mcmillan

at a glance

Canada's Anti-Spam Law: Are You Ready?

Ten years in the making, Canada's "anti-spam" law, colloquially called CASL in spite of its actual 51-word title, comes into force on July 1, 2014. With its significant penalties (including directors' and officers' personal liability and class action lawsuits) and broad prohibition, those doing business in Canada or commercially communicating with Canadians must come to realize that CASL covers much more ground than "anti-spam" law: it regulates most electronic interactions and significantly alters the Canadian landscape of electronic business.

Prohibition on Commercial Electronic Messages*

CASL stringently regulates "commercial electronic messages" (CEMs), being messages sent to an electronic address where one of its purposes is to encourage participation in a commercial activity. This prohibition is not limited to "spam", "mass mails", certain marketing efforts, or even messages that are "primarily" commercial: it applies to all CEMs. The prohibition applies if a computer system located in Canada is "used to send or access the electronic message", so it even applies to messages sent to or from other jurisdictions. There are rules that might lessen the burden for messages sent from Canada to certain countries, but they are vaguely drafted; the possibility remains that those sending CEMs from Canada must comply with both CASL and the other jurisdiction's laws on unsolicited messages.

CASL generally prohibits sending a CEM unless both: (a) the recipient has consented to receiving it (express or implied); and (b) the message contains prescribed information and an unsubscribe mechanism. There are indeed exceptions (narrowly drafted) and specified implied consent rules (time limited and governed by detailed and nuanced rules that will require tracking contact lists with a newfound granularity), but the burden of establishing them is on the sender. Even requests for consent are CEMs, and so a business must paradoxically have consent in order to even send the request for express consent to begin with. There is no possibility of pre-checking "I consent" boxes, or of burying consent in privacy language, end use licenses, or other terms and conditions. All of this places urgency to obtain express consent where practicable (or, if that is not practicable, to institute business processes that facilitate implied consent management) before CASL comes into force. CASL was clearly designed to make express consent the "gold standard", but implied consent or other exceptions may be more practical for many businesses even if the management of it will be difficult.

Prohibition on False/Misleading Electronic Messages*

CASL amends the Competition Act to prohibit directly or indirectly promoting any business interest (or products or services) using false or misleading representations in any of the individual sender, subject matter, content, or URL/locator elements of an electronic message. Like other Competition Act prohibitions, these are enforced separately criminally (prison to 14 years and large fines) as well as through "reviewable conduct" mechanisms such as administrative penalties (up to $10,000,000 for corporations), private rights of action or other remedies. These prohibitions apply to all electronic communications (not just "spammers"), and the general impression of the message will be taken into account. As a result of CASL, email or other electronic message campaigns will be subject to additional, more stringently-legislated scrutiny.

Prohibitions on Harvesting Information or Using It*

CASL amends the Personal Information Protection and Electronic Documents Act to specifically prohibit the collection and use of personal information or electronic addresses without consent or knowledge in the case of (a) data mining or other types of automated crawling, or (b) any means of telecommunication if it is obtained through accessing a computer system in an illegal manner. There are exceptions for law enforcement or investigative purposes.

Prohibition on Installing Computer Programs**

An example of the dangers of CASL's "anti-spam" moniker is that CASL introduces new consent requirements when

** in force July 1, 2014*
*** in force January 15, 2015*

installing software during any commercial activity (or causing those computers to send messages once installed). This prohibition applies if the target computer system is located in Canada, or if the person performing the prohibited act is in Canada (or under the direction of someone in Canada). This affects all software installations on all computing devices (including "smart" televisions, wearable computing devices, and even automobiles and some home appliances). Even more stringent disclosure and consent rules apply if the software does any specified activities, like collecting personal information, changing settings or preferences, intercepting or manipulating data, or installing others' software. No malicious intent is required; these provisions will apply to legitimate businesses such as repair people, software vendors, and IT consultants.

Consent may be obtained through opt-in express consent. There are information and disclosure requirements when obtaining consent, particularly if the software performs certain functions (as described above), and consent cannot be tucked into terms and conditions or buried in the license agreement (EULA). Deemed consent occurs when the circumstances reasonably dictate for particular types of software (examples include HTML code, JavaScript, or operating systems) or situations (like upgrading already consented-to software, or network operators patching security flaws). Consent will also be deemed for upgrades and updates on existing installations as of January 15, 2015, for three years thereafter (so until January 15, 2018), which "transitional period" should be used to obtain express consent.

Prohibition on Altering Transmission Data*

CASL generally prohibits, in a commercial context, the alteration of transmission data so as to re-route an electronic message without the sender's or the recipient's consent. Primarily, this appears to be directed at "man-in-the-middle" attacks (eavesdropping on or intercepting communications). Similar to consent requests for CEMs, express consent must be in a prescribed form, containing identity and contact information as well as the purposes for which the consent is being sought, and the person expressing consent must be given the opportunity later to withdraw that consent.

** in force July 1, 2014*

Enforcement and Liability—Employers, Directors and Officers

CASL contemplates enforcement by two methods: CRTC enforcement, and private lawsuits. Until July 1, 2017 (3 years from coming into force), the CRTC will enforce CASL by pursuing violations through imposing undertakings (essentially, covenants to correct violations) or administrative penalties, the latter up to $1,000,000 for individuals and $10,000,000 for others. The general public will report violations through the fightspam.gc.ca website, and the CRTC can publicly name violators and punishments. On July 1, 2017, private individuals will be able to pursue CASL contraventions through private lawsuits (PRAs), with compensation equal to damages and expenses plus up to $200 per violation to a maximum of $1,000,000 per day (expect class action lawsuits on this).

Whether pursued by CRTC or through PRAs, officers and directors of companies are personally liable if they directed, authorized, assented to, acquiesced or participated in the violation or contravention. Employers are also vicariously responsible for the acts of their employees. Because of this, businesses must take care to conduct themselves, and directors and officers must exercise their duties, to avail themselves of CASL's general "due diligence defense". If a breach is found, evidence of the due diligence measures undertaken by the business may act as a full defence or factor into damages or penalties. CASL "first contact" or email/communication policies will be key to compliance.

For more information, please contact:

Ryan J. Black
604.691.7422
ryan.black@mcmillan.ca

Dawn Mains
403.231.8390
dawn.mains@mcmillan.ca

Janine MacNeil
416.307.4124
janine.macneil@mcmillan.ca

Elisabeth Preston
613.232.7171 ext.196
elisabeth.preston@mcmillan.ca

Éloïse Gratton
514.987.5093
eloise.gratton@mcmillan.ca