W3C Workshop on Web Tracking and User Privacy

Position Paper

Online Tracking, Targeting and Profiling: A Canadian Privacy Perspective

Andrew S. Patrick
IT Research Analyst
Office of the Privacy Commissioner of Canada

The paper is based on the *Draft Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing* (October 25, 2010). The full report can be found at `http://priv.gc.ca/resource/consultations/report_2010_e.cfm` and the final report will be issued in May, 2011.

In the spring of 2010, the Office of the Privacy Commissioner of Canada (OPC) held consultations on online tracking, profiling and targeting. The OPC received 21 written submissions and held two public events in Toronto and Montreal attended by representatives of industry, as well as academics, advocates, and members of the public.

The written submissions focused primarily on behavioural advertising — what it is, what the benefits and risks are, and what self-regulatory measures are in place. Many respondents and participants raised various privacy issues including the blurring of the public/private divide and its effects on reputation was seen as a significant issue. Children's activities online and the need to incorporate privacy into digital citizenship programs were also concerns that were raised.

The OPC believes that traditional notions of public and private spaces are changing. Canadians, though, continue to consider privacy to be important but they also want to engage in the online world. The two are not mutually exclusive, but we think more needs to be done to protect privacy so that individuals can trust those offering her products, services and places to be social.

It is still early days in terms of research into people's perceptions of their audience and the possible disconnect between who they think their audience is and the reality. Complicating how people communicate and interact online, as researcher danah boyd notes, is that social networks, in particular, have certain properties that alter social dynamics: persistence, searchability, exact copyability, and invisible audiences. In terms of social networking activity, some early research suggests that individuals do make distinctions with respect to their intended audience and wish to exert some measure of control. The difficulty in exerting control lies in the architecture of a site. When privacy controls are difficult to find or understand on a web site, the ability of the individual

to exert any control drops. If the site is popular and the individual is keen to be part of the community, he or she may risk being more open in order to participate in the site.

The OPC questions the view that since people put information "out there" that it therefore is available for any kind of use. Some research is showing that people intentionally project specific personas online and post information that will support these personas, usually to gain some status. It is not clear that the intention is always to be public. For example, someone may want to cultivate a professional presence online, but they may also want a separate social space to engage with friends outside of the work context. Making and keeping these worlds separate is neither obvious nor easy.

Moreover, in Canada, although personal information may appear in the public domain that does not necessarily mean it can be used for any purpose. For example, PIPEDA (Canada's private sector privacy law) provides that some publicly available personal information can be collected, used and disclosed without an individual's consent; however, the purposes for which that information may be collected, used or disclosed, are nonetheless limited.

The OPC is of the view that the consequences of the apparent breakdown between public and private lives can be seen most clearly in terms of harm to real world reputations. Individuals — teachers, politicians, police officials — have lost jobs, been publicly embarrassed, or lost benefits because of what they have posted online. Online, data persists. Information that harms an individual's reputation may never really go away. Moreover, with the increasing popularity of location-based applications, one consequence of telling people where you are is that you also tell them where you are not, potentially leaving one's home at risk.

There are also implications with respect to the accuracy of the profiles data miners construct. Much has been made about the use of social network profiles in determining employability or in determining acceptance to post-secondary education facilities. However, tracking and profiling online browsing behaviour also has consequences and is of great concern given the near invisibility of the practice. If these practices only resulted in targeted marketing, the risks of inaccuracy might seem minimal (although it could be problematic if people do not receive benefits that others do). If profiles are used more broadly, perhaps for granting loans, assessing insurance risks or assessing national security risk, the unforeseen consequences can be potentially more serious. There are also other potentially serious public policy issues that do not touch on privacy, such as limitations on freedom of speech.

The concept of "harm" appears to be used by some to distinguish certain practices that should require consent and those that should not. It should be noted, however, that PIPEDA does not contain such a concept. Rather, it requires that purposes be "appropriate", identified to the individual and consent obtained (the type of consent may vary). Instances where consent is not required are limited.

The OPC has been following developments in the area of identity management as part of its strategic priorities. Identity management may be helpful in providing individuals with better means of controlling their personal information but it also has privacy implications in that, if not done well, it may make it easier for data to be linked to previously separate identities. We are interested in the ideas surrounding "digital identity" being proposed by Kim Cameron and others. Digital identities should be flexible so that they sometimes correspond with natural, flesh-and-blood identities, and sometimes they are completely separate. Identities should allow someone to be public and private, according to the context. Identities should also allow the verification of a claim (e.g., old enough to drink) while adhering to a principle of minimal disclosure (e.g., not revealing the actual date of birth). We are tracking efforts to develop identity metasystems that allow for the effective creation and management of different identities.

The OPC supports the view that privacy considerations should be a critical component of the design stage of any technology or use of technology. In our recent submission to the Government of Canada on the Digital Economy Strategy, we noted that more could be done to prevent privacy problems or mitigate the effects on privacy protection posed by new technology by making privacy an integral part of the development of the digital economy. Other data protection authorities in other parts of Canada and the world are calling for "privacy by design" to be required in data protection legislation. The Information and Privacy Commissioner of Ontario, Ann Cavoukian, has been a long-time proponent of the concept of privacy by design.

The OPC is also of the view that privacy needs to also become an integral part of the business processes and models that rely on technology through a careful analysis of companies' activities. Privacy impact assessments (PIAs) are a useful tool that the private sector should be encouraged to use, since greater emphasis on such analysis may prevent problems from arising.

Expecting users of the web to navigate the privacy implications of the many services and business practices online, understand these implications, and consent to the practices may be unreasonable without a strong baseline of privacy protection. Knowledge and consent are key in PIPEDA but there are other principles that organizations need to consider more carefully and build into technology and business models.