Bulletin | Cybersecurity, Privacy and Data Protection

January 2021

Canada's Anti-Spam Legislation – Legal compliance reminder for mobile app industry

In November 2020, Canadian regulators issued a public reminder to companies involved in the mobile applications industry about their legal obligations under *Canada's Anti-Spam Legislation* (commonly known as "CASL") and other statutes regarding the promotion, installation and use of mobile apps. The regulatory guidance is important for all organizations that distribute mobile apps to their employees and customers.

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 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. Since CASL came into force in 2014, CRTC has taken enforcement action against organizations and individuals who have violated CASL, and issued enforcement decisions and accepted voluntary undertakings (settlements).

When CASL came into force, it resulted in changes to the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") to prohibit: (1) the collection of personal information by unlawful access to a computer system, and the use of the collected personal information; and (2) the use of address harvesting computer programs to collect an individual's electronic address without consent, and the use of the collected electronic address. Those prohibitions are enforced by the Office of the Privacy Commissioner (OPC).

When CASL came into force, it also resulted in changes to the *Competition Act* to prohibit false or misleading representations in any of the following elements of an electronic message: (1) sender information; (2) subject matter information; (3) locator information (information, including a hyperlink/URL, in a message identifying a source of data); and (4) the body of the message. Those prohibitions are enforced by the Competition Bureau.

CASL rules for computer programs

Following is a summary of some key elements of CASL's rules for computer programs, including mobile apps.

- **Broad application:** The computer program rules apply to all computer programs unless a specified exception applies. The rules are not limited to malware/spyware or other kinds of fraudulent or harmful computer programs.
- **General prohibitions:** 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:** A request for express consent regarding the installation of a computer program must clearly and simply set out specified information. If a computer program performs specified invasive functions that 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 set out additional information and satisfy additional requirements.
- **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 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) 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.

In September 2020, the CRTC published updated guidance titled *Canada's Anti-Spam Legislation Requirements for Installing Computer Programs* to help organizations comply with CASL's computer program rules. See BLG bulletin *CASL – Regulatory guidance for computer program installation rules*.

Guidance for mobile app industry

In November 2020, the CRTC, the OPC and the Competition Bureau jointly issued a news release to announce their issuance of letters to 36 companies involved in the mobile applications industry to encourage them to review and revise their practices to ensure compliance with CASL and related provisions in PIPEDA and the *Competition Act*.

The news release and letter remind mobile app companies of their legal obligations regarding the promotion, installation and use of mobile apps, and encourage mobile app companies to avoid practices that put Canadians at risk of fraud, identity theft and financial loss. The letter includes the following examples of mobile app practices that present legal compliance concerns:

- Apps that convey false or misleading representations to promote a product, service or business interest.
- Apps that collect consumer information without adequately disclosing to consumers how their information will be used or shared (even when the apps are free) or apps that make representations that are false or misleading regarding the collection, use, sharing, storage or disposal of consumer information.

- Apps designed or marketed to collect or use electronic addresses in bulk from a device (e.g., apps that harvest a user's contacts for their own use or to sell/share with other persons) without the user's express consent.
- Apps designed to send unsolicited commercial electronic messages from a device once installed without consent.
- Apps that collect or use personal information by accessing, or enabling access to, a user's computer without consent.
- Apps that don't completely identify their functions, particularly functions that collect personal information, change or interfere with settings, preferences or data, or cause a computer to communicate with another computer system without authorization.
- Apps that, when installed, download a second program on a user's computer or device without the user's knowledge or consent.
- Apps that generate malicious activity once installed (e.g., sending out phishing messages or emails with links to malware).

The letter encourages companies involved in the mobile applications industry to exercise due diligence by adopting additional preventative measures such as: (1) developing and implementing a written corporate compliance program; (2) adopting robust client and app vetting practices; (3) including CASL compliance obligations in agreements with app developers and other persons; and (4) documenting those operating policies and procedures.

Comment

Regulatory guidance regarding CASL's computer program rules is important not only for mobile app developers, but also for organizations that procure and distribute mobile apps to their employees and customers and may be liable for the unlawful operation or use of the apps.

Organizations that distribute mobile apps should also be mindful of their obligations under PIPEDA and provincial personal information protection laws regarding the use of mobile apps to collect, use and disclose personal information. Canadian privacy commissioners have issued guidance for developing and using mobile apps in compliance with personal information protection laws. See for example, *Seizing opportunity: Good privacy practices for developing mobile apps* and *Ten tips for communicating privacy practices to your app's users*.

Organizations that distribute mobile apps 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**.