ONLINE BEHAVIOURAL ADVERTISING: AN UPDATE FOR ADVERTISERS, AD NETWORKS AND AGENCIES

Posted on August 10, 2015

Categories: Insights, Publications

On April 7, 2015, The Office of the Privacy Commissioner of Canada ("OPC") released its findings on its investigation into Bell's Relevant Advertising Program ("RAP"),[1] an online behavioural advertising ("OBA") service, stating that Bell had violated the federal *Personal Information Protection and Electronic Documents Act ("PIPEDA")*. A few days later, on April 16, 2015, a national class action suit was filed in the Ontario Superior Court of Justice against Bell Mobility Inc. and Bell Canada Inc. claiming $750 million in damages for breach of contract, breach of the *Telecommunications Act*, intrusion upon seclusion and waiver of tort arising from the unauthorized use of customers' personal information for the RAP. A similar suit was also filed in Quebec. Taken in combination with the OPC's research report on online behavioural advertising released in June 2015[2] and recent changes to PIPEDA,[3] advertisers, ad networks and agencies should be aware of the increased legal risks associated with the purchase, sale or delivery of OBA.

What is OBA?

If you have ever browsed the Internet to research a particular topic (for instance, "Paris vacations" or "digital cameras") only to find that this topic reappears in advertisements on other websites when you return to your computer at a later time, you have likely experienced OBA. The increased appearance of tailored advertisements relating to digital cameras, flights to Paris, or whatever topic you had been researching, is not likely a coincidence.

OBA is a business model that tracks and records users' web browsing activity to build detailed profiles of user information in order to deliver targeted advertisements in an effort to enhance revenue. User profiles are developed across websites, over time, through the use of technology such as cookies. Cookies utilize small computer files containing strings of characters that are sent to a user's computer when that user visits a website. The computer files store information in the user's web browser about that user's interests and preferences, and these interests and preferences are then applied when the user accesses other sites.

OBA and Privacy Requirements

The use of OBA and the method of building detailed user profiles raises privacy law implications. In Canada, the

collection, use and disclosure of personal information is governed by PIPEDA, or equivalent privacy legislation in certain provinces.

In its OBA Guidelines published in 2011, the OPC declared that it generally considered information collected for the purpose of online behavioural advertising to be "personal information" and therefore subject to privacy legislation.[4] Pursuant to privacy laws, consent of the individual is required for the collection, use and disclosure of personal information.[5] Depending on the circumstances and the type of information collected, express consent may be required or implied consent may be permitted. Express consent is generally required for the collection of sensitive information , which is information that could lead to personal harm, financial or reputational damage, embarrassment of an individual or that could reveal deeply personal or intimate details of the lifestyle and personal choices of an individual.

In the context of OBA, the requirement to obtain express (opt-in) consent is highly contextual and is also based in part on the reasonable expectations of the online consumer. For instance, a user of a website providing free services may reasonably expect his/her email address to be collected in exchange for the free service since the collection of information for advertising is likely to be the website's sole source of revenue. In that case, the consent of the user to collect his/her personal information could be implied once the user accesses the free services. Likewise, consent may be implied if the website uses certain limited personal information for an explicit, specific purpose, made clear to the user at the time such information is collected. Organisations that collect, use and disclose personal information - whether based on the implied or express consent - must provide users with a mechanism whereby they can retract their consent (opt-out) for the collection and use of their personal information.

OBA and Class Actions: the Bell Relevant Advertising Program case

The Bell RAP fell afoul of the OBA Guidelines on a vast scale, leading to the class action launched in April of this year.

In November 2013 Bell began using customer network usage and account/demographic information, including postal code, gender, age range, credit rating and payment patterns, in order to serve Bell customers with targeted ads. Express opt-in consent was not obtained, but customers had the choice to opt-out. Although RAP advertisers did not have access to information that constitutes personal information under *PIPEDA*, the granularity of the RAP's categories permitted the selection of highly specific groups. Advertisers using Bell's RAP program could target, for example, 26-30 year old English-speaking males in the K2C 0P9 postal code with high monthly pre-paid mobile account bills for an iPhone 5C, below average credit, and an interest in hockey.

The Commissioner's subsequent inquiry determined that Bell failed to gain adequate consent from its customers for the RAP. The Commissioner found that the sheer breadth of information collected, when taken

in combination, qualified as sensitive information and required explicit opt-in consent. The findings also stated that while internet users might expect web services to track usage for the purposes of OBA in order to generate revenue to support services that are otherwise free, Bell charges for its services. As such, it was reasonable for Bell customers to expect that Bell would obtain express/opt-in consent for a secondary use of that information such as the RAP.

In its attempt to monetize the collection and use of its paying customers' personal information, Bell exposed itself to potential liability. Petitioners of the class action claim that Bell was unjustly enriched and ought to be held liable for its breaches of both contract and statute.

Risks for Advertisers, Ad Networks and Ad Agencies

1. The "Sliding Scale" of Consent

Advertisers, ad networks and agencies should also take note of the Digital Privacy Act's recent changes to *PIPEDA*, which received Royal Assent on June 18, 2015. Among other amendments, changes to *PIPEDA* include what is referred to as a "sliding scale" of consent which could render existing consents null. To validly consent, an individual to whom an organization's activities are directed must reasonably expect the nature, purpose and consequences of the collection, use or disclosure of his/her personal information. Applied to OBA, this new requirement means that if an Internet user visiting a website can reasonably expect that information pertaining to his online behaviour – such as clicking on a banner – can be collected, used to refine ad targeting pertaining to the goods advertised on such banner and disclosed by the website to the ad network who will then disclose same to the advertiser and/or the advertiser's agency, then implied consent may be valid. As soon as the OBA program goes beyond (average) user's reasonable expectations though, express consent should be obtained.

2. Risks Associated with Aggregating Data

In light of the Bell RAP Findings and the OBA Research Report, advertisers should be asking themselves whether the fragments of information they are collecting could be, in combination, considered personal information or sensitive information requiring express consent. Social media usernames alone may not lead to identifiable individuals but combining them with IP addresses may do so. Combining usernames with cookie data, interest keyword tags culled from Reddit, or Yelp check-ins may transform personal information into sensitive information requiring express consent. Ad networks and others that refine and analyze cookies, display and clickthrough data in the service of delivering OBA may leave themselves similarly exposed.

3. Advertisers may be found in breach of PIPEDA

Among those implicated in Bell's RAP case was The Source Inc. ("The Source"), which participated in the RAP

program as an advertiser. The Source was not involved in the administration or management of the RAP. Being a Bell affiliate, however, The Source was given access to the data underlying the RAP – in other words, access to personal information, including customer network usage information, interest categories and account/demographic information held by Bell. As a result, despite being merely an advertiser, The Source was implicated in Bell's breach of *PIPEDA*.[6] Advertisers should therefore be mindful of the potential risks associated with digital campaigns carried on their behalf by ad agencies using personal information collected on others' websites.

5 Key Recommendations

In light of the OBA Guidelines, the Bell RAP Findings and the OBA Research Report, the following key recommendations should be considered when engaging in the use, sale or delivery of online behavioural advertising:

1. Obtain appropriate consent (implied versus express)

As seen in the Bell RAP case, implied consent is not always appropriate for OBA, even if the pieces of information collected from an individual are each of a non-sensitive nature. Combining non-sensitive information for increased precision of ad targeting may trigger express consent requirements (opt-in) and heightened safeguard levels consistent with the collection, use and disclosure of sensitive information.

2. Provide users with unsubscribe (opt-out) mechanisms

Whether relying on express or implied consent, an unsubscribe system should allow users to opt-out of the OBA practices and retract their consent to collect, use and disclose their personal information. A common practice for opt-out models is the use of an icon placed directly on the ad (such as "Ad Choices" icons), which users can click to learn about the OBA practices of the website and opt-out.

3. Provide users with clear information regarding OBA practices

A website that relies on OBA should provide users with detailed information regarding its OBA practices. This information can be accessed by users through the use of ad icons described in Recommendation #2 above, which is generally more effective than being buried in a website's lengthy privacy policy. When the icon on the ad is clicked by the user, the website should clearly state what information is collected for OBA, how it is collected and what it is used for.

4. Ensure opt-out models are user-friendly

The OPC, in the OBA Research Report, found that although most websites it examined contained opt-out mechanisms, the opt-out procedures were inconsistent, inadequate and confusing. A user's experience when

clicking on an ad icon to gain information about OBA and to have the option to opt-out, should be consistent, clear and obvious. The opt-out mechanism should use prominent font sizes and colours to attract the attention of the user. The user should not have to scroll through lengthy text or click on multiple pages to locate the opt-out mechanism. Users who elect to opt-out should receive notice that they have successfully done so. If the user re-visits a website in which (s)he previously opted-out of OBA, the opt-out page should indicate that (s)he has already opted-out. Data collected from the user should be immediately destroyed and rendered non-usable upon opting-out.

5. Handle information with care

Once personal information is collected with appropriate consent, adequate safeguards should be in place for the use of said information. Increased protection should be implemented for sensitive information and personal information should be made anonymous so that the identity of individuals cannot be ascertained. Information that has been collected should be destroyed as soon as it is no longer required.

Conclusion

Risk assessments by advertisers, ad networks and agencies contemplating the use of OBA providers or programs should be made in the light of the Privacy Commissioner's OBA Guidelines and findings regarding Bell's RAP (and the ensuing class actions) as well as the recent changes to *PIPEDA*.

These developments signal a general trend towards increasing legal protection for personal information, one by no means limited to the Canadian context.7 For further consultation on privacy matters or to obtain a copy of our privacy checklists, please contact us at the coordinates below.

by Elisa Henry, Hilary Hennick and A. Max Jarvie, Student-at-Law

1 *PIPEDA Report of Findings #2015-01*, [Bell RAP Findings]; See our bulletin analyzing this decision: Lyndsay A. Wasser & Joanna Vatavu, "*Bell Gets a Bad Rap for its RAP (Relevant Advertising Program)*" (June 2015).

2 Office of the Privacy Commissioner "Online Behavioural Advertising – Follow Up Research Report", June 15 2015 [OBA Research Report].

3 See Digital Privacy Act, SC 2015, c 32 [Digital Privacy Act].

4 See Office of the Privacy Commissioner, "*Privacy and Online Behavioural Advertising*" (updated June 2012).

5 Sensitive information typically includes information pertaining to the medical and health condition of an individual, his/her family's life and behaviour at home, sexual orientation, religious, political and philosophical opinions, race and ethnicity, financial information, private communications and physical location.

6 The Commissioner also found in its report that, since The Source had no involvement in the RAP, Bell should cease sharing such information with The Source—thereby highlighting the narrow circumstances in which personal information may be legitimately shared for the purposes of targeted online behavioural advertising. Although not expressly stated, "involvement in" is clearly meant to indicate "involvement in the management or administration of".

7 Those doing business in the European Union, for example, will soon be obliged to comply with sweeping new EU reforms coming into force that significantly increase the ambit of legislated protections for personal data, particularly in digital form. See <https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package>.

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.