June 2013

mcmillan Privacy Bulletin

CASL Update #3 – Computer Download Rules – Potential Impact For Online Advertisers

CASL Status

In response to Industry Canada's release of its draft regulations for *Canada's Anti-Spam Law* (CASL) in January of this year, some 135 responses were received. Industry Canada has indicated that it is considering the diverse comments contained in these responses with the goal of issuing final regulations sometime in the fall. If this timing holds, the betting is that CASL will come into force in the fall of 2014.

The final regulations will contain certain definitional clarifications and potentially some further (or expanded) exemptions or exceptions to CASL. The extent that these further adjustments go toward facilitating organizations' compliance with the law remains to be seen.

The Computer Download Rules

In addition to CASL's rules governing commercial electronic messages (CEMs), the legislation includes significant requirements relating to licensing and downloading of computer software. The intended focus of these download rules is to prevent unauthorized access, control or data collection into or from a user's computer (such as may occur with malware and viruses). However, parallel to the experience with the anti-spam CEM rules, they will have a scope beyond this specific focus and will apply to downloading of all software and programs.

In addition, the CASL rules may have a significant impact on user tracking as currently conducted by diverse online parties for purposes of serving targeted ads. Regulation of targeted advertising (also referred to as "online behavioural advertising" or "interest-based advertising") is currently a significant focus for privacy regulators and industry stakeholders alike.

The thrust of the computer download rules is to require express user consent for such downloads plus disclosure of the purposes applicable to the consent, contact information of the person seeking consent and a general description of the function and purpose of the program. Where the program collects personal information, or changes or interferes with the user's control or use of, or access to, their computer or causes it to communicate with another computer or activate a program without the knowledge of the user, a more detailed description is required. However, the consent, contact information and program description requirements do not apply to updates or upgrades of programs in respect of programs installed with a prior consent that contemplated such updates or upgrades. Furthermore, for certain specified programs including cookies, downloaded HTML code and Java Script, and installed operating systems, express consent is deemed to have been given provided it is reasonable to conclude that the user has consented to their installation.

Online Behavioural Advertising (OBA) And Tracking

Online tracking of user online activities is a powerful but controversial tool that enables advertisers and others to build data files about consumers that may be used for diverse purposes, in particular serving targeted advertising. This data collection is performed through several technologies. In most cases it involves the downloading or installation of a cookie or data file onto the user's computer system.

These technologies enable the collection of user data, including websites and pages viewed, products purchased, searches and other activities and also may provide device-specific data ("fingerprint data") and location information. While in most instances this data is only associated with the user's computer

system internet address, some data collected may be directly personally identifiable (such as product or service purchase data providing user identity).

Privacy regulators in Canada, the United States and Europe view online tracking as collection and use of personal information, whether or not an individual is identified specifically and have stated that such collection must comply with applicable privacy laws. They disagree with the argument that data only associated with an internet address is not "personally identifiable", and in any event take the view that, once collected from diverse sources and aggregated with other parallel data, such data becomes personal information.

While industry stakeholders have argued that some or all of the data collected in this manner is not "personally identifiable", they acknowledge that user choice must be provided. However there is disagreement as to whether this choice should extend to tracking or only apply to the targeting part of the equation.

Regulators in Canada and the United States have spelled out clearly their expectations regarding the collection of tracking data: users must be advised of the data collection and provided with an opportunity to decline to have their data collected or if collected, to be used for specified purposes. The functionality to decline collection is referred to as "Do Not Track". Secondarily, regulators have indicated also the need to have a capability for users to be able to decline consent to be targeted by advertising that is based on tracking data (referred to as "Do Not Target"). To date, North American regulators have issued guidelines indicating their compliance expectations but they have not undertaken any specific enforcement actions and have been looking to the internet advertising industry to provide user-friendly techniques that address the privacy requirements on a voluntary basis.

In contrast to the U.S., enforcement of such expectations in Canada could be effected under our private sector privacy laws – the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and its provincial counterparts. In the U.S., which has no generally applicable privacy law, Congress has been urged to adopt

a "Do Not Track" law if industry efforts are not considered adequate. By contrast, the European Union has enacted a "Cookie Directive" which specifically addresses tracking and makes clear that consent to track is required. Multi-national businesses have been required to respond to this Directive.

Both the federal Privacy Commissioner and the U.S. Federal Trade Commission have indicated general support for an industry initiative ("*AdChoices*") developed in the U.S. by the Digital Advertising Alliance which is set to roll out in Canada through the collective efforts of several industry self-regulatory associations. The technique involves an icon placed on web pages intended to notify a user that he or she may be targeted and to provide an ability to register an "opt-out" from such targeting.[1] If the opt-out is selected, all industry stakeholders who have agreed to participate (including search engines, websites, data aggregators and advertisers) will honour it with the result that the user should not receive ads generated or delivered by any of those organizations. In addition, the organizations agree not to collect any such data for targeting purposes.

The concern with the *AdChoices* initiative is that, to date, it does not address all tracking. While it provides an opt-out from targeting and appears to require websites and advertisers to decline to collect data for such purpose, it does not provide a functionality for opting out or declining consent to tracking generally.

By contrast, and controversially within the adverting industry, Microsoft and Mozilla have introduced what is considered an "opt-in" functionality to their latest browsers, which, as a default, directs internet parties to stop all tracking. In the face of this controversy, the U.S. Senate is debating a Do Not Track standard and a committee of the World Wide Web Consortium (W3C), which

[1] The Privacy Commissioner has indicated some concerns with respect to the initiative that she believes need to be addressed. In particular, consumers must understand the purpose of the *AdChoices* icon. This requirement would address the "knowledgeable consent" aspect of its use in connection with OBA. See the Commissioner's speech at the *Marketing and the Law Conference*, Dec. 6, 2011.

sets internet functionality standards, is seeking to achieve that objective with a view to heading off possible legislative action.

Impact Of CASL

As noted, data collection for online tracking is performed by the use of cookies as well as other technologies most of which involve the installation of a data file or software onto a user's computer. This action may fall within CASL's download rules and therefore be subject to the statute's disclosure and consent requirements.[2]

Notwithstanding the intense regulator, industry, and possible legislative attention that has been focussed on OBA, little or no notice has been registered with respect to the potential application of CASL on the tracking side of the equation. However, CASL as currently enacted may have a significant impact on and, in Canada at least, potentially drive the adoption of an industry-wide standard for either opting in or opting out of tracking. As noted, CASL's download rules require certain disclosures as well as user consent.[3]

Furthermore, these rules apply whether or not "personal information" is being collected and therefore avoid the debate as to whether data related only to an internet address is regulated by the privacy laws. However if "personal information" *is* being collected (e.g. specifically identifying data such as in a purchase order), more comprehensive disclosure is required.

---

[2] Web-tracking tools may or may not be computer programs within the relevant CASL definition (s. 342.1(2) of the *Criminal Code*: "computer program" means data representing instructions or statements, that when executed in a computer system, causes the computer system to perform a function). However s. 10(8) of CASL, the deemed consent rule, appears to include cookies and HTML code specifically as computer programs.

[3] For programs that collect personal information or affect control of a user's computer, more detailed information must be provided, and clearly and prominently brought to a user's attention. For certain downloads including cookies, express consent is assumed, provided that the user's conduct is such that it is reasonable to believe he or she has consented to the installation. This latter rule, which may be considered a form of implied consent, clearly requires that an *informed consent* exist. What is not clear is whether to achieve this level of consent, the information disclosure stipulated by the CASL requirements for seeking express consent also must be met.

As noted above, "Do Not Track" has not yet been embraced by the industry self-regulatory initiatives and as yet has not been acted on by privacy regulators or, in the U.S., by Congress. While it appears that this day is coming in the not-too-distant future,[4] much of the current debate revolves around whether any Do Not Track functionality should be opt-in or opt-out. Put differently, the issue is whether Do Not Track is the default setting (e.g. on a browser) which a user must deactivate if they wish to have their data collected (i.e. tracked) or whether they need to "opt-out" of collection by taking some positive step.

CASL may have a significant impact on this debate in Canada, since it requires "consent" in some form, and possibly expressly, for any tracking technology that is considered to involve the installation of a computer program on a person's computer system. Assuming CASL's application, clear disclosure of the proposed data collection/tracking and its general nature and purpose must be made in order for the consent to be valid. Interestingly, while regulatory attention on the OBA/tracking issue has been focussed to date within the federal Privacy Commissioner's office, the CRTC, which has enforcement and guidance jurisdiction with respect to CASL, now may have a role to play as well.

by David Young and Robert Hester

For more information on this topic please contact:

Toronto	David Young	416.307.4118	david.young@mcmillan.ca
Toronto	Robert Hester	416.865.7803	robert.hester@mcmillan.ca

a cautionary note

[4] See draft reports of the W3C's *Tracking Protection Working Group*.