GREEN EGGS AND SPAM: THE SURPRISING SIDE DISH TO CANADA'S ANTI-SPAM LAW THAT MAY CATCH SOFTWARE BUSINESSES OFF GUARD

Posted on December 2, 2014

Categories: Insights, Publications

Try not to think of Canada's Anti-Spam Law (as it is colloquially known, "**CASL**") as an anti-spam law.1On July 1, 2014, the first parts of CASL became law, regulating electronic communications to or from Canadians for commercial purposes. It generated a lot of "buzz" both nationally and abroad: consumers were inundated with requests from businesses for their consent; charities and other organizations openly worried about CASL's effect on their operations; and lawyers and business people hotly debated the efficacy and approach of CASL.

Lost in that discussion was the important fact that CASL is not really an anti-spam law. Instead, it regulates most electronic interactions, with the broad intent of preventing activities that undermine them.

As a prime example, the legislation's software installation provisions will come into force on January 15, 2015. If the anti-spam elements earned the legislation its "CASL" title, then these new provisions are equally as deserving of bestowing the title "Canada's Software Installation Law" ("**CSIL**"). While the authors doubt it will catch on, this article will refer to the software aspects of the law as CSIL (with apologies to all of the Cecils out there).

CSIL is unique in the world as the only explicit law prohibiting, in the course of commercial activities: (1) the installation of computer programs on another person's computer system without the express consent of the owner or an authorized user of that system, (2) causing such a computer program to be installed without such consent, or (3) having installed such a computer program, causing it to communicate with other electronic devices without such consent. For the prohibition to apply, the installer (or the party directing them) must be in Canada at the relevant time, or the target computer system must be located in Canada. Computers are very broadly defined, including smartphones, tablets, desktops and laptops, and even wearable technology, car computers or smart appliances.2

In order to obtain consent for a prohibited activity under CSIL, the requester must clearly and simply set out: (1) the reasons the consent is sought; (2) who is seeking consent (and if it is not the requester, information about both persons and the relationship between them); (3) certain contact information; (4) a statement indicating

that the target can withdraw their consent at any time; (5) a description, in general terms, of the functions and purpose of the computer program to be installed; and (6) if the computer program performs specified functions (such as collecting personal information, interfering with control of the computer, changing the computer's settings, preferences or commands, or causing the computer to communicate with another system without consent) additional disclosure about the nature and purpose of those functions.

Of course, to obtain that consent, the CSIL restrictions on sending electronic messages will also apply.

In the same way that CSIL does not only apply to repeated unsolicited communications but instead to most messages with a commercial purpose, CSIL does not only apply to malicious programs (such as spyware, spam botnets, viruses, and adware): it applies to all computer programs, and even includes interactions between businesses.3

Fortunately, there are some limited exceptions. If the program in question is included in the following list, consent is deemed to have been given as long as the user's conduct is such that it is reasonable to believe they have consented to its installation: (1) Cookies or HTML;4 (2) Javascript; (3) Operating system; (4) any other program that is executable through another program to which consent has already been given;5 (5) software installed solely to correct failure in a computer system, (6) telecommunications service providers' software that solely protects the security of their networks or updates or upgrades the network.

It should also be noted that CSIL also prohibits any person from aiding, procuring, inducing, or causing a person to "install or cause to be installed" software. This raises the question: who exactly is caught by CSIL? Does it apply to a person who writes an installation program that can be downloaded from the Internet or executed from a compact disc or flash drive that, once executed by the user, installs the intended computer program onto a computer? Does it apply to a person who creates auto-installing media, such as a CD? Does it apply to a program repository, such as Apple Inc.'s App Store or Google Inc.'s Google Play Store, that operates a website from which computer programs can be downloaded and installed? How does it apply to updates and upgrades?

On November 10, 2014, the CRTC posted a *Frequently Asked Questions* (FAQ) document that answered a few of these questions and others, and highlights include the following:6

- The CRTC takes the position that CSIL does not apply to software that is "self-installed" by the owner or an authorized user of the target computer system. The CRTC uses the specific example of someone downloading an application from an app store as an instance of when CSIL will not apply.
- In addition, the CRTC's view is that CSIL does not apply to the "offline installation" of computer programs, so long as the computer programs being installed are those expected to be installed by the owner or authorized user. The CRTC provides two counter examples: (1) if a consumer purchases a music CD and

inserts it into their computer to listen to music or copy songs, and upon loading, the CD automatically installs concealed software, the CRTC will consider the developer to have caused a program to be installed without the express consent of the owner or authorized user, in breach of Section 8, and (2) if a free game installed by a user includes concealed malware, CSIL would not apply to the free game (as it is self-installed) but CSIL would apply to the concealed malware (as it was caused to be installed).

- The CRTC gives its interpretation on how to apply the "additional disclosure" requirements for certain functions by way of example: if a game developer includes functionality to collect information from the GPS, camera, and microphone in a manner that would not be expected by the user, consent would be required if installing the app on another person's computer or if installing an update or upgrade to a self-installed app on another person's computer.
- The CRTC makes a distinction between patches or bug fixes and "updates or upgrades" (in a manner that, in our view, the software industry does not). The CRTC characterizes "patches" or "bug fixes" as software installed solely to correct a failure in a computer system (which do not require consent), whereas an "update or upgrade" involves the replacement of software with a newer version, which may substantially alter its characteristics or operation (and consent is required). When an installer gets initial consent to install the original computer program, it can also seek consent for all future updates and upgrades. But where consent was not obtained on original installation because the program was self-installed, or if the status of consent is in doubt, the installer must request express consent before any updates or upgrades are rolled-out to end-users.
- Where a previously installed program offers an update, and the user installs the update, this would constitute "self-installed software" and is not covered by CSIL. This is contrasted with a situation where a program automatically installs updates in the background without prompting the user.

Of course, lingering questions still remain.

First, when considering Section 9's breadth, what level of conduct must one be engaged in to "aid, procure, induce, or cause" a person to "install or cause to be installed" a computer program? Would a hosting service or website that contains, advertises, or distributes programs that breach Section 8 be caught by this provision? What level of diligence must such a service engage in to protect itself? The examples given by the CRTC are not helpful in this regard:

- in the CRTC's example of a free game with concealed malware, it is unclear what the rationale is for CSIL's applicability to the concealed malware (whether as a standalone program or built into the game) because a self-installed game is not covered by CSIL; and
- in the CRTC's example of consent for GPS, camera or microphone functions in a game's update or upgrade, consent requirements clearly do apply if the update is "pushed" to the end user, but this is

typically handled by the app store or repository, and not by the developer internally.

Second, much discretion is left when determining "reasonability" for the deemed consent or additional disclosure provisions. The CRTC reiterates the reasonability test, stating that, for example, if a user disables Javascript in their browser, the user would not be considered to have deemed express consent to install Javascript programs. But, apart from situations where a user clearly indicates that they do not consent to the installation of certain programs, it remains to be seen what the CRTC will consider to be "reasonable" in situations which are less clear.

Third, it remains unclear where the line will be drawn between "updates or upgrades" and "patches or bug-fixes". As a practical matter, developers frequently roll bug-fixes and feature upgrades into the same update. Where a company does not have express consent to provide future updates or upgrades, would they then be required to separate out patches from upgrades? Would a company be required to do so even if the core-functionality of the program remains unchanged? Furthermore, how can a person supplying an update or upgrade be certain that consent for those upgrades and updates was previously obtained, or has not been revoked?

Last, and in our view most important, while publications such as the CRTC FAQ are certainly of assistance in predicting how the CRTC will interpret the provisions of CSIL, the interpretation provided is non-binding and the CRTC is free to change its view at any time. It seems unlikely that the CRTC would do so if its mandate is to instill confidence in the new law, but significant caution should be taken before relying on the CRTC's interpretation.

But CSIL contains a private right of action that will come into force on July 1, 2017, meaning that individuals (or, more likely, classes of individuals) will be able to sue for violations in their own right. With a three-year limitation period on these private rights of action, it remains unclear whether litigants could "reach back" to violations that occur from January 15, 2015, or whether it would only apply to violations after the private right of action comes into force.7 It remains to be seen whether the courts will accept the CRTC's view on the legislation in cases before them: much like the Canada Revenue Agency or Minister of Finance are frequently corrected by the rulings of courts, it is equally possible for the CRTC to be incorrect about the application of the law.

For these reasons, it remains prudent to take a conservative approach to the new legislation when considering your obligations.

CSIL will necessarily change the way that installers, technicians, repair persons, distributors, repositories, publishers and developers engage users when installing programs on their computers. However, in the same way that the law should not solely be thought of "anti-spam" law, the computer program aspects should not be

thought of as "anti-malware" law: these provisions apply to all computer programs, subject only to the minimal exceptions set out above.

by Ryan J. Black, Sharon Groom and Tyson Gratton

1 In fact, the phrase "unsolicited communication" or even "spam" does not feature in CASL's official 51-word title, which begins: "*An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities*[...]".

2 The definition is made by reference to the Criminal Code, which has well-developed case law on the interpretation of the term "computer system". A "computer system" is defined as "a device or group of interconnected or related devices one or more of which (a) contains computer programs or other data, and (b) pursuant to computer programs, (i) performs logic and control, and (ii) may perform any other function". "Data" means signs, signals, symbols, or concepts that are being prepared or have been prepared in a form suitable for use in a computer system.

3 This is similar to how CSIL does not only apply to unsolicited communications, but instead to all electronic communications with a commercial purpose.

4 We note that it is surprising to think of these as "computer programs", when they are more akin to data.

5 Though an installer of such "plug-in" may not be confident that consent had been given.

6 http://www.crtc.gc.ca/eng/info_sht/i2.htm.

7 It is important to note that it is currently unclear whether the private right of action would apply retroactively to allow a person to bring a claim for a violation that occurred during the transitional period from July 1, 2014, to July 1, 2017. Based on the staggered coming-into-force dates and comments made by Industry Canada at public question-and-answer sessions, it does not appear that the private right of action was intended to apply retroactively, but CSIL is arguably open to this interpretation. This is of obvious concern to business, as one could easily image a line of class action lawyers at the courthouse on July 1, 2017, seeking to file class actions for conduct occurring over what was ostensibly the "transition period" before the private right of action comes into force.

A Cautionary Note


mcmillan