CASL Bulletin

October 2020

CASL – Regulatory guidance for computer program installation rules

Canada's Anti-Spam Legislation (commonly known as "CASL") imposes restrictions and requirements for the installation and use of computer programs on another person's computer system. Some aspects of the rules can be challenging to interpret and apply. In September 2020, the Canadian Radio-television and Telecommunications Commission published updated guidance to help organizations understand and comply with CASL's computer program rules.

CASL

CASL creates a comprehensive regime of offences, enforcement mechanisms and potentially severe penalties designed to prohibit the sending of unsolicited commercial electronic messages ("CEMs"), the unauthorized commercial installation and use of computer programs on another person's computer system and other forms of online fraud. Following are some key aspects of CASL:

- CASL creates an opt-in regime that prohibits, subject to limited exceptions, the sending of a CEM unless the recipient has given consent (express or implied in limited circumstances) to receive the CEM and the CEM complies with prescribed formalities (e.g., information about the sender and an effective and promptly implemented unsubscribe mechanism).
- CASL prohibits, subject to limited exceptions, the installation and use of a computer program on another person's computer system, in the course of a commercial activity, without the express consent of the owner or authorized user of the computer system.
- CASL imposes liability on organizations and individuals (including corporate directors and officers) for both direct and indirect/vicarious CASL violations. CASL provides a due diligence defence.
- CASL violations can result in regulatory penalties of up to $10 million per violation for an organization and $1 million per violation for an individual. CASL includes a private right of action that is not in force.

The Canadian Radio-television and Telecommunications Commission ("CRTC") is responsible for enforcing CASL's rules regarding CEMs and computer programs. The CRTC has taken enforcement action against organizations for alleged violations of CASL's computer program rules. See BLG bulletins _CASL Enforcement Action – $250,000 in Penalties for Aiding the Distribution of Malvertising_ and _CASL enforcement – $100,000 penalty for sending messages and installing software without consent_.

CASL rules for computer programs

Following is a summary of some key elements of CASL's computer program rules, which are found in CASL, the *Electronic Commerce Protection Regulations* and the *Electronic Commerce Protection Regulations (CRTC)*, and are supplemented by CRTC's *Compliance and Enforcement Information Bulletin CRTC 2012-548* and *Compliance and Enforcement Information Bulletin CRTC 2012-549*.

- **Broad application:** The computer program rules are not limited to malware/spyware or other kinds of fraudulent or harmful computer programs. The rules apply to all computer programs, including updates and upgrades to a computer program, unless a specified exception applies.
- **Geographic scope:** The computer program rules apply if a computer program is installed on a computer system located in Canada at the relevant time, or if the person installing or directing the installation or use of the computer program is in Canada at the relevant time.
- **General prohibition:** A person must not, in the course of a commercial activity, install or cause to be installed a computer program on another person's computer system, or cause an electronic message to be sent from another person's computer system on which the person installed, or caused to be installed, a computer program, unless the person has obtained the express consent of the owner or authorized user of the computer system or a specified exception applies. CASL also prohibits aiding, inducing, procuring or causing to be procured a violation of the computer program rules.
- **Express, opt-in consent:** A person must obtain express, opt-in consent to the installation of a computer program on another person's computer system or the sending of messages from another person's computer system.
- **Request for consent – Standard computer programs:** A request for express consent regarding the installation of a computer program must clearly and simply: (1) set out the purpose for which the consent is sought; (2) describe, in general terms, the function and purpose of the computer program that is to be installed if consent is given; (3) specify prescribed information about the identity and contact details of the person seeking consent and any other person on whose behalf the consent is sought; and (4) state that the person whose consent is sought can withdraw their consent.
- **Request for consent – Invasive computer programs:** If a computer program performs specified invasive functions that a person knows and intends will cause a computer system to operate in a manner that is contrary to the reasonable expectations of the owner or authorized user of the computer system, then a request for consent to the installation of the computer program must: (1) be separate and apart from a license agreement; and (2) describe and bring to the attention of the computer system owner or user, separately from any other information provided in the request for consent, additional prescribed information about the computer program's invasive functions. In addition, the person seeking consent must obtain a written acknowledgement from the person giving consent that they understand and agree to the computer program's invasive functions.
- **Separate/discrete consent:** A consent to installation or use of a computer program on another person's computer system must be specific and separate from consents to other kinds of CASL-regulated conduct (e.g., the sending of commercial electronic messages), and must not be subsumed in, or bundled with, requests for consent to the general terms and conditions of use or sale. A person who alleges they obtained consent to the installation or use of a computer program on another person's computer system has the onus of proving the consent.
- **Deemed consent for certain programs:** A person is considered to expressly consent to the installation of certain kinds of computer programs (e.g., a cookie, HTML code, Java Scripts, an operating system, or a program that is necessary to correct a failure in the operation of a computer system or program and is installed for that sole purpose) if the person's conduct is such that it is reasonable to believe that the person consents to the program's installation.
- **Removal of invasive computer programs:** A person who obtains consent to the installation of an invasive computer program based on an inaccurate description of the program must provide a procedure to assist with the removal of the program.

CRTC's updated guidance

Some aspects of CASL's computer program rules can be challenging to interpret and apply. In September 2020, the CRTC updated its guidance titled *Canada's Anti-Spam Legislation Requirements for Installing Computer Programs* to clarify previous guidance regarding the computer program rules and add some useful examples. The guidance warns that it provides general information only, is not legal advice, and is not binding on the CRTC itself.

Following is a summary of key parts of the updated CRTC guidance:

- **Self-installed software:** The CASL rules for software installation do not apply when the owner or authorized user of a computer or device installs a computer program on the computer or device. For example: (1) the owner of a mobile device accesses an online app store and downloads and installs an app on the device; (2) the owner of a device downloads software from a website and installs it on the device; and (3) a business installs software on business devices used by its employees. However, if a computer program performs functions that are not reasonably expected by the owner or authorized user of a computer system, then the program cannot be installed on the computer system without additional information disclosures and the express consent of the owner or user of the computer system.
- **Owner/authorized user:** The "owner" or "authorized user" of a computer or device includes any person who has permission to use the computer or device. For example: (1) if an employer provides a device to an employee, then the employer is the owner of the device, and the employee is the authorized user of the device; (2) if an individual owns a computer but provides it to their relative for their sole use, then the relative is the authorized user of the computer; (3) if a person leases a device, then the lessor is the owner of the device, and the lessee is the authorized user of the device; and (4) if a device is sent out for repair, then the person conducting the repair is an authorized user of the device, but only to the extent they perform the agreed-upon repairs to the device.
- **Cause to be installed:** Following are examples of when a computer program is "caused to be installed": (1) malicious software that is automatically installed without the user's knowledge when the user attempts to install other software; or (2) software concealed on a music CD that is installed when a person inserts the music CD into their computer.
- **Deemed consent for certain programs:** A person will not be considered to have consented to the installation of a cookie or Javascript if the person has disabled those items in the person's browser software.
- **Consent:** Valid consent to installation of a computer program must be obtained based on information disclosures made before the program is installed. A person who relies on consent to installation of a computer program has the burden of proving the consent, and therefore should keep a record of the consent.
- **Updates/upgrades:** Consent to installation of an update or upgrade to a computer program on another person's computer or device may be obtained in various ways, including when a person obtains consent for the installation of the original computer program. Consent to installation of updates or upgrades might be required even if consent was not obtained for the installation of the original computer program (e.g., if the original computer program was self-installed by the owner or authorized user of the computer or device).
- **Invasive computer programs:** Following are examples of computer programs that perform functions that would not normally be expected by a computer system owner or user and for which additional information disclosures and separate express consents are required: (1) a program that collects user credentials, such as usernames and passwords; (2) a program installed on a user's home computer that prevents the user from being able to start the computer; (3) a program that turns on location tracking services without the user's knowledge; (4) a program that blocks the user's access to documents stored on the user's device; (5) a program that causes a computer system to send spam emails to the user's friends and family without the user's authorization; and (6) an internet browser extension that may be activated by a third party to collect, store and use the user's personal information without the user's knowledge.

Comment

The CRTC's recent enforcement action against OneClass and updated guidance regarding CASL's computer program rules are important reminders that organizations that distribute or install computer programs should implement an effective CASL compliance program to reduce the risk of CASL contraventions and help establish a due diligence defence and ameliorate potential sanctions if a CASL contravention occurs. For more information, see BLG bulletin *CASL Compliance Programs — Preparing for Litigation*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's national Compliance with Privacy and Data Protection group includes lawyers, located in BLG's offices across Canada, with expertise in CASL, privacy law, cyber risk management and class action litigation. We provide both proactive CASL compliance advice and legal advice to help respond to a CASL contravention. Additional information about BLG's national Compliance with Privacy and Data Protection group and our services is **available here**.