David Young Law
Compliance Bulletin

November 2014

CASL's Computer Download Rules – Coming to an App Store Near You

David Young

November 2014

On January 15, 2015 the second chapter in Canada's anti-spam legislation ("CASL") saga opens with the coming into force of the law's computer download rules. The download rules while intended to strike at bad actors only, in fact have broader application - to *all* digital system providers, including, very importantly, app developers and app stores. Subject to certain exceptions, they also apply to any computer system or program provider who delivers software (both the base program and all updates) to a user, electronically (i.e. online).

The full scope of CASL comes into force in a multi-stage process. Its first main thrust, the commercial electronic "messaging" (or CEM) rules, came into force with a delay for certain provisions on July 1, 2014. However CASL is more than just an "anti-spam" statute – it has significant application to unconsented-to disruptive, invasive or otherwise unintended computer communications, including alteration of transmissions and installation of "malware" and "spyware". The download rules are intended to address these activities.

As with CASL's messaging rules, the download rules contain provisions that will require clarification and further interpretation. To assist organizations seeking to achieve compliance by the January 15 in-force date, the CRTC has been holding meetings with representative affected stakeholders and on November 10, 2014 published a guidance document entitled "CASL Requirements for Installing Computer Programs".

Providers/suppliers of computer systems including app stores, developers, and other providers of software including providers of software embedded in products such as automobiles and appliances urgently need to address these new rules and determine what procedures or protocols may be required to continue to market their products post-January 15, 2015.

The Basic Requirements

The computer download rules have two basic requirements - consent and disclosure. Where they apply, a provider is required to obtain consent to a download, unless consent is implied or deemed, and to make disclosure of the nature of the software and how it will impact a user's computer.

The consent required is *express consent* which, as with the messaging rules, is not defined under CASL but is understood to mean a positive, "opt-in" consent. In addition, when consent is requested, the

David Young Law • Hudson's Bay Centre, Suite 3500, 2 Bloor Street East, Toronto, ON M4W 1A8
T. 416-968-6286 • M. 416-318-5521
Privacy and Regulatory Law Counsel • davidyounglaw.ca

request must include disclosure according to CASL's standard consent request protocol as well as information specifically stipulated under the download rules.

Two, limited, categories of implied or deemed consent are exceptions to this rule. For previously-installed programs, consent to all updates/upgrades between January 15, 2015 and January 14, 2018 is implied. A second category of program downloads benefit from a deemed consent where it is reasonable to conclude that the user consents to their installation (notwithstanding no specific express consent).

The provider must disclose the function and purpose of the software and, for downloads that perform certain functions contrary to a user's reasonable expectations, more detailed information including a description of the program's "material elements" and its foreseeable impact on the user's system.

Application

The download rules apply to anyone whether or not in Canada who "installs" or "causes to be installed" a "computer program" on another person's "computer system" located in Canada in the course of a commercial activity. They also apply to persons within Canada who perform such downloads onto computer systems anywhere in the world.

Under CASL, "commercial purpose" includes any transaction involving a purchase, sale, or barter of something, whether or not is it expected to produce a profit. As with the messaging rules, the download rules apply to both businesses and not-for-profit organizations. Furthermore, they apply to both purchased and free downloads.

Key Technical Terms

Definitions for CASL's key technical terms – computer program and computer system – are the *Criminal Code* definitions. Those definitions are very broadly written.

A *computer system* is a device or network of devices that contains computer programs or other data by which it performs logic, control and other possible functions. Clearly then, a computer system includes not only traditional desktop computers and laptops, but also most if not all tablets and mobile devices.

A *computer program* is defined as data representing instructions or statements which, when executed in a computer system, causes it to perform a function. A computer program therefore includes any recognized form of software that causes a system to perform functions as well as any updates to that software – including, significantly, apps on mobile devices and updates to those apps.

The terms "install" and "cause to be installed" are not defined by CASL but relevant dictionary meanings would apply (e.g. "make a machine or service ready to be used" – *Merriam Webster Online* and more

specifically for digital applications, "load software into a computer" – *Oxford Dictionaries Online*). However for the purposes of CASL, the CRTC has indicated that somewhat narrowed definitions for these terms are applicable.

Most significantly, the CRTC has indicated that self-installed software is not included within CASL's application. So, if the device user purchases an app from an app store, which then downloads the app onto the device at the owner's request, the transaction will not be considered an installation by the app store. Similarly, updates to the app, if installed by an action of the owner, will not be subject to CASL. However if an initial app installation results in an update being installed in the background without any request by or notice to the user, or automatic updates are downloaded subsequent to the initial installation without any positive action by the user, the installation or download would be considered *installed by the software provider* and subject to the download rules.

The CRTC also has indicated that the phrase "cause to be installed" is to be given a narrower meaning – essentially interpreted to mean software that is installed *covertly* along with other software that a user has installed. This could be malware or merely a supplement to software ancillary to installation of a primary software program. The common element is a secondary installation that results from the installation of a primary software item *without knowledge of the user*. The CRTC is giving consideration to providing additional guidance as to when a computer program or function is the secondary as opposed to the primary function within a system and when installation is covert or undisclosed.

The CRTC has indicated in its stakeholder meetings that "firmware" or software that is installed by a manufacturer of a product prior to sale will be considered self-installed by the manufacturer and that on sale to a customer, the benefit of self-installation and any consents for updates and upgrades transfer to the buyer.

Consent

As with CASL's messaging rules, a key requirement of the download rules is user consent – specifically consent of the "owner" or an "authorized user" of the computer system. The CRTC has indicated that an owner or authorized user includes anyone who has permission to use the device or the computer system. This would extend to employees of a system owner, children, spouses and other relatives of the owner or an authorized user, persons leasing a system or device and maintenance/repair service providers.

As noted above, "express consent" is not defined in CASL. However, *requests for consent* must conform to the same protocol stipulated for requests for consent under the messaging rules. Consent must be given by an active, positive, act, which can be oral or written; best practice is to obtain consent in a written form (which may include digitally).

The protocol for requests stipulates that the following items be stated:

- the purpose of seeking consent
- the name and any carrying on business name of the requestor and any person on whose behalf the request is made;
- the street address and at least one of a telephone number, email address or website address for the requestor or the person for whom the request is made; and
- a statement that consent may be withdrawn (best practice is to include a link for unsubscribes).

As well as the consent request protocol requirements, disclosure must be made of certain additional information regarding the nature and impact of the program proposed to be downloaded (see below – Disclosure of Computer Download Information).

It should be noted that express consent obtained prior to the coming into force of the download rules does not need to comply with the request protocol or disclosure requirements. However it is recommended that any current requests for consent made prior to the in-force date should comply with the rules.

Implied and Deemed Consents

The download rules provide for two circumstances when actual express consent is not required.

Consent is *implied* for any updates or upgrades to existing software downloaded prior to January 15, 2015, for a transitional period of three years. Following this transitional period, consent will be required for all updates/upgrades within CASL's application unless exempted by its deemed consent rules.

Express consent is *deemed* to have been given for downloads of specified types of software provided that it is reasonable to conclude that the user's conduct is consistent with such consent. This qualifying criterion makes this deemed consent in effect a form of implied consent.

The types of programs for which such deemed consent applies are the following:

- cookies
- HTML code
- JavaScript
- operating systems

- programs executable only through another program for which consent has already been given
- programs installed by a telecommunications service provider for the purposes of protecting its network from security threats, or upgrading its network
- programs installed for purposes of correcting a defect or failure in a computer or previously-installed software.

The CRTC has provided guidance as to the meaning of certain terms used in this deemed consent provision:

- a "cookie" is a non-executable computer program that cannot carry a virus or install malware;
- an 'operating system" is a computer program that has special access to the hardware of a system and acts as a platform to allow other programs to use the hardware; examples are Microsoft Windows, Mac OS/IOS, Linux, and Android and Blackberry operating systems, as well as embedded systems such as found in automobiles and appliances;
- a "telecommunications service provider" ("TSP") is an organization that provides telecommunications services without any requirement that it own or control the equipment or software on which the services are provided; in this regard, the CRTC indicates that automobile manufacturers would be TSPs if their vehicles contain wireless functionalities;
- "correcting a failure" includes taking steps to ensure the safe and proper functioning of computer programs and systems which would include fixing security vulnerabilities and software errors, including "bug fixes".

Disclosure of Computer Download Information

The second key requirement of the download rules is that, in addition to the basic consent request protocol, a person proposing to download software must also disclose certain information regarding the program to be installed and, for a specific category of programs, more detailed information regarding its functions.

For all downloads, when seeking consent the provider must clearly and simply describe in general terms the function and purpose of the program to be installed. However, for programs that perform certain defined functions that the provider knows will cause the user's system to operate in a manner not reasonably expected by the user, the provider must also clearly, prominently and separately from any other information provided, describe the material functional elements of the program including their purpose and their reasonably foreseeable impact on the system's operation. Furthermore, the provider must obtain the user's acknowledgement in writing (which may be digital) of the program's specified functions.

Downloads that are subject to these more rigorous disclosure requirements are those that:

i) collect personal information stored on the computer system;
ii) interfere with the user's control of the system;
iii) change or interfere with the system settings or commands without the user's knowledge;
iv) change or interfere with data stored on the system in a manner that interferes with the user's lawful access to that data;
v) cause the computer system to communicate with another system or device without the user's authorization; or
vi) install a program that may be activated by a third party without the user's knowledge.

An ancillary rule is that a provider is required, for a period of one year following the installation, to assist a user to remove or disable software that performs one of these functions if the description of the function, purpose or impact of the software given to the user was inaccurate.

These more rigorous disclosure requirements clearly impose a higher and more explicit level of information to be provided to users. While they clearly apply to, and are intended to prevent, surreptitious download of malware and other unwanted software, they also would apply to any legitimate download that fits the criterion of "not reasonably expected" by the user. This potential impact is consistent with the broad application of the download rules.

An example could be *automatic updates* to a gaming app that contain a functionality to collect location or video data. While the initial download of a "user-installed" app would not require consent, automatic updates may be subject to the more extensive disclosure rules. Another example of where the rules may apply would be an app, or an update, that results in the system or device sending data to another computer without the user's consent. Again, this requirement responds to concerns with unauthorized information extraction caused by malware or spyware; however it also could apply to legitimate app functions that result in data (such as location data) being extracted from the system or device without the user's acknowledgement.

For software downloaded in connection with a user-installed app, a key consideration in avoiding the more onerous disclosure requirements is sufficient disclosure at the time of initial installation. This disclosure should be directed to ensuring that the software is considered user-installed and not treated as a covert installation by the provider. Furthermore, disclosure should be sufficient to negate any argument that the app's functionality was "not reasonably expected" by the user.

Compliance Checklist

CASL's download rules will have significant impact for software vendors, app developers and vendors of the increasing number of offline products incorporating embedded software connected to wireless networks. To ensure compliance with the rules, the following key items should be addressed:

1. Review and confirm status of existing consents for in-place software and for future updates/upgrades.
2. Review procedures and characteristics of all software installations to determine installation status (provider vs. user) and therefore applicability of the download rules.
3. Confirm procedures and disclosures made in connection with user-installed software to ensure that user is aware of the existence and functions of any ancillary software.
4. Identify programs that qualify for deemed consent and review disclosures to ensure that the user's reasonable expectation is consistent with consent.
5. Review potential applicability of the enhanced disclosure rules – the characteristics and functions of all software and whether or not they are within the user's reasonable expectations.
6. Develop and put in place consent protocols including disclosure compliance where consents are required for future downloads/updates/upgrades.

For more information please contact:

David Young 416-968-6286 david@davidyounglaw.ca

Note: The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.