PUBLIC INTEREST ADVOCACY CENTRE
LE CENTRE POUR LA DEFENSE DE L'INTERET PUBLIC
ONE Nicholas Street, Suite 1204, Ottawa, Ontario, Canada K1N 7B7
Tel: (613) 562-4002. Fax: (613) 562-0007. e-mail: piac@piac.ca. http://www.piac.ca

March 15, 2010

VIA E-Mail ONLY

Melanie Millar-Chapman
Office of the Privacy Commissioner of Canada
112 Kent Street
Place de Ville, Tower B, 3rd Floor
Ottawa, ON
K1A 1H3

Dear Ms. Millar-Chapman:

Re: 2010 Consumer Privacy Consultations – Comments of PIAC

The Public Interest Advocacy Centre (PIAC) is pleased to enclose their comments on the privacy implications of online tracking, profiling and targeting for the 2010 Consumer Privacy Consultations of the Office of the Privacy Commissioner of Canada.

As well, PIAC is interested in participating in panel discussions for the consultation and we look forward to hearing from the OPCC in this regard.

Thank you.

Yours truly,

John Lawford
Counsel

Janet Lo
Counsel

encls.

2010 Consumer Privacy Consultations

Understanding Online Tracking, Profiling and Targeting

Comments of the Public Interest Advocacy Centre

March 15, 2010

John Lawford, Counsel
(613) 562-4002 x 25
lawford@piac.ca

Janet Lo, Counsel
(613) 562-4002 x 24
jlo@piac.ca

Public Interest Advocacy Centre
ONE Nicholas Street, Suite 1204
Ottawa, Ontario K1N 7B7

About the Public Interest Advocacy Centre

The Public Interest Advocacy Centre (PIAC) seeks to advance the interests of individuals and groups who are generally unrepresented or underrepresented in issues of major public concern. We champion those issues that involve the delivery of important public and utility services. The Centre seeks to ensure that the public interest is served, and not neglected, by decision makers in government and the private sector when decisions are made about consumer issues. The Centre undertakes solid legal and research services on behalf of consumers. The Centre focuses primarily on consumer issues concerning telecommunications, energy, privacy, the information highway, electronic commerce, financial services, broadcasting, and competition law.

PIAC has published two recent reports on behavioural marketing and privacy. In 2008, PIAC published a report entitled "All in the Data Family: Children's Privacy Online", reviewing the privacy risks to children when commercial entities target children through personal information collected when children join online playgrounds.[1] In 2009, PIAC published "A 'Do Not Track List' for Canada?", a report that examines online behavioural targeted advertising and online behavioural tracking.[2]

PIAC's Survey of Consumer Attitudes

Last year, PIAC conducted a survey to gauge consumer knowledge of online behavioural targeting practices, consumer attitudes towards behavioural marketing and the desirability of a "Do Not Track List". The survey was conducted by Environics Research Group with 1,570 Canadians aged 18 and over, respondents who were representative of gender, age, family income, education, language, employment, region and community size demographics in Canada.

In PIAC's findings, we observed that consumers were not comfortable with unfettered collection and use of their personal information overall. Specifically, when asked about their comfort level with online tracking for the purpose of targeted and behavioural advertising, only 8% of respondents responded that they were "very comfortable" and 17% were "somewhat comfortable". By contrast, a full 25% were "not very comfortable" and nearly half (49%) indicated they were "not at all comfortable" with such tracking. An even higher percentage of respondents expressed discomfort with companies and organizations that share information about their behaviours as consumers with third party organizations for the purpose of targeting advertising, with 25% "not very comfortable" and 53% "not at all comfortable".

PIAC's survey also suggests that consumers are more comfortable with online tracking for the purpose of customer service or advertising by a company or organization they

[1] Public Interest Advocacy Centre, "All in the Data Family: Children's Privacy Online" (September 2008), online: http://www.piac.ca/privacy/children_s_privacy_threatened_by_play_websites_and_social_networking.
[2] Public Interest Advocacy Centre, "A 'Do Not Track List' for Canada?" (December 2009), online: http://www.piac.ca/privacy/tracking_consumers_online_behavioural_targeted_advertising_and_a_do_not_track_list_in_canada.

have prior dealings with. Almost half of consumers were most likely to consent to the 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 would be 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%) and even fewer were likely to consent to the use of such information for targeted advertising by companies or organizations they have not 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 comfortable with online tracking and targeted advertising by market researchers and data brokers (9%).

The survey was conducted as part of PIAC's report on consumer tracking and behavioural targeted advertising and the full survey results are produced as Appendix A to that report.[3]

Definition(s) of Personal Information

Behavioural targeting or tracking puts the definition of "personal information" as it is used in Canada under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) severely to the test. This is due to the concept of "de-identification" which is generally cited by online advertisers and data aggregators as their method of protecting individual privacy while permitting their industry to function. The goal of de-identification is to make information no longer "personally identifiable information" – a concept imported by marketers from European data protection law.[4]

The EU's Working Party on the Protection of Individuals with Regard to the Processing of Personal Data proposed the following definition in its Directive 95/46/EC (adopted 20 June 2007):

> "Personal data shall mean any information *relating to* an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[5] [Emphasis added.]

---

[3] See Appendix A of Public Interest Advocacy Centre, "A 'Do Not Track List' for Canada?" (December 2009), online: http://www.piac.ca/privacy/tracking_consumers_online_behavioural_targeted_advertising_and_a_do_not_track_list_in_canada.

[4] See Robert Ellis Smith, "Is Identity of Your Computer 'Personal Data'?" *Privacy Journal*, Volume 35, Number 11 (September 2009) at 1 and 7.

[5] See Article 29 Working Party, Opinion 4/2007 on the concept of personal data, online: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

The European definition of "personal data" is akin to that in PIPEDA. PIPEDA defines "personal information" as:

> "personal information" means information *about* an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.[6] [Emphasis added.]

Under both definitions, it is crucial to note that while personal information or personal data must be "in relation to" or "about" an "identifiable" "individual" or "natural person" that the data need not, at the time of its creation, collection, use, disclosure or at any time in its life cycle, necessarily identify on its own, or together with other information identify or potentially identify a person. That is, the person must be a "real" person, and identifiable in some way as such, but need not be identified by the method of the personal data or personal information in issue. When that personal information or personal data is used to identify that person, or is used for any other purpose, however, certain rules apply, at least in Canada and in the E.U.

The theory employed by behavioural marketers, however, is that personal information may be freely collected, used and disclosed, for targeted marketing purposes and market research (with minimum, often opt-out) consent, provided the data is in some way "anonymized" or "de-identified" by removing key data elements such as name or birthdate – in other words, taking out the PII. They call this removed information "personally identifiable information" (PII).[7] As explained by Ellis Smith:

> The debate is muddled by the use in Europe of the term personally identifiable information (PII), which is information that can be used to locate or identify an individual, regardless of its sensitivity. Unique ID numbers, mother's maiden name, fingerprints, addresses, and photographs are examples.
>
> This term has found its way into usage in U.S. government documents. Corporate America seems to have embraced the term (using it to denote what is properly called personal information).[8]

Ellis Smith explains that the EU concept of PII is an add-on to the definition of "personal data" for situations where the context may not appear serious, nonetheless, EU regulators have added this extra layer of data protection by listing certain data elements as special, with special handling characteristics, even if they do not attract the high standards of sensitivity, precisely as they could be used to identify the person.

---

[6] PIPEDA, subsection 2(1), definition of "personal information". There is no definition of "personally identifiable information" in PIPEDA.

[7] Note that in some cases, website operators (initial collectors in the behavioural targeting chain) often purportedly deem, by the fiat of their contracts and privacy policies, that all personal information shall be considered PII. Google's is a classic. See Google.ca Privacy Policy (online: http://www.google.ca/intl/en/privacypolicy.html , Last modified: March 11, 2009): ""Personal information" is information that you provide to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google." [Emphasis added.]

[8] See Robert Ellis Smith, *op. cit.* at 1.

The concept of PII as those data elements which are liable to identify a person has no place in Canadian law, however. Whether Canada should add an extra layer of protection for such PII as the Europeans have done is a matter for PIPEDA review. What Canada should NOT do is import this unwritten and non-legal definition into our discussion of what is going on with Canadians' personal information online, even if online behavioural marketers habitually use the concept in privacy policies, contracts with third parties and in terms of use.

The OPCC has made several rulings affirming that personal information is information *about a particular individual*, not that the information must, at that time nor even in some realistically likely fashion in the future, ever be capable of, on its own or combined with other information, identifying that person.[9] This difference appears academic, philosophical or ephemeral, however it is in fact key – and the key to understanding both consumer and consumer advocate unease with, and rights to avoid, behavioural targeting. The result of the confusion of PII with the entire sphere of personal information, however, is cataclysmic from a personal privacy perspective.

We therefore call upon the OPCC to impose a level of intellectual rigour in its consultations with industry and other stakeholders on behavioural targeting and to require participants to acknowledge that they cannot, in Canada at least, confidently base their logical and legal arguments upon the chimera of PII, rather than the Canadian law that protects all "personal information".

Consent

Likewise, the concept of "consent" to collection, use and disclosure of personal information is severely challenged in the face of behavioural targeting. On the one hand, there are assurances by marketers and related online participants in privacy policies that consent is ALWAYS obtained for all information, while on the other hand there are assurances that most of the aggregated data collection and processing requires no consent whatever (given the definition of PII as personal data adopted by most market players, above).

Google again is a standard example. Google's definitions of "aggregated non-personal information" and "sensitive information" both support the theory that personal information is limited to PII and both definitions attempt to limit recourse to the rules in PIPEDA that apply to personal information by ignoring or assuming consent:

[9] See, just on the issue of details of real estate transactions for example, the OPCCC findings in: PIPEDA Case Summary #2009-002, PIPEDA Case Summary #2008-390 and PIPEDA Case Summary #2006-349. In this latter case, the OPCCC stated: "Under section 2, personal information is defined as information about an identifiable individual. She noted that it states only that the individual must be "identifiable," not necessarily *identified*. Under each unit photograph is the street address of the building, and the unit number, thereby ensuring that each photograph of a unit could be traced back to the individual living in the unit." [Emphasis in original.]

> "Aggregated non-personal information" is information that is recorded about users and collected into groups so that it no longer reflects or references an individually identifiable user.[10]

That is, aggregated personal information is "non-personal information" and attracts no consent requirement. This is a "black-is-white" statement and one that cannot be made without examining each piece of information to see if it is indeed personal information on the definition we support detailed above.

> "Sensitive personal information" includes information we know to be related to confidential medical information, racial or ethnic origins, political or religious beliefs or sexuality and tied to personal information.[11]

That is, "sensitive personal information" is what Google defines it as, not how PIPEDA defines it (PIPEDA, Principle 4.3.4: "any information can be sensitive, depending on the context"). It is further limited to what "we [Google] know to be" sensitive information, that is, Google's actions are to be judged on its own subjective standard not that of an objective observer. Google continues by noting that it will only seek express (opt-in) consent for disclosure of sensitive information. Therefore, by implication, for all other personal information collection, use or disclosure, Google relies upon opt-out (implicit) consent which is theoretically obtained by a statement to this effect in the Google privacy policy or any of myriad other privacy policies depending on the service accessed.[12]

Such a course of action ignores any requirement to specify in any realistic detail what is being collected, used or disclosed by a behavioural marketer (for example, the DoubleClick privacy policy goes into some detail about cookies but does not provide the individual with any information on what information the cookies collect) and makes it impossible to obtain an informed consent to the use of the individual's personal information, which the Federal Court of Appeal has stated is the only real "consent standard" in PIPEDA.

Given that PIPEDA is a complaints-driven regime, it appears to be a cruel catch-22 that consumers are unaware of the extent of behavioural targeting using their personal information gleaned online because companies refuse to detail this use, thereby precluding any real ability of an individual to formulate a complaint.

---

[10] Google.ca Privacy Policy, *supra*.
[11] Google.ca Privacy Policy, *supra*.
[12] Google.ca Privacy Policy, *supra*: "Google only shares personal information with other companies or individuals outside of Google in the following limited circumstances: - We have your consent. We require opt-in consent for the sharing of any sensitive personal information." For other privacy policies, see Google Privacy Center: http://www.google.ca/intl/en/privacy.html. Note that if one follows the DoubleClick Privacy Policy (which states simply that DoubleClick "will use non-personal information about your browser and your activity at this site to serve ads on this and other sites" and then a link to a DART opt-out page, you will finally find a chart giving some limited detail of what information cookies can collect and use. See list of "targeting criteria" in the chart detailing the DART cookie, including "Location information from IP address" and the intriguing "User list", online: http://www.doubleclick.com/privacy/dart_adserving.aspx.

One might say that this is of little consequence if the result of such profiling is simply delivery of better targeted advertisements. In other words, if consent does not work, little harm can result. However, we beg to differ, as our discussion of our survey results shows that Canadians are uncomfortable with the concept of such individualized targeting occurring at all and as our detailing of the potential risks of profiling and social sorting, discussed below, also make clear.

One final argument over consent is the extent to which a company can demand personal information as a condition of supplying a service. In principle, PIPEDA Principle 4.3.3 should exclude all behavioural targeted advertising, as no advertising, and certainly no profiling of an individual is necessary to allow Internet users to access a website or to buy a product online.

However, as accepted in the OPCC's Facebook decision, the Internet economy runs on personal information as a "price" of using "free" services such as social networking and the OPCC has accepted this advertising and profiling as an "explicitly specified, and legitimate purpose" for personal information.[13] If this is an accepted principle, then 4.3.3 is simply a dead letter in relation to behavioural advertising, provided adequate notice of the use is given.

PIAC is especially concerned about youth privacy in an age where youth are engaging in social networking and other websites and online services that perform market surveillance as a business model. Elsewhere, PIAC has advocated for age-graduated levels of consent to reflect the reasonableness of information processing when dealing with the personal information of children and teens who are developing a social and personal sense of privacy and self-worth in their online interactions.[14] PIAC stands by its previous recommendations on youth privacy and encourages the OPCC consultations to consider how online tracking, profiling and targeting affect young consumers.

PIAC's final concern in relation to consent is the OPCC's refusal to impute a consent requirement where "publicly available" information has been enriched by data aggregators and data miners. In PIPEDA Case Summary #2009-004, *No Consent Required for Using Publicly Available Information Matched with Geographically Specific Demographic Statistics*, the OPCC allowed enrichment of phone book information with demographic information from Statistics Canada. What the OPCC may have failed to appreciate is the fact that white pages phone book information was gathered for a completely different purpose than that to which it was put by data miners. The purpose of white pages listing information is to permit telephone subscribers to contact other subscribers easily in order to get the full benefit of the "network effect" of having all users on the phone network easily contactable. When directories were produced in

---

[13] See PIPEDA Case Summary #2009-008, *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*, at paras. 130-1.

[14] See, for example, PIAC's report "All in the Data Family: Children's Privacy Online" (September 2008), online: http://www.piac.ca/privacy/children_s_privacy_threatened_by_play_websites_and_social_networking and PIAC's PIPEDA complaint against teen social networking site Nexopia (January 2010), online: http://www.piac.ca/privacy/piac_files_privacy_complaint_against_nexopia. .

machine-readable format, the CRTC allowed the provision of this information to other directory companies besides the incumbent local exchange providers on the basis of providing more competition in the directory business.[15] This provision was hemmed in by significant privacy principles.[16]

However, the OPCC, in bestowing the title of "publicly available" upon this type of personal information (directory information) and then refusing to require consent for the new use the information after its "enrichment" with yet more personal information simply guts PIPEDA Principle 4.5. It ignores the general safeguards that the CRTC sought to uphold over the years in many decisions on directories. It allows an entire industry to be constructed with the express purpose of doing indirectly what PIPEDA forbids directly. In our opinion, this decision ratifies a process that is clearly NOT in the public interest, and yet the purpose for which the phone data (and StatsCan data) was collected would in our opinion imply a requirement to only allow uses without consent that were *clearly in the public interest*, not the private interest of market actors.

Re-identification of Aggregated De-identified Data

As mentioned above, private companies generally employ various techniques to "anonymize" (or de-identify) the personal data they collect before imparting them or selling them to third parties. Behavioural targeted advertising companies integrate technology into their services intended to accomplish the same task. For instance, data linked to a certain customer's name or IP address, which could in turn be linked to an individual directly, may be assigned a unique randomized number by the company instead (e.g. Customer *#12345* spent *X* amount of time at this site and purchased a certain product). By omitting the name, address and IP address of the customer, the data is considered to be non-personal. Since restrictions on the collection and use of data become more lax once the "personal" aspect of the data is removed, the problem worsens as more and more data about an individual's online activity is collected, which once aggregated and analyzed, can serve to re-identify an individual quite accurately. Two reported examples of successful attempts to re-identify individuals through de-identified data have put into question the efficacy of current data de-identification techniques.[17]

In 2006, Netflix carried out a project providing a monetary incentive for researchers to improve their movie-recommendation system. The company provided data on 500,000 of its subscribers' ratings of various movies and removed the subscribers' names and other personally-identifiable information. Two researchers at the University of Texas,

---

[15] See, for example, Telecom Decision CRTC 95-3, *PROVISION OF DIRECTORY DATABASE INFORMATION AND REAL-TIME ACCESS TO DIRECTORY ASSISTANCE DATABASES* and Telecom Decision CRTC 95-14, *WHITE DIRECTORY - APPLICATION TO REVIEW AND VARY DECISION 95-3*

[16] See Telecom Decision CRTC 95-14: "(1) subscribers should be informed of the implications for their personal privacy of the use of telecommunications services, (2) subscribers should be able to maintain their current level of privacy at no additional charge, and (3) personal information should be collected, used and disclosed only with express consent, except where clearly in the public interest or as required by law."

[17] For more examples of the process of re-identification, see the Electronic Privacy Information Center's webpage: http://epic.org/privacy/reidentification/.

Arvind Narayanan and Vitaly Shmatikov, collated this data with reviews found in the database of the International Movie Database (or IMDb) and were able established the identity of two Netflix subscribers (IMDb's terms of use prevented them from executing a more comprehensive search of their records). According to the study, even attempting to complicate the re-identification task by inserting errors into the dataset would not overwhelm the researchers' algorithm used, which could theoretically identify up to 99% of the Netflix subscribers.

That same year, America Online released a three-month record of web searches of 657,000 of its American subscribers. While AOL attempted to protect its users' privacy by removing their screen names and IP addresses from the dataset of roughly 20 million web searches, researchers were able to identify individuals solely by analyzing the searches tied to their unique randomized customer identification number.

Thus, even a small amount of de-identified data on an individual, once combined with another dataset available either publicly or privately through sale, may still serve to re-identify the individual. In PIAC's view it is up to the companies that are engaged in data aggregation to put forth credible solutions to this problem, rather than require customers to bear the constant risk of re-identification. PIAC submits that where re-identification is possible or occurs, where those advertisers who de-identified the information can be shown to have negligently, deliberately or with reckless disregard allowed this information to be re-identified, that this should constitute a new use of personal information which *a priori* cannot have been consented to by the individual despite any attempted terms to the contrary in a privacy policy.

Limitations on the Scope of Tracking

In an interview with BBC News on behavioural tracking on the internet, Sir Tim Berners-Lee envisioned a scenario in which his insurance company would raise his premiums by 5% upon finding out that he has researched a number of books on a particular type of cancer online. It is relatively incontestable that information on an individual's medical conditions is sensitive and that such information may be used against the individual, not to mention that the mere existence of the internet activity mentioned above may lead to erroneous conclusions by the insurance company (the individual may have been researching his/her friend's condition or performing research for any other number of reasons).

While an advertising company may promise to place limitations on the scope of their tracking, e.g. by not recording a user's interest in certain "sensitive" subjects such as medical conditions or personal bankruptcy, the collection and use of such data must satisfy a more stringent consent requirement (effectively express or "opt-in" consent) in light of PIPEDA Principles 4.3.4 to 4.3.6. Yet, these principles are only enforced by individual complaint or theoretically by an OPCCC industry audit. As a result, few if any online marketers avert to these principles and instead create self-serving and easy to manage lists of what they in their sole discretion deem to be "sensitive".[18]

[18] See above, Google Privacy Policy in relation to "sensitive personal information".

A different approach is that of the European Commission, which in Article 8 of its Directive 95/46/EC, prohibits the processing of certain classes of personal data, namely "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[19] Likewise, there are decisions on the scope of "sensitive" information (health information in particular) from the Ontario Information and Privacy Commissioner: see OIPC's recent HO-007 and its discussion of s. 4(1) of PHIPA of Ontario. Nevertheless, this listing approach leaves room for companies to collect and use data not properly falling within an excluded class.

In addition, there are a number of potential harms regarding profiling and social sorting (detailed below) that will not be resolved by relying upon the "sensitivity" criterion.

Security of Stored Personal Data

While companies and organizations implement security measures to protect the data that they collect, store and use, the fact that sensitive personal data of consumers may be stored on multiple servers in different jurisdictions coupled with the fallibility of security measures is cause for concern. PIAC anticipates that this issue will return in greater detail during the course of the OPCC's Notice of Consultation and Call for Submissions relating to cloud computing.

Harms of Online Behavioural Targeted Advertising, Online Consumer Tracking and Consumer Profiling

Proponents of online behavioural targeted advertising and consumer tracking often boast benefits to the online consumer, such as customized settings or product recommendations based on the consumer's previous purchases or tastes. Marketers may also argue that behavioural advertising provides utility to the consumer, resulting in increased efficiencies and increased social welfare.

While PIAC recognizes that these marketing techniques may improve aspects of the consumer experience, we submit that few consumers fully understand the role and extent that data collection plays in providing behavioural targeted advertisements and consumer tracking. Consumer tracking, profiling and 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 may not always collect accurate information about individuals.[20] Where errors are collected and become part of a consumer's profile, targeted online

---

[19] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

[20] Philippa Lawson, "Techniques of Consumer Surveillance and Approaches to their Regulation in Canada and the USA" (March 2005), online: http://www.idtrail.org/files/Techniques%20of%20Consumer%20Surveillance%20w%20footnotes.pdf at p. 7. Lawson cites research suggesting that information in consumer profiles collected in the course of Customer Relationship Management is often riddled with errors.

advertisements may be based on these errors and negatively affect the user's online experience. Consumers may not realize that there are errors in their profile as they may not be aware of the existence of their consumer profile or they may have difficulty accessing database records in order to correct inaccurate information. Worse still, important decisions may be made about the consumer on the basis of this information by employers, insurance companies, governments and other companies. Such decisions are made without the individual's knowledge and without any opportunity for them to correct inaccurate information or expose decision-making based on prejudice or misinterpretation.

PIAC is especially concerned about consumer profiling, as it is a tool to facilitate the practice of discrimination.[21] With consumer profiling, consumers can be sorted as individuals or groups by vendors. It would be in the vendor's best interests to create a pricing scheme tailored to individual customers, offering a basket of select services to a type of client or by avoiding certain customers based on their purchase or online histories.[22] Consumer profiling could place low-income and vulnerable consumers at risk, as their profiles may lead them to be neglected, avoided or preyed upon. Facts about an individual, such as prior bankruptcy, may disqualify vulnerable consumers from economic transactions.

Such profiling shifts the balance of power in business-to-consumer relationships. With consumer profiling, any semblance of equal footing between businesses and consumers is displaced as profiling allows for segregation based on social or economic criteria. Online consumer profiling is an efficient and effective system for monitoring, making it possible for the vendor or service provider to make subtle distinctions of rank.[23]

Data mining can produce dangerous social impacts and threatens consumer privacy. Moreover, data mining practices manipulate and threaten consumer autonomy. Online behavioural targeted advertising based on data mining practices will push individuals to make certain consumer decisions by narrowing the options they receive and offering persuasive arguments at the right time to lower the resistance of the consumer.[24] When the motives of the advertisements are not obvious and the system appears to know the consumers' thoughts and desires better and earlier than they know themselves, how will

[21] It should be noted that the United Kingdom's Office of Fair Trading (OFT) has expressed a concern that consumers could suffer if their personal web usage is used to set the price they are offered for a particular service or product, especially if consumers are unaware of this practice. OFT is conducting two 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 complete its investigation into online advertising and pricing by spring 2010. See "Office of Fair Trading launches market studies into advertising and pricing practices," Office of Fair Trading (15 October 2009), online: http://www.oft.gov.uk/news/press/2009/126-09.

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

[23] Lawrence Lessig recounts how markets were previously based on hierarchical social orders, wherein information about an individual's social rank allowed systems of hierarchy to be imposed and persist as social mobility was difficult. As mobility increased and citizens could visit other markets, hierarchical systems were challenged as the fluidity of society made consumers' social rank difficult to track. Lessig argues that online consumer profiling brings us back to the past, where hierarchical social orders can now persist.

[24] Zarsky at p. 22.

the consumer be aware of where these desires came from? Legal scholar Lawrence Lessig argues that it is possible that consumer profiles will begin to normalize the population from which the norm is drawn as observation affects the observed.[25] In the broader societal context, thoughts and beliefs could be directed by pre-sorted information chosen by others in the case where there is not sufficient diversification in the media market.

Such foundational concerns with possible societal ill-effect of consumer profiling and discrimination should lead the OPCC to carefully consider the privacy implications of current and future industry practices of online targeted behavioural advertising and consumer tracking.

Conclusion

PIAC is grateful for this opportunity to comment on online tracking, profiling and targeting. PIAC would be delighted to participate in-person at the panel discussions about online tracking, profiling and targeting. We look forward to working with the Office of the Privacy Commissioner on this important consumer issue.

[25] Lawrence Lessig, "Code and Other Laws of Cyberspace" (1999) Basic Books, New York, NY at p. 154.