May 2011

mcmillan privacy bulletin

Canada's anti-spam legislation ("CASL") – advance preparation is needed now

Canada's new Anti-Spam law, or CASL for short, was passed in December and is now awaiting proclamation.[1] This will happen as soon as draft regulations have been gazetted for comment and then issued in final form, which could be as early as this September. Industry Canada is hoping to release the draft regulations by late June, although bringing the new Industry Minister up to speed on the law will have to compete with other legislative priorities.

Originally conceived primarily as a law to counter spam, CASL will have a major impact on how Canadian businesses conduct operations and market their products. New rules for electronic communications will compel companies to review their current email practices and, most likely, require them to re-qualify their email customer/contact lists to make them compliant. In many cases, doing this before CASL comes into force will have significant advantages.

The legislation also address computer hacking and interception of electronic communications.

CASL overview

The general rule is that express, "opt-in" consent must be obtained from intended recipients, subject to a proviso that "implied" consent may be used within specifically defined circumstances such as a contractual relationship with a recipient. This approach contrasts broadly with the consent rules under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") — which have governed businesses' e-mail marketing activities since January 1, 2000 — and will require more stringent procedures than under that Act. PIPEDA permits "opt-out" consent and does not limit implied consent to specific relationships or transactions, as under CASL.

The bottom line is that most organizations which currently maintain PIPEDA-compliant e-mail contact lists likely will discover that those lists are not grandfathered under the new legislation and that they will need to be re-qualified by fresh, opt-in consent. If they do not have such consent today, they will need to take steps prior to the effectiveness date since following that date they will not be permitted to contact persons on their lists by electronic means (unless they fall within an excepted or implied consent category), even for purposes of seeking consent.

---

[1] *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, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act,"* passed December 15, 2010.

In addition to the consent rules, CASL stipulates that all e-mails must include a readily usable "unsubscribe" mechanism and contain prescribed sender identity information. As well, the Act creates new offences under the *Competition Act* for false or misleading subject lines or sender particulars.

basic prohibition

The basic prohibition contained in CASL is against sending "commercial electronic messages" unless the recipient has consented to receiving the message and the message contains certain prescribed information, including the identity of the sender and the sender's contact information, as well as the unsubscribe mechanism. The definition of "electronic message" is very broad and extends to voice communications (although a separate provision excludes two-way voice, pre-recorded one-way voice and fax communications, many of which currently are governed by the separate National Do Not Call Rules). What is considered "commercial" is similarly very broad — including any offer to transact any product or service or an interest in land, offer an economic opportunity (including gambling) or to promote any of these activities.

The required unsubscribe mechanism must remain operative for 60 days. An unsubscribe request must be acted on within 10 days.

exclusions/exemptions

Several broad categories of messages are excluded entirely from the prohibition or, while governed by it, will have no consent requirement.

Excluded entirely are messages between individuals having a family or other personal relationship (which will be defined more explicitly by regulation) and business-to-business inquiries or applications. A second category of messages will be required to comply with the content provisions but not the consent requirement. This category broadly includes commercial communications that have a consensual basis, specifically: providing a quote in response to a request, facilitating a commercial transaction, providing warranty, product recall or safety information about a purchased product, providing information regarding the ongoing use of a purchased product or service or an employment relationship, or delivering a product or service (including upgrades) respecting a previously purchased product or service, to which the purchaser is entitled.

A further broad group of electronic communications in effect is exempt from the consent requirements by falling under the category of "implied consent." The most important of these are the sub-categories of "existing business relationship" and "existing non-business relationship." The term "implied consent" is defined to include only specified circumstances: in addition to the two noted sub-categories, it includes a person posting an e-mail address in effect inviting communications or providing an e-mail address to a sender with no indicated intent not to receive messages, provided that any message sent is relevant to the person's business. There is scope to add additional sub-categories by regulations, however, to date, there is no indication that this will be done.

The scope of the "implied consent" rule is delimited by the explicit definitions given to the operative terms "existing business relationship" and "existing non-business relationship," both of which — when account is taken for their differential contexts — have similar elements. In essence, the required element is either a commercial relationship (e.g., product purchase or written contract) or a non-commercial relationship (gift or donation,

volunteer work or membership in an organization) in existence currently or within the previous two years. In addition to an actual transaction, an existing business relationship includes an inquiry made within the previous six months.

express consent

The scheme of the legislation is, broadly, that if a person wishing to send commercial e-mails does not qualify within either of the exempt categories (essentially, personal or on-going commercial relationships) and cannot qualify under the defined "implied consent" category, that person must obtain a recipient's express consent prior to sending any e-mail communication. *This limitation extends to any e-mail requesting consent to receive future communications*.

Express consent under CASL must be given on an "opt-in" basis. The request for consent must set out clearly the purposes for which it is sought and, in a prescribed manner, identity information of the requestor. A further provision places the onus on the organization to prove that consent was obtained. Finally, the required "unsubscribe" function means that a readily available "opt-out" (e.g. link) also must be provided.

Obtaining express consent to send commercial e-mails will be a significant consideration under CASL. The two exempt categories and the defined "implied consent" sub-categories will permit e-mail communication for active, or recently ended, commercial and non-commercial relationships. However, organizations that rely on e-mail to communicate and market to a broader community will need to obtain express consent to ensure that their messages are compliant. Furthermore, most organizations that maintain e-mail contact lists are unlikely to want to limit those lists to current or recent customers (or donors). While such recipients clearly are an important element in contact lists, organizations typically do not remove them from their lists once that active relationship has ended. To comply with the new legislation, removal of names from a list would need to be done at the two-year post-transaction (or six-month post-inquiry) point. Even if organizations *were* inclined to "scrub" their lists in this manner, effective management of such a process would be challenging requiring not only comprehensive input criteria (e.g., relevant end-dates of transactions; date of last inquiry) but also an active due diligence function to ensure compliance.

re-qualifying contact lists

It is more likely that organizations will seek to develop permanently qualified contact lists, which can only be done through obtaining express consent. Clearly, qualifying contact lists under CASL will be a challenging — and potentially costly — process for organizations. Various strategies may be identified. However the common denominator will be that, over and above currently existing, PIPEDA-compliant, consents (which likely will not qualify as express consent, or in any event are unlikely to be recorded as such), a new, positive opt-in consent will be required.

The legislation appears to recognize — to a degree — the burden that this requalification will place on organizations. A three-year "transitional period" is provided for — essentially extending the two-year post-transaction period for an additional year in respect of lists that qualify under the implied consent rule at the time the legislation comes into force.[2] However

[2] Also extends the six-month post-inquiry period to the full three years.

this extension only applies in respect of recipients who otherwise qualify on the basis of an existing business or non-business relationship that includes electronic communications. It does not address any grandfathering or transitional mechanism for existing contact lists. Consequently, organizations should be considering qualification procedures in advance of the legislation coming into force, since, once that occurs, current consents will not qualify for purposes of e-mail requests for a CASL-compliant consent — only CASL qualifying consents may be used, which for the most part likely will fall under one of the new defined "implied consent" sub-categories.

computer hacking

The new Act also contains anti-hacking prohibitions — against unauthorized interference with private electronic messages, and unauthorized downloads and access to computer systems. The general rule is that express consent is required to interfere with a message or to download. Furthermore, if downloaded software will perform functions such as collecting the user's personal information or changing settings already installed on a computer, or interfering with stored data, this fact must be described clearly, prominently and separately apart from the license attached to the software.

Downloading of certain computer programs, such as cookies, where it is reasonable to assume the user's consent, as well as upgrades to existing programs that have been installed previously with the user's consent, are deemed to have received express consent.

non-compliance

The implication of non-compliance with the Act's e-mail prohibitions can be severe, as is reflected in the remedial and offence provisions in the legislation. The legislation's thrust is to remedy bad practices of spammers. However it casts its net so widely that compliance-oriented organizations across the board, as well as small businesses who may lack the sophistication to knowledgeably comply, will face the same risks of non-compliance.

CASL provides for three categories of remedies or penalties:

(i) administrative monetary penalties (or "AMPs") for violations of the Act in amounts of up to $1,000,000 for individuals and $10,000,000 for other entities;

(ii) criminal offences for obstructing an investigation; and

(iii) a private right of action for persons suffering actual loss or damage as a result of non-compliance with CASL or the related prohibitions contained in the *Competition Act* and PIPEDA.

With respect to both the violations and the criminal offences, directors and officers who authorized an organization's non-compliance will be personally liable.

The private right of action is significant and potentially far-reaching. It is available to any individual or other person who has suffered damage as a result of non-compliance. While it will be necessary to prove actual damages, it is possible to envisage class actions involving potentially thousands, or even millions, of plaintiffs.[3]

[3] By contrast, the US "CAN-SPAM" law limits the private right of action to service intermediaries such as ISPs which may incur unwanted costs as a result of illegal spamming.

summary

Canada's new proposed new Anti-Spam law, CASL, while containing significant tools to combat bad spam and to make e-mail marketing more user-friendly and respectful, will require the broad spectrum of Canadian businesses and charities to devote significant attention (and resources) to re-qualifying their procedures for e-mail communications. Industry Canada, the author of the Act, appears to appreciate this potential impact. However the transitional provisions provided in the Act may be of limited assistance. Organizations that use email as a key communications tool will need to re-qualify their contact lists and should consider doing so in advance of the law coming into force.

By: David Young and Robert Hester, Student at Law

For more information on this topic, please contact:

Toronto	David Young	416.307.4118	david.young@mcmillan.ca
Montréal	Eloise Gratton	514.987.5093	eloise.gratton@mcmillan.ca
Vancouver	James Bond, Q.C.	604.691.7437	james.bond@mcmillan.ca
Ottawa	Barbara Sinclair	613.232.7171	barbara.sinclair@mcmillan.ca

a cautionary note