CRTC clarifies that anti-spam law won't apply to self-installation of computer programs - most of the time

November 18, 2014

David Elder

CRTC staff has issued **important guidance on its interpretation of section 8** of **Canada's Anti-Spam Legislation** (CASL), noting that the law would not apply to most installations initiated by users, including the downloading of mobile apps from popular digital distribution platforms like The App Store, Google Play and BlackBerry World.

While much attention has been paid to **the core anti-spam provisions of CASL**, which came into force on July 1, less attention has been paid to date with respect to section 8, which governs the installation of computer programs in the course of commercial activity. However, as the January 1, 2015 coming into force date nears for that provision, many businesses have been struggling to understand their legal obligations and take the necessary steps to comply.

Section 8 of CASL generally provides that a person must not install or cause to be installed a computer program on another person's computer system without prior express consent. Both the terms "computer program" and "computer system" are very broadly defined, and would include a wide range of programs and devices.

Given that it has become commonplace for businesses to develop and distribute mobile apps as promotional tools, often free of charge, the computer installation provisions of CASL have been attracting attention from companies well beyond the software industry.

Accordingly, it will be welcome news to many that the CRTC has indicated that in most cases, self-installed software is not subject to the requirements of CASL, including software installed from a disc or downloaded from a website or mobile app store. However, business should be aware that even in self-install scenarios, they may still have obligations under the anti-spam law.

In this regard, application developers and distributors may still be subject to CASL as having "caused to be installed" programs on another person's system. The Commission's guidance indicates that it will view businesses as having caused programs to be installed where the installation includes unexpected programs or functionality. Where a person causes a program to be installed on another's system, prior express consent must be obtained, in the required form, and certain disclosures must be made, depending on the nature of the programs/features. In some cases, businesses causing a program to be installed must also ensure that the installing party is provided with an electronic address at which they can request to remove or disable the program, and in must also provide no-cost assistance to the installing party to remove or disable the program.

While these provisions appear to be targeted at spyware and malware, they will have broader application to more legitimate programs and functions. Unexpected programs could include “tag-along” installations of programs such as browsers, toolbars and anti-virus software that are tied to the installation of a primary program. Unexpected functionality could include the collection or personal information from a device (even if only to identify the user), the modification of user settings or causing the program to communicate with another computer system, such as where programs report system errors and crashes to the software developer.

The CRTC has indicated that the reasonable expectations of users will be the key to a determination of what programs and features might be “unexpected”, based on a review of all relevant circumstances, including the nature of the program being installed and the nature and extent of the disclosures made by the relevant developer or distributor.

Businesses could also continue to face CASL obligations respecting automatic updates or upgrades to self-installed programs. The law would not apply to scenarios where a user is notified that an update is available, then takes an active step to install the update (which would be considered to be a self-install), but rather to updates/upgrades that are installed automatically, without user prompting or action. Auto-updates are generally prohibited without consent, but the law explicitly provides that consent may be collected in advance to future updates. Accordingly, businesses may want to consider building such terms (and express consents) into the download/installation process for programs, in order to pave the way for future upgrades/updates.