



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

[Home](#) → [Privacy topics](#) → [Technology](#) → [Online privacy, tracking, and cookies](#) → [Tracking and ads](#)

Policy position on online behavioural advertising

December 2015

Revised: August 13, 2021

Scope of the Policy Position

The following policy position addresses the application of the *Personal Information Protection and Electronic Documents Act's* (PIPEDA) to the collection and use of data about individuals' web activities by means of such technology as cookies, web beacons, supercookies, zombie cookies, device data, for the purposes of online behavioural advertising (OBA) only. OBA (online behavioural advertising) is defined as tracking and targeting of individuals' web activities, across sites and over time, in order to serve advertisements that are tailored to those individuals' inferred interests.

There are a number of purposes for online tracking, profiling and targeting individuals, and various techniques for conducting such tracking ¹ (#fn1). Some purposes include measuring web site usage to improve the functionality of the site; fraud prevention; and online behavioural advertising (OBA). In terms of tracking techniques, public discussion and attention typically centre on tracking cookies. However, "device fingerprinting" also captures data about the device an individual is using, for example, the IP address, the unique device identification number (of a cellphone, for example) or data gathered from the browser an individual uses (such as capabilities, time zone, plug-in data, and screen size). Device fingerprinting is sometimes used to detect and prevent fraud. In recent years, developers have been looking to expand its usage into the online advertising environment ² (#fn2).

This policy position with respect to OBA (online behavioural advertising) is aimed at all parties involved in online tracking, profiling and targeting, including the advertising industry, browser developers, and web site operators. It is not intended to apply to other uses of browsing information; "social media listening"; advertising in the mobile context; or the activities of a single site and its members/users. Those practices may also give rise to privacy issues, and organizations engaging in them should reflect on their obligations under PIPEDA (Personal Information Protection and Electronic Documents Act's) with respect to their practices.

While the OPC (Office of the Privacy Commissioner of Canada) does not provide advance rulings and any future complaints under PIPEDA (Personal Information Protection and Electronic Documents Act's) on the subject of behavioural advertising will therefore need to be assessed on a case-by-case basis, it is nevertheless possible and appropriate to provide general guidance

(/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/gl_ba_1112/) concerning the likely compliance and non-compliance of certain behavioural advertising practices.

The online advertising industry and behavioural advertising

During the OPC (Office of the Privacy Commissioner of Canada)'s 2010 Consultations on Online Tracking, Profiling, and Targeting, and Cloud Computing

(/en/about-the-opc/what-we-do/consultations/completed-consultations/2011/report_201105/) (Consultations), we heard from numerous industry representatives, and some companies, about the importance of advertising generally, and behavioural advertising, specifically.

Summary of industry positions provided during the Consultations

The industry stressed that online advertising helps support free online content, and helps small web site operators compete and continue to create free local and niche content. IAB Canada argues that, when consumers receive advertisements based closely on their interests, the ads function as a valued service rather than an interruption of their browsing experience.

Others in the industry noted that online advertising helps “power the Internet” and drives the digital economy, arguing that growth comes from the ability to target online advertisements to Internet users. One company suggested that Canadian advertisers can expect three significant benefits from interest-based advertising:

- Customer loyalty will increase and frustration will decrease as Canadians are exposed to less but more relevant advertising;
- Advertisers will have leaner marketing budgets, allowing them to devote more resources to product development; and
- Canadian business will be able to compete with international and online entities like eBay and Amazon for market share.

One company stated that the revenue from behavioural advertising allows companies to enhance the online experience for users and that this is especially helpful for small businesses, allowing them to access a wider range of advertisers. The company argued that this supports a diversity of voices on the Internet.

Online advertising

There are different kinds of advertising on the Internet. These include:

Random Advertisements: These are ads that are randomly placed. Since these advertisements are not based on website content or user preferences, they would typically be less economically successful to marketers.

Contextual Advertisements: Contextual advertising uses information about a user’s current visit to a site in order to serve a targeted advertisement to the user on that site. For example, if a user is visiting a website about pets, then ads related to pets might be shown.

Webpage Contextual Advertisements: In this advertising model, an advertisement is delivered based on the content of a particular webpage. For example, when an individual visiting a website about pets goes to a webpage on that site about puppies, they would see ads about dogs. If that individual then goes to a webpage on that site about kittens, they would see ads about cats.

1st Party Targeted Ads: The first party with which an individual has a relationship creates a profile about an individual, and serves them advertisements based on this profile. The user is not tracked over different unrelated websites.

Online Behavioural Advertising: In this case, an advertising service places an advertisement on a webpage based on tracking data collected across multiple unrelated websites. This practice refers to using information about where a user *has been*. For example if a user has visited websites about pets in the past, then ads related to pets might be shown on various web sites, even sites that are not related to pets (e.g., an online newspaper).

According to the Interactive Advertising Bureau of Canada's representations to our Consultation process, surveys indicate that consumers do not want to pay for content on the Internet and that they are willing to be exposed to online advertising in order to receive free online content. A Canadian Marketing Association 2009 study noted that 50% of Canadians were "somewhat uncomfortable" with marketers using browsing information to serve more relevant ads. Interestingly, according to this study, approximately 51% of Canadians delete their cookies at least once a month. ³ (#fn3)

A joint Berkeley and University of Pennsylvania study found that consumers were more persuaded by the benefits of behavioural advertising if there was more transparency, consumer choice, and data retention limits. ⁴ (#fn4)

KPMG recently issued its Consumer and Convergence Report for 2011. The report notes that 46% of Canadians were "somewhat willing" to have their online usage tracked by advertisers, particularly when tracking provided a "payoff" (i.e. free services). This number is up from 36% in 2008. The percentage of Canadians who were "not at all willing" dropped from 49% in 2008 to 38%. ⁵ (#fn5)

Independent studies on the monetary value of behavioural advertising are few, with the majority conducted by the industry. A number of industry association studies have suggested that online behavioural advertising can play a significant role in an organization's strategy, noting that it is an effective tool to generate purchase conversion and contribute to revenue generation.

Some studies have suggested that the advertising industry was expected to be worth roughly USD 411.7 billion by the end of 2011, of which USD 70.9 billion (or 17%) is associated with Internet advertising. There were no clear estimates as to the proportion of online advertising attributable to behavioural advertising, as reported percentages ranged from 18%-30%. ⁶ (#fn6)

In the *Report on the 2010 Consultations on Online Tracking, Profiling, and Targeting, and Cloud Computing* (Consultations Report), the OPC (Office of the Privacy Commissioner of Canada) considered the complexities around tracking, profiling and targeting practices for behavioural advertising purposes. We examined PIPEDA (Personal Information Protection and Electronic Documents Act's)'s application to such practices, and we considered the appropriate form of consent, given our past positions on opt-out versus opt-in consent.

The OPC (Office of the Privacy Commissioner of Canada)'s analysis of the Consultations highlighted a number of areas of concern with respect to online tracking practices, which can be summarized as follows:

- The discrepancies in characterizing what is and is not personal information. In general, most participants agreed that there were privacy implications from online tracking (even if not all agreed that the data collected from tracking was personal information).
- A lack of transparency around tracking, profiling and targeting and what this means in terms of obtaining meaningful consent – a requirement under PIPEDA (Personal Information Protection and Electronic Documents Act's). Most people don't even know that they are being tracked, and don't know the quantity or nature of the information being collected, thereby making it difficult to opt in or opt out. We saw knowledge, consent, transparency, and limiting collection as needing further attention.
- The number of parties involved in the tracking and targeting industry is not known with certainty but appears to be high. These entities are largely unknown to users, and this makes determining accountability challenging.
- The situation is especially challenging in the case of children – they are online at younger ages and unaware that they are being tracked, let alone being advertised to. Obtaining meaningful consent as required by law is a challenge.

The Consultations were intended to inform the Office on emerging technology and business practices that may have an impact on Canadians' privacy, and to inform us in advance of PIPEDA (Personal Information Protection and Electronic Documents Act's) review. The Consultations Report did not explicitly issue a position on whether or not the tracking and profiling practices were compliant with PIPEDA (Personal Information Protection and Electronic Documents Act's).

Analysis of Practices under PIPEDA (Personal Information Protection and Electronic Documents Act's)

The purpose of PIPEDA (Personal Information Protection and Electronic Documents Act's) is to “establish...rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.” In considering the question of balance, the purposes for which personal information is being collected, used, or disclosed need to be examined, as well as the types of information involved and the method for collecting and using the information.

The present policy position paper examines: 1) whether the information at issue is personal information; 2) whether OBA (online behavioural advertising) can be an appropriate purpose for collection, use and/or disclosure of personal information under PIPEDA (Personal Information Protection and Electronic Documents Act's); 3) and if so, what is the appropriate form of consent. The paper will also present some specific recommendations to bring OBA (online behavioural advertising) practices into compliance with PIPEDA (Personal Information Protection and Electronic Documents Act's).

1. Is the information at issue personal information as defined in section 2 of PIPEDA (Personal Information Protection and Electronic Documents Act's)?

Section 2 of PIPEDA (Personal Information Protection and Electronic Documents Act's) defines personal information as “information about an identifiable individual”. The Federal Court has previously held that information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information ⁷.

Much of the information at issue in OBA (online behavioural advertising) – third-party tracking cookies, IP addresses, browser settings – may not be personal information in and of itself, in that, alone, it may say nothing *about* an *identifiable* individual. However, when combined and used for the purpose of profiling a user in order to target advertisements to him or her based on inferred interests, the information can become information about an identifiable individual. A closer examination of the processes involved in OBA (online behavioural advertising) may be useful in illustrating this point.

Online behavioural tracking can involve the collection of a variety of information. In its simplest form, the tracking involves placing a third-party cookie in a user's web browser, where that cookie only contains a seemingly random serial number. More complex uses can include directly identifying information in the cookie, such as name, email address. It is useful, however, to examine the simple case of a cookie having only a serial number.

Even though the serial number itself may not identify individuals, because it follows them around as they visit various web sites, it can quickly be associated with a wide range of information, including:

- a user's IP address
- browser type, identification strings, and technical parameters
- web sites visited, and thus areas of interest
- search terms and other information entered into online forms
- transactions or purchases
- usernames and/or IDs on web services, such as social networking sites.

There have also been documented cases ⁸ where companies who engage in online tracking are explicitly passing directly identifying information, including names and email addresses, from web services to advertisers. This information can be seen in web request parameters and Referrer headers.

Information collected during web tracking can be combined with other forms of information, resulting in detailed profiles. The OBA (online behavioural advertising) industry often promotes this capability as a valuable marketing tool. We have also seen announcements ⁹ about companies planning to combine online tracking information with offline purchase information.

Therefore, in the context of OBA (online behavioural advertising), given the fact that the purpose behind collecting information is to create profiles of individuals that in turn permit the serving of targeted ads; given the powerful means available for gathering and analyzing disparate bits of data and the serious possibility of identifying affected individuals; and given the potentially highly personalized nature of the resulting advertising ¹⁰, it is reasonable

to take the view that the information at issue in behavioural advertising not only implicates privacy but also should generally be considered “identifiable” in the circumstances. While such an evaluation will need to be undertaken on a case-by-case basis, it is not unreasonable to generally consider this information to be “personal information”.

Position: Taking a broad, contextual view of the definition of personal information, the OPC (Office of the Privacy Commissioner of Canada) will generally consider information collected for the purpose of OBA (online behavioural advertising) to be personal information, *given*: the fact that the purpose behind collecting information is to create profiles of individuals that in turn permit the serving of targeted ads; the powerful means available for gathering and analyzing disparate bits of data and the serious possibility of identifying affected individuals; and the potentially highly personalized nature of the resulting advertising.

Can serving behaviourally targeted advertisements be an appropriate purpose under subsection 5(3) PIPEDA (Personal Information Protection and Electronic Documents Act's) and a condition of service?

Subsection 5(3) of PIPEDA (Personal Information Protection and Electronic Documents Act's) states that personal information may be collected, used or disclosed for purposes that a reasonable person would consider appropriate in the circumstances. Principle 4.3.3 states that an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

Content and services on the Internet are largely free in a monetary sense for all users. There are a limited number of services, primarily media outlets such as print newspapers that also operate in the online environment. These offer a subscription model, in which an individual pays a certain amount of money, and provides some personal information, in order to receive the services online. The success of this approach has been mixed and advertising is still used on these sites. ^{11 (#fn11)} Most users appear to expect information on the Internet to be free.

Web sites generally require advertising in order to make money. Advertisements that are tailored to individuals' tastes and preferences are more lucrative since more people are likely to click on them. While many people are uneasy about being tracked online, some people also indicate that they value advertisements that are targeted to their interests.

In the case in which the Office first addressed online advertising, the 2009 Facebook findings, we looked at different advertising models used by the company (as they operated at that time). In the Facebook Ads (FB Ads) model, Facebook delivered advertisements on behalf of advertisers to its users. Facebook used user profile information to do so. We found that the use of the individual's personal information could be a condition of service provided that the individual clearly understood how their information was being used. We acknowledged that some use of personal information was reasonable given that the site was free for people to use but not free for Facebook to run. ^{12 (#fn12)} Although we did not expressly refer to subsection 5(3), we implicitly accepted that the use of personal information for behavioural advertising in those circumstances could be appropriate.

FB Ads presented a somewhat different model of behavioural advertising than the one that involves third parties – typically unknown to the user – tracking individuals across the web. For one thing, it was FB doing the ad serving; our understanding at the time was that it was not disclosing personal information to advertisers except in aggregate form. Therefore, the number of parties involved was limited, and there was a direct relationship between the user and the company delivering the advertising.

Position: Given that some users may be uncomfortable with the notion of being “followed” around the web, yet think that advertisements geared to their interests are useful and, given that services are generally free and users ought to expect that some personal information may be needed to access services and information, OBA (online behavioural advertising) may be considered an appropriate purpose for the collection, use and/or disclosure of personal information from the perspective of the reasonable person. However, OBA (online behavioural advertising) should not be considered a term or condition for individuals to use the Internet generally. There are still other forms of advertising that web sites can rely on. There must also be meaningful consent, and there should be limitations on the types of information collected and used for profiling. Safeguarding the information is also vital, as is limiting the retention of the data to the least amount of time possible.

Meaningful consent: opt-in or opt-out ?

The Consultations Report also considered opt-out (implied) consent to OBA (online behavioural advertising) within the context of the policy guidelines we have previously outlined for reliance on implied consent. These guidelines state:

- The personal information must be demonstrably non-sensitive in nature and context.
- The information-sharing situation must be limited and well-defined as to the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure.
- The organization's purposes must be limited and well-defined, and stated in a clear and understandable manner.
- As a general rule, organizations should obtain consent for the use or disclosure at the time of collection.
- The organization must establish a convenient procedure for opting out of, or withdrawing consent to, secondary purposes. The opt-out should take effect immediately and prior to any use or disclosure of personal information for the proposed new purposes. ¹³ (#fn13)

It is important to keep in mind that those guidelines were developed in a different context, involving more traditional business models and marketing techniques, in which individuals provide personal information in exchange for a product or service and their personal information is sold to third parties for "secondary marketing purposes". While marketing is hardly secondary to the business of the Internet, the guidelines nevertheless continue to provide a useful framework, even in the online environment. However, as the Consultations Report noted, two criteria pose a challenge: obtaining consent at the time of collection and determining the sensitivity of the information. Nevertheless, these are important criteria, and certain actions can be taken by organizations to address those criteria.

With that in mind, we have adapted this framework for opt-out consent and OBA (online behavioural advertising), recognizing that OBA (online behavioural advertising) may be considered acceptable provided certain conditions are met. Businesses with an online presence need to generate revenue and behavioural advertisements appear to be more lucrative than contextual advertisements. Other business models are less popular in the online environment where individuals expect information and services for free (those models nevertheless still rely on some personal information being provided to an organization as well). Individuals also expect instant access. Constant notifications to users about cookies and blocked access to ad-supported sites will frustrate users and potentially create fatigue or a backlash against efforts to protect their personal information.

Position: Opt-out consent may be acceptable provided certain conditions are met. The following are such conditions, along with two proposed restrictions.

Conditions and Restrictions: A Framework for Opt-Out

The conditions under which opt-out consent to OBA (online behavioural advertising) can be considered acceptable are:

- Individuals are made aware of the purposes for the practice in a manner that is clear and understandable – the purposes must be made obvious and cannot be buried in a privacy policy. Organizations should be transparent about their practices and consider how to effectively inform individuals of their OBA (online behavioural advertising) practices, by using a variety of communication methods, such as online banners, layered approaches, and interactive tools;
- Individuals are informed of these purposes at or before the time of collection and provided with information about the various parties involved in OBA (online behavioural advertising);
- Individuals are able to easily opt-out of the practice - ideally at or before the time the information is collected;
- The opt-out takes effect immediately and is persistent;
- The information collected and used is limited, to the extent practicable, to non-sensitive information (avoiding information that is generally considered sensitive such as medical or health information, financial data, ethnic and racial origins, political opinions, genetic and biometric data, an individual's sex life or sexual orientation, and religious/philosophical beliefs); and
- Information collected and used is destroyed as soon as possible or effectively de-identified ¹⁴ (#fn14).

Restrictions to OBA (online behavioural advertising)

1. Zombie cookies, supercookies, third-party cookies that appear to be first-party cookies, device fingerprinting, and other techniques that cannot be controlled by individuals

There are certain types of tracking that are used in OBA (online behavioural advertising) that an individual cannot stop or control without taking extraordinary measures (and some cannot be stopped or controlled at all). These include so-called zombie cookies, super cookies, and device fingerprinting. In other cases, some parties engaged in OBA (online behavioural advertising) are using third-party cookies that have been disguised as first-party cookies. If an individual tries to clear first-party cookies (to get rid of these third-party cookies), he or she risks rendering certain web sites that rely on the operation of 'actual' first-party cookies unusable. Given that individuals cannot effectively opt out of these techniques, it is our view that such techniques should not be allowed at this time. While it is possible that a technological solution to this lack of user control could emerge, for the moment, where a tracking technique offers no option for user control, and therefore no ability to consent or withdraw consent, and the technique is used to collect personal information for OBA (online behavioural advertising) purposes, the OPC (Office of the Privacy Commissioner of Canada)'s position is that such tracking should not be undertaken because it cannot be done in compliance with PIPEDA (Personal Information Protection and Electronic Documents Act's).

2. Children's personal information

The most obvious type of information that should not be tracked involves children's information. Operators of web sites that are targeted at children should not permit the placement of any kind of tracking technologies on the site. It is hard to argue that young children could meaningfully consent to such practices, and the profiling of youngsters to serve them online behaviourally targeted ads seems inappropriate in such circumstances. The Canadian advertising industry has indicated that it will require its members to not knowingly target children; this is a position that the OPC (Office of the Privacy Commissioner of Canada) endorses and encourages.

The key issue here is the great difficulty organizations are likely to encounter in obtaining meaningful consent to OBA (online behavioural advertising) from very young users of the Internet.

We see children going online at younger and younger ages. Many adults don't understand what's happening behind their computer screens – we certainly can't expect children to fully appreciate how their personal information is being collected and used. The advertising industry itself has also expressed concerns about this issue.

In terms of what age would be appropriate for implied consent to OBA (online behavioural advertising), PIPEDA (Personal Information Protection and Electronic Documents Act's) does not refer to specific age thresholds for providing consent, but rather to the concept of meaningful consent. What is meaningful for a 17 year-old may not be the same as what is meaningful for a nine-year-old. Practices need to correspond to cognitive and emotional development. What is appropriate will also depend on the specific context.

Given the practical obstacles to obtaining meaningful consent from children, especially implied consent, organizations should avoid knowingly tracking children and tracking on websites aimed at children.

Summary

This policy position paper deals only with online tracking and targeting for OBA (online behavioural advertising) purposes. For the purposes of this paper, OBA (online behavioural advertising) means tracking and targeting of individuals' web activities, across sites and over time, in order to serve advertisements that are tailored to those individuals' inferred interests.

Consistent with a broad and contextual interpretation of the definition of "personal information" under PIPEDA (Personal Information Protection and Electronic Documents Act's), data collected and used for OBA (online behavioural advertising) purposes will often constitute "personal information".

Advertising plays a key role in providing free content on the Internet. There are different types of advertising available; OBA (online behavioural advertising) is but one type of online advertising. However, given the way in which it is done, it carries heightened implications for privacy. OBA (online behavioural advertising) may be considered a

“reasonable purpose” under subsection 5(3) of PIPEDA (Personal Information Protection and Electronic Documents Act’s), though not a condition of service for accessing and using the Internet generally.

Meaningful consent is required for OBA (online behavioural advertising). ^{15 (#fn15)} Implied or opt-out consent for tracking and targeting individuals for behavioural advertising purposes may be acceptable provided that the following parameters are in place:

- Individuals are made aware of the purposes for the practice in a manner that is clear and understandable – the purposes must be made obvious and cannot be buried in a privacy policy. Organizations should be transparent about their practices and consider how to effectively inform individuals of their OBA (online behavioural advertising) practices, by using a variety of communication methods, such as online banners, layered approaches, and interactive tools;
- Individuals are informed of these purposes at or before the time of collection and provided with information about the various parties involved in OBA (online behavioural advertising);
- Individuals are able to easily opt-out of the practice - ideally at or before the time the information is collected;
- The opt-out takes effect immediately and is persistent;
- The information collected and used is limited, to the extent practicable, to non-sensitive information (avoiding information that is generally considered sensitive such as medical or health information, financial data, ethnic and racial origins, political opinions, genetic and biometric data, an individual’s sex life or sexual orientation, and religious/philosophical beliefs); and
- Information collected and used is destroyed as soon as possible or effectively de-identified.

Some forms of tracking can be blocked or prevented while other methods cannot. If users cannot block or otherwise prevent a given method from being used for OBA (online behavioural advertising), the industry should not engage its use for OBA (online behavioural advertising) purposes at this time.

Likewise, given the great difficulty organizations are likely to experience in obtaining meaningful consent from children to OBA (online behavioural advertising), the industry should avoid knowingly tracking children and tracking on websites aimed at children.

The Office’s guidance with respect to OBA (online behavioural advertising) is aimed at all parties involved in online tracking, profiling and targeting, including the advertising industry, browser developers, and web site operators.

Footnote 1

-
- 1 “Social media listening” is another type of “tracking”. It uses information that individuals post on social networking sites, forums, comment boards, and which can be profiled for a variety of purposes. There have been reports about the use of data profiling of social network sites to determine credit worthiness, for example. Some of these techniques are used to research what people are interested in or are buying. Tracking involves the use of datamining tools applied to information that individuals offer up on web sites. There are many privacy issues associated with such activities. This activity is outside the scope of this paper.
 - 2 Some consider it the “next wave” of tracking, given that people often block or delete tracking cookies. Race Is On to 'Fingerprint' Phones, PCs
 - 3 <http://www.the-cma.org/downloads/regulatory/SubmissionAdvertisingMar10.pdf> and http://www.the-cma.org/PublicUploads/224933BehaviouralAdvertising_09.pdf
 - 4 Turow, Hoofnagle, et al, “Americans Reject Behavioral Advertising and Three Activities To Enable It” pg 25 – 26.
 - 5 See “The Converged Lifestyle: KPMG’s Consumer and Convergence Report 2011”, KPMG International

- 6 The Network Advertising Initiative, "[Study Finds Behaviorally-Targeted Ads More than Twice as Valuable, Twice as Effective As Non-Targeted Ads](#)". March 24, 2010. Lee, Edmund "[Quantcast Teams With Ad Industry to Offer Free Privacy Icon](#)" *Ad Age Digital*, July 25, 2011.
- 7 *Gordon v. Canada (Minister of Health)*, 2008 FC 258
- 8 Krishnamurthy, B., Naryshkin, K. and Wills, C.E. "[Privacy leakage vs. Protection measures: the growing disconnect](#)" Web 2.0 Security & Privacy Conference, May 2011, Oakland, CA.
- 9 Steel, E. "[Using credit cards to target web ads.](#)" Wall Street Journal Online. October 25, 2011.
- 10 The tracking information is used to alter the user's experience as he or she uses the web. Even if users are collected into groups for the purposes of targeting, membership in the group is based on information about individual behaviours.
- 11 [The New York Times' digital paywall is unlikely to collect enough revenue to offset a long-running decline in the newspaper's print advertising, according to an analysis sent to investors Wednesday. Times loses almost 90% of online readership.](#)
- 12 Subsequent to our finding, the US Federal Trade Commission found that Facebook members' user IDs were being shared with advertisers, contrary to what users were told. The issue was addressed by Facebook in May 2010.
- 13 Determining the appropriate form of consent under the *Personal Information Protection and Electronic Documents Act*
- 14 Given that anonymization can be challenging to achieve, deletion of any data collected (after it is used) is preferred.
- 15 Following the development of this policy position [PIPEDA \(Personal Information Protection and Electronic Documents Act's\)](#) has been amended to include section 6.1 which states that for the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

Related content

[Online Behavioural Advertising in Brief](#)

(/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/02_05_d_52_ba_02/)

[Frequently Asked Questions about Online Behavioural Advertising](#)

(/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/02_05_d_52_ba_01/)

[Guidelines on Privacy and Online Behavioural Advertising](#)

(/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/gl_ba_1112/)

Date modified:

2021-08-13