PALLETT VALO LLP
Lawyers & Trade-Mark Agents

Your Authority For:
Business Law • Commercial Litigation • Commercial Real Estate
Construction • Insolvency & Corporate Restructuring
Employment & Labour • Wills, Estates & Trusts

www.pallettvalo.com

Privacy Law

October 2014

Just When You Thought You'd Heard Enough about Canada's Anti-Spam Law …

A recent sampling of mobile app launches include apps distributed by or on behalf of financial institutions, grocery stores, drug stores, shopping centres, broadcasters, accounting firms, airlines, newspapers, movie theatres, real estate brokerages, social media sites and coffee shops. With the pervasive use of software in commercial activities and the proliferation of mobile apps and tools designed to assist and improve communications with businesses and their customers, provisions of Canada's anti-spam law ("CASL") concerning the distribution and installation of computer programs should be of particular concern to all businesses who distribute or intend on distributing software either alone or as part of their product or service offerings.

In previous newsletters, we have given guidance on the provisions of CASL concerning the sending of "commercial electronic messages" ("CEMs"). Those provisions came into effect on July 1, 2014. With this newsletter, we focus on the provisions of CASL concerning the distribution and installation of computer programs, which will come into force on the fast approaching date of **January 15, 2015**.

Computer Program Installations. The software provisions of CASL apply to anyone who, in the course of a commercial activity, directly or indirectly installs a computer program on another person's computer system ("installer"). A computer program is broadly defined to mean 'data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function.' A computer system is also broadly defined to mean 'a device that, or a group of interconnected or related devices one or more of which, (a) contains computer programs or other data, and (b) pursuant to computer programs, performs logic and control, and may perform any other function'. A computer system can include desktop computers, laptops, tablets, smartphones, and other computing devices.

The CASL provisions will apply if the installer is located in Canada (regardless of where the computer system is located) and will also apply if the computer system is located in Canada (regardless of where the installer is located or where installation originates from).

Express Consent. Aimed at helping with the growing problems associated with malware and spyware, CASL will require every installer to obtain the express and informed consent from the owner or user of the computer system on which computer program is installed ("device owner"). It doesn't matter whether the software installation is triggered by the installer – otherwise known as a push installation – or the device owner – otherwise known as a pull installation; in either case, the applicable provisions of CASL will apply. Unlike the case with CEMs, implied consents will not be permitted.

Express consent will be deemed to exist for certain classes of computer programs (including cookies, HTML code, Java scripts, operating systems, programs executable only through another computer program for which consent was obtained, programs that are necessary and installed only for the purpose of correcting a failure in the operation of the computer system or a program installed on it, and certain other prescribed programs). In addition, as a provisional measure, if a computer program was installed on a person's computer system before July 15, 2015, CASL states that consent for the installation of an update or upgrade to that program is not required until July 15, 2018 (or, if earlier, until the date the device owner notifies the installer that they no longer consent to receiving the installation of the update or upgrade).

Request for Consent. A request for express consent must clearly and simply set out the purpose for which consent is being sought, the person or entity seeking consent (including the identity of anyone on whose behalf consent is being sought) and the function and purpose of each computer program being installed. A request for consent must be separated from any software license terms and separately agreed to by the device owner. An installer will also need to separately identify and describe, if they exist, certain prescribed functions of the computer program, including whether it will:

- collect any personal information stored on the computer system,
- interfere with the device owner's use or control of the computer system,
- surreptitiously change or interfere with any preferences, settings or commands on the computer system,
- change or interfere with any data stored on the computer system in a manner which disrupts or interferes with access or use of the data by the device owner,

- causes the computer system to communicate with another computer system without authorization, or
- install another computer program that can be surreptitiously activated by a third party.

In addition, if the computer program performs any of the functions set out above, the installer must provide a device owner with an electronic address at which the installer can be reached. If during a period of one year after installation, the device owner believes that the function, purpose or impact of the computer program installed under the consent was not accurately described when consent was requested, the device owner can send a request to the installer at that electronic address to remove or disable the computer program. The installer must, at no cost to the device owner, assist the device owner in removing or disabling the computer program as soon as feasible upon receipt of a request, so long as the original installation of the consent was in fact based on an inaccurate description of the material elements of the functions described above.

Potential Penalties. As with other CASL violations, a failure to comply could result in administrative penalties of up to $1 million per violation, for an individual, or up to $10 million per violation, for a business. In addition, there are criminal sanctions which will, upon a summary conviction of a business, require payment of fines for each violation of up to $100,000 for a first offence or $250,000 for a subsequent offence. For individuals, the criminal fines required upon a summary conviction are up to $10,000 for a first offence or $25,000 for a subsequent offence. Finally, CASL provides for a private right of action beginning July 1, 2017, and provides for statutory damages of up to $1 million per day. We anticipate that numerous class action lawsuits will be launched once these private right of action provisions go into effect.

Directors, officers, agents and mandataries of a corporation can be held liable for the acts of their organization if they directed, authorized, assented to, acquiesced in or participated in the CASL violation.

Practical Advice. As with the provisions of CASL relating to CEMs, the enforcement of the computer program installation provisions of CASL will be complaint driven. According to the CRTC, it received almost 85,000 complaints regarding CEMs in the first two months after the sections of CASL concerning CEMs came into force on July 1, 2014. Thus, it is likely that we will see many complaints also being filed after January 15, 2015 concerning the unauthorized installation of computer programs. The CRTC has stated that it will focus its attention and investigations on cases where there are a significant number of complaints or where there appears to be a major transgression.

If you or your organization, through a website or otherwise, offer mobile applications or tools, embed software features into your products or services or otherwise make software available to your customers or members, you should be reviewing the functions of your software and any embedded or 'piggyback' third party software included with it. You should also be reviewing your end-user license agreements as well as your installation processes to ensure compliance with CASL requirements.

If you require assistance with any of the above, the members of our Privacy Law Group would be pleased to assist you.

Joe Conte is a member of the Privacy Law Group.

Pallett Valo LLP Privacy Law Group

Pallett Valo LLP's Privacy Law Group advises and supports private sector organizations to comply with their obligations under Canada's Anti-Spam Legislation and the *Personal Information Protection and Electronic Documents Act*. We assist our clients in developing privacy policies and practices to meet strategic business needs and to ensure compliance with privacy legislation. We are also experienced in advising clients regarding the *Freedom of Information Act and Protection of Privacy Act,* the *Personal Health Information Protection Act,* and the *Municipal Freedom of Information and Protection of Privacy Act*.

Contact Members of the Privacy Law Group

Andy Balaura abalaura@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 225

Joe Conte jconte@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 217