CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

May 2014

Director Alert

Canada's Anti-Spam Law ("CASL"): It's the Law on July 1, 2014 – questions for directors to ask

Author: Jennifer Babe, LL.M, ICD.D

Why Should I Read This Alert?

a) despite its name, this Act covers much more than spamming mass emails;
b) as a director or officer you are exposed to personal liability under this statute;
c) it is very likely that your organization is subject to this new legislation;
d) the potential economic penalties are steep

This legislation is imminent and directors need to take steps to ensure their organizations are prepared.

What is CASL?

If your first question as a director is: "What is CASL?", then you are not alone in asking this question, and there is an immediate need for you and your board to get up to speed on this sweeping and difficult legislation. Canada is the last G20 country to enact anti-spam legislation and when this statute goes into effect on July 1, 2014, Canada will have the most onerous and broad legislation in this area on the planet.

This Director Alert aims to provide you with information about the following:

a) the legislation, what it regulates generally, and in particular "commercial electronic messages", called "CEMs";
b) the penalties for a CASL breach; and
c) the questions as a director you should ask of your organization about its CASL preparedness.

This article is providing general information. Your organization needs to consult its legal counsel to help it create a compliant CASL regime unique to its own operations.

The Legislation

On December 4, 2013, the government announced that the bulk of the legislation would go into force on July 1, 2014. The statute is:

> 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* (S.C. 2010, c. 23)

The CASL provisions against altering someone else's computer without their consent goes into force in January 2015 and the right of private prosecution (class actions) goes into effect July 1, 2017.

As there is no official short title for this Act, it is called unofficially, "Canada's Anti-Spam Legislation" or "CASL".

What Does CASL Regulate?

CASL covers a broad range of activities, including prohibiting:

a) sending a CEM via any electronic medium (email, social media, instant messenger, etc) without the recipient's express or implied consent;
b) hacking, malware and spyware;
c) phishing, fraudulent or misleading practices;
d) altering someone else's data transmission;
e) privacy invasion via your computer, including data mining for personal information or using personal information collected from data mining; and
f) as of January 2015, altering someone else's computer device unless you have their consent (such as downloading a conference app to your smart device), or it is part of your contract obligations to do so (such as updates from your software virus protection supplier), excepting only certain programs listed in CASL, such as cookies, HTML, and Java.

CASL is sweeping, capturing CEMs sent business-to-business, business-to-consumers and between individuals.

Will CASL Apply to Our Organization?

CASL will most likely apply to your organization. CASL has the potential to impact any individual or organization in Canada that sends electronic messages (i.e. email, text, sound, voice, and image) to an electronic address (i.e. business, consumer, individual).

There is no exemption in CASL for not-for-profits, charities, volunteer associations or the MUSH sector (municipalities, universities, schools and hospitals). The regime focuses on the action being done, and not the entity doing the action.

Penalties

The regulators will use economic disincentives, in addition to civil sanctions, to protect electronic commerce. The penalties for a CASL breach include:

a) administrative monetary penalties of up to $10 million per violation on an organization and up to $1 million per violation on an individual;
b) personal liability on officers and directors;
c) vicarious liability on the entity for acts of its employees and agents; and
d) private prosecutions to be allowed as of July 1, 2017. These will likely be in the form of class action claims.

To be able to defend against claims, directors and organizations need to create a due diligence defence by demonstrating that they have taken proactive steps to establish policies, procedures and processes to address CASL compliance, and monitored to enforce these policies going forward.

CEMs

A CEM is a message sent to a third party in any electronic media, business to business, business to consumer, or between individuals. CASL creates a general prohibition against transmitting a CEM to an electronic address, unless:

a) the intended receiver consents to its receipt, and
b) the message includes certain prescribed information.

The onus of proving consent is on the sender of the CEM. Subject to certain limited exemptions and exclusions, the sender of the CEM needs the prior express consent from the recipient.

The threshold issue will be: is it a commercial electronic message? Commercial activity involves any transaction, act or conduct or regular course of conduct that is of a commercial character, whether or not it is done in expectation of profit.

The regulator has said that very generally, a CEM is one that encourages or deals with an exchange of money, such as the sale of goods or services for a fee.

Privacy Consent vs. CASL Consent

Having privacy consent is not CASL consent. Quebec's privacy law requires the positive consent of the individual to the use of his or her "personal information" for marketing purposes. The federal privacy statute, and those in effect in BC and Alberta, allow for a free and easy opt-out from getting marketing information.

CASL prohibits the sending of any CEM or marketing information by electronic means without the express opt-in by the recipient. Without CASL consent, or the ability to rely on an implied consent or exemption, your organization will need to return to phone calls (subject to the do not call legislation), faxes and postal delivery.

Some Exemptions and Implied Consents for CEMs:

The following are some of the CASL provisions dealing with implied consent or an exemption from the Act that may be used by organizations when considering the CEMs they send. Each of these needs to be considered using the legislated definitions and whether the mandatory content and unsubscribe mechanism must still be provided despite the implied consent or exemption.

Many of these provisions are subject to interpretation, and readers are cautioned not to rely merely on this short form listing:

a) Consent may be implied where:
   i) there is an "existing business relationship" or "existing non-business relationship". Note that this implied consent is time limited;
   ii) the recipient has "conspicuously published" their email address (i.e. company website) and the message is relevant to the recipient's business role; and
   iii) the recipient has disclosed their email address to the sender (i.e. provided business card) and the message is relevant to the person's role or duties in business or official capacity.

b) Exempt from CASL are CEMs sent:
   i) internally within a business by an employee, representative, consultant or franchisee, where the CEM concerns the activities of the business;
   ii) between businesses, if they have a relationship and the message concerns the activities of the organization to which it is sent;
   iii) between individuals who have a "personal" or "family" relationship (as defined);
   iv) to a person who is engaged in a commercial activity if it consists solely of an inquiry or application related to that activity (e.g. an employment inquiry);
   v) in response to a request, inquiry or complaint or is otherwise solicited by the person to whom the message is sent;
   vi) interactive two-way voice communications and faxes and voice messages sent to telephone accounts (subject to the national do not call list regime); and

vii) as otherwise set out in the Act for such matters as enforcing a legal right, a safety matter such as a product recall, or providing information about a benefit plan to employees.

CEMs Have Mandatory Content and Unsubscribe Requirements

As noted before, a CEM must deal with both the consent requirements and the mandatory information content and unsubscribe mechanism. Even where consent is implied or there is an exemption from consent, some CEMs must still have the mandatory content and unsubscribe.

Generally speaking the mandatory information to include with each CEM includes the identifying party seeking consent, the identity of an agent assisting it, such as a marketing firm sending out the CEMs for the principal, and contact information.

The unsubscribe mechanism must be without cost to the recipient and easy to use, such as an email or phone call. It can be a link to a webpage, but the regulator has said at a presentation that it should not require the recipient to navigate through several pages and be complicated to do. The request to unsubscribe must be honoured by the sender of the CEM within 10 days.

The Three Regulators

The CASL regulators are:

a) the Commissioner of Competition under the *Competition Act;*

b) the Privacy Commissioner under the *Personal Information Protection and Electronic Documents Act*; and

c) the Canadian Radio-television and Telecommunications Commission (CRTC).

The CRTC will run the spam reporting centre to receive complaints from the public, and investigate and prosecute offenders. These regulators will share information among themselves and with international bodies in international investigations and prosecutions.

Cross Border

CASL applies to CEMs sent from a computer device in Canada or accessed by someone using a computer device located in Canada. Hence senders of CEMs into Canada must comply with CASL, and if a Canadian is sending CEMs out of Canada, CASL provides you must comply with the law of the jurisdiction of the recipient of your CEM.

Getting Ready for Compliance

There is a short window of opportunity before July 1, 2014. Now is the time to obtain express consent to receipt of your organization's CEMs by electronic means. Once CASL is proclaimed into force the Act makes it an offence to send an email to get this consent.

Questions for directors to ask

1. Who on the senior management team is accountable for our CASL compliance work?

2. When will the board of directors get a report from management on the state of the CASL team's work and their recommendations on internal policies for our CASL compliance? Has our privacy policy been updated to reflect CASL?

3. What steps are being taken before the July 1, 2014 start of CASL to collect express consent?

4. Where does CASL appear on our risk management dashboard?

(cont'd on next page)

Questions for directors to ask (cont'd.)

5. So much of CASL is dependent on information technology systems. Do we have the budget to adapt our IT systems to comply?

6. Is there any impact on our existing covenants to regulators or third parties, such as our bank credit agreement, about our "compliance with all its laws"?

7. Have we considered amendments to our contracts with third party suppliers to the organization, such as marketing firms and software providers, about their CASL compliance and their indemnities to the organization? For example, can our electronic newsletter distributor capture unsubscribe messages and put them into effect in 10 days?

8. Have we changed our definition of "member" under our federal articles of continuance before or after July 1, 2014 for the "member" implied consent?

9. What is the impact on our cost of fund raising as a registered charity if we consider our CEMs to be "primarily for fund raising purposes" to use this CASL exemption?

10. Has our employees' manual been updated for any "bring your own device" rules for CASL and have we done employee training?

11. What is our plan to establish a due diligence defence for any regulatory investigation or civil cause of action?

12. Does our insurance policy cover a CASL complaint? (Note: we are hearing no insurers are prepared to sell coverage for this open ended risk.)

13. Does our directors' liability insurance policy cover me for defence costs for my personal liability? (Note: generally speaking, no insurance policy pays fines or penalties.)

14. Is CASL compliance a standing board agenda item as we get ready to comply and then ensuring compliance is maintained?

A checklist for CASL preparation is posted on the CASL services portion of the Miller Thomson website.