Bereskin & Parr LLP

Privacy regulators weigh in on behavioural advertising

As online advertising revenue grows, conflict between advertisers and consumer privacy is also on the rise. Time for the regulators to take the lead?

Online advertising is a major industry. The Interactive Advertising Bureau of Canada reports that in 2009 Canadian online advertising revenues were C$1.82 billion, and forecasts that in 2010 revenues will rise to C$2.1 billion.

In recent years the tension between online advertising and consumer privacy has given rise to several controversies. Lawsuits have been filed against Facebook over its Beacon programme, NebuAd and internet service providers for teaming up to create user profiles, and some of the Internet's most popular websites over Quantcast's 'zombie' cookies.

Online behavioural advertising employs technologies to track users' activities over time to build profiles used to deliver targeted advertisements. The goal is to deliver relevant and effective advertising to users. Behavioural advertising can involve one website tracking users' behaviour on its own website or an advertising network tracking users' behaviour across multiple websites participating in its network. By observing users' behaviour, their interests, demographics and other characteristics are inferred to create profiles. The information collected can include websites visited, length of time spent on pages, advertisements clicked, information entered, searches performed and internet protocol addresses. Advertisers can identify categories of interest that may be broad (eg, sports enthusiast) or specific (eg, sports enthusiast from Canada who takes a ski trip at least once a year).

The main tracking technology is cookie technology. Cookies are alphanumeric text files stored on (and later retrieved from) a computer's hard drive by a single website. A cookie can identify a repeat visitor to a website and collect information. 'Third-party cookies' enable advertising networks to recognise a visitor who visits any website that is part of its network. They are broadly dispatched from multiple websites within the advertising network and users may be tracked across these websites over time. Other technologies that can be used for behavioural advertising include web beacons, web 'fingerprinting', deep packet inspection and data mining.

The use of these tracking technologies and techniques has raised 'Big Brother' concerns about advertising networks. In the past two years, regulators and industry participants in jurisdictions around the world have taken a closer look at behavioural advertising and its impact on individuals' privacy rights.

On the self-regulatory front, in July 2009 a consortium of organisations, including the Interactive Advertising Bureau, the Direct Marketing Association and the Better Business Bureau, introduced Self-Regulatory Principles for Online Behavioural Advertising.

Among the regulators, in Canada, the Office of the Privacy Commissioner launched a consultation in early 2010 on the online tracking, profiling and targeting of advertisements. In October 2010 a report of findings was issued, which concluded with a call for further submissions by early December 2010. In the United States, in July 2009 the Federal Trade Commission issued Self-Regulatory Principles for Online Behavioural Advertising. And in Europe, on June 22 2010 the Data Protection Working Party (set up under Article 29 of the EU Data Protection Directive (95/46/EC)) issued an opinion on behavioural advertising and the obligations of the various parties under existing privacy directives.

There is general recognition that behavioural advertising is necessary, and even beneficial, in that it enables website operators to continue to provide free content. However, there are concerns that current implementation does not respect the privacy rights of consumers at whom behavioural advertising is targeted.

There is consensus that the information stored by cookies is personal information that attracts the protection of the 10 privacy principles found in the Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Information, regardless of whether it immediately identifies an individual.

A principal concern is the lack of transparency. There is concern that the average internet user may be unaware that his or her behaviour is being tracked to serve targeted advertisements and may not understand the technology being used. There is consensus that transparency is vital: clear, concise, consumer-friendly and easily accessible information about behavioural advertising is necessary.

Another concern is lack of consumer consent to and control over the collection and use of their information for behavioural advertising. To give consent and exercise control, consumers must appreciate what they are consenting to and understand how to exercise control. As such, transparency is a prerequisite for meaningful, informed consent and control. All agree that providing highly visible information is a precondition to obtaining valid consent. Privacy policies and terms of use that are overly complex or legalistic are no longer sufficient. Regulators encourage the use of interactive and layered notices before cookies are dispatched. Users must be told in shorter, clearer and easily accessible ways:

- what technologies are being used to create profiles;
- the type of information that is being collected and used;
- whether tracking occurs across multiple websites; and
- that profiles will be used to deliver targeted advertising.

While there is general consensus that users should have control and choice over whether their information is used for behavioural advertising, the timing and nature of consent and the appropriate form of control are the subjects of ongoing debate.

At present, browser settings and opt-out mechanisms are among the primary ways of obtaining consent to, and giving consumers control over, the use of their information for behavioural advertising. However, these are no longer considered sufficient.

Many browsers default to accept cookies and the average internet user may be unaware of how to change browser settings to reject cookies. The EU opinion calls for browsers to have default privacy-protective settings. It states that it is a fallacy to believe that by not setting browsers to reject cookies, an individual is deemed to have provided "a clear and unambiguous indication of his/her wishes". Privacy policies and terms of use may discuss cookies only in general terms without specific reference to advertising networks. Internet users may miss the instruction or not appreciate its importance. The EU opinion deems "generic warnings" about cookies to be unsatisfactory.

Even when dealing with consumers who are fully cognisant of browser settings, browsers are capable of deleting only traditional cookies and deleted cookies may be recreated or 're-spawned' (a 'zombie' or 'flash' cookie). For example, more recently, some advertising networks have been using flash cookies to supplement or replace traditional cookies. Flash cookies cannot be deleted through typical browser settings and there have been reports of flash cookies being used to restore traditional cookies that were refused or erased. To clear all the different types of cookie, consumers must install special applications, which the Canadian paper says is an unreasonable expectation to place on consumers.

There is encouragement to move away from opt-out mechanisms, which generally require consumers to go to the website of the advertising network and indicate that they wish to opt out from being tracked for the purposes of being served targeted advertisements. Both the EU opinion and the Canadian paper suggest that such mechanisms are inadequate to obtain the average consumer's meaningful, informed consent. The EU opinion states that most consumers lack a basic understanding of how the information is collected, how the technology works and where and how to opt out. It asks advertising networks to give consumers the opportunity to opt in before information is used for behavioural advertising. The Canadian paper repeats a long-held view of the Office of the Privacy Commissioner of Canada that opt-in consent is the preferred method. It notes that the sensitivity of information is relevant to the appropriateness of opt-in versus opt-out consent. Some information (eg, financial and medical) is almost always considered to be sensitive (although any information can be sensitive, depending on the context). However, the Canadian paper acknowledges that it is easy to become lost in the issue of 'opt in and opt out', when a principal issue that needs serious consideration is that of meaningfulness. Are purposes and practices clear so that the consumer is giving meaningful consent?

Both the EU and Canadian papers support 'privacy by design'. The Canadian paper notes that the ability of individuals to exert control lies in the 'architecture' of a site: "when privacy controls are difficult to find or understand on a website, the ability to exert any control drops." The Canadian paper says that one-click access to information about behavioural advertising, with the opportunity to opt out of behavioural advertising (using a permanent cookie), could address some of the concerns, but only if it works and is broadly implemented. In the United States and Canada, there is discussion as to the feasibility of a Do Not Track Registry, which would allow consumers to opt out of being tracked online.

Generally, regulators have received one recent initiative favourably. In October 2010 a group of the largest media and marketing trade associations in the United States launched the Advertising Option Icon (i icon) programme. The programme uses a logo accompanied by notices displayed within or near online advertisements or on webpages where data is collected and used for behavioural advertising. However, the programme may not put the issue to rest. The Canadian paper says that "while we are encouraged by innovative ways to better inform individuals, and we think the i icon is a step in the right direction, opt-out consent may not sit well with many users".

The i icon programme is a concerted attempt at self-regulation. However, many still question whether the era of self-regulation is nearing an end or whether it still has relevance among regulators. The path is still unpaved, but presently it still appears to have a place. For example, in July 2010 US Representative Bobby Rush introduced the Best Practices Act bill, which proposes safe harbour for entities that participate in self-regulatory programmes approved by the Federal Trade Commission. WTR

Jennifer McKenzie
Partner
jmckenzie@bereskinparr.com

Jennifer McKenzie (BA, LLB) is a partner, barrister, solicitor and registered trademark agent with Bereskin & Parr LLP. She is head of the firm's regulatory, advertising and marketing group. She specialises in marketing, advertising, consumer protection law, privacy law and trademark prosecution and enforcement.

Catherine Lovrics
Associate
clovrics@bereskinparr.com

Catherine Lovrics (BA, LLB) is an associate, barrister, solicitor and registered trademark agent with Bereskin & Parr LLP. She is a member of the firm's trademark, copyright/new media and regulatory, advertising and marketing practice groups. She is the author of numerous articles and the recipient of the 2010 Lexology Legal Writing Award in the category for Author of the Year for E-commerce Canada.