Security Numbers is obviously problematic for privacy reasons. Perhaps IP addresses could be used for some tracking platforms (targeted ads while surfing the Internet), but that would not address the problem completely. Home addresses might be used for other purposes (direct mailings), but existing laws already allow consumers to block most junk mail (at least in the US).

3. Are there other barriers to implementing or enforcing a “Do Not Track List” in Canada?

   A large industry has already developed in this field, so there would be strong opposition and political pressure to create loopholes and exceptions. Also, governments rely increasing on data brokers to provide information about individuals that is either too expensive or illegal for governments to collect and organize. Thus, opposition will be entrenched and difficult to overcome.

4. What would be the estimated costs of having a “Do Not Track List” in the Canadian e-commerce industry?

   I do not know. The history of privacy debates in general, however, is that industry will have little difficulty providing cost estimates—both compliance costs and the lost consumer “benefits” of tracking and profiling. On the other side, privacy advocates will find it difficult to quantify the consumer benefits of a DNT list because most of those benefits are not easily converted to dollar values. Thus, you end up with an incomparability problem that usually results in no political action.

5. Should the “Do Not Track List” be regulated or self-regulatory?

   How should the “Do Not Track List” be enforced? Enforcement will be difficult in either system, although I favor a regulated system, with heavy fines imposed against violators. The data collection industry is too diverse and opaque for self regulation to work. If individuals are tracked and profiled, they will have no way of knowing who collected the data and passed it along to someone else. Thus, private

enforcement by individuals will be rare. Giving legal standing to privacy and consumer organizations could help, with attorney's fees and other awards given for successful legal actions.

6. Do you view the use of personal information obtained from user social profiles from popular networking sites for targeted marketing purposes as intrusive behaviors?

   Yes. In individual instances, it may seem benign, but as profiling get more detailed and sophisticated, and as new technologies emerge (RFID, etc.), generally accepted societal norms of privacy and anonymity will be lost. While this would not be the end of the world as we know it, it would certainly be a far different world than the one in which we now live.

7. Should users of social networking sites or other online services assume any risk (i.e. financial, personal, privacy, etc.) of providing any personal, including sensitive, information to the service provider?

   They should assume as little privacy risk as possible. People who use such networks have a right to assume that their private data will be secure and will only be used for their intended purposes. If a site wishes to use data in other ways, it must make this intent known to its customers explicitly (explaining precisely what those uses will be), and receive their explicit consent to those uses. If requiring truly informed consent means that few users will agree (as I suspect it will), the site may decide to charge for its services. So be it. People have no effective way of pricing the value of their personal information because they have know idea where it will end up and how it will be used. The only effective way to protect privacy is to keep personal information secure and used only for the intended purpose.

8. Do you believe that educating consumers and increasing their awareness of the technologies used to track their online activities, the means of obtaining their personal information, and the use of such information, are sufficient to protect consumer interests and their privacy rights?

   No. Disclosure and information may be effective consumer protection mechanisms in other areas, but with privacy disclosure does not work. People have no way of knowing how their data will be used, how it will be aggregated with other data, how it will be transferred and to whom, and how it can ultimately help or harm them. Moreover, if a data collector does use personal information in a way that a consumer does not intend or authorize, and even if the breach results in some harm (ID theft, etc.), tracing the harm to the data breacher is often impossible. In short, consumers cannot effectively weigh the costs and benefits of data sharing, so disclosure of technologies and data collection practices provides only a false sense of consumer protection. It is analogous to allowing cancer-causing elements to be ingredients in food, with disclosures to consumers about the contents. Consumers simply cannot evaluate the risks.

9. Evaluate the potential effectiveness and benefits of a “Do Not Track List” as means of protecting consumers’ privacy rights.

   An effective DNT list would be a monumental achievement and could reverse the enormous privacy invasions that have occurred to date. Benefits would include the restoration of the degree of privacy and anonymity that people have enjoyed for many years when they chose to live at a particular address, order merchandise through the mails, watch television, listen to radio, take money out of their checking account, or use their computers. In the past, engaging in any of these every-day activities involved giving up a minimum amount of information to an entity that had narrowly defined ways of using it. At present, if we choose to live in the modern world, our private lives are an open book, and there is little that we can do about it unless the law makes it illegal to track us.

10. If you believe there are other important factors to consider in the introduction of a “Do Not Track List” in Canada that is not mentioned above, please briefly explain them.

    The problems mentioned above (overcoming industry’s costs-benefit arguments, confronting the government interest in using data brokers, and ensuring effecgtive enforcement) are huge obstacles. I admire the effort, and I wish the project success.

End of Questionnaire