PALLETT VALO LLP
Lawyers & Trade-Mark Agents

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

www.pallettvalo.com

Privacy Law

May 2013

Canada's Anti-Spam Legislation: The Clock is Ticking…

As you've probably heard, Canada has enacted tough new legislation to combat unwanted electronic communications, or spam, a problem that's both annoying and expensive. Unwelcome sales messages cost businesses time and money by impeding the flow of legitimate business communications and electronic commerce. The new Anti-Spam Law (known unofficially as "CASL") represents the federal government's attempt to fight spam, and is considered to be one of the toughest anti-spam laws in the world.

When CASL takes effect in late 2013 or early 2014 (timing for the new rules is discussed in more detail below), however, it will do more than just penalize spammers: by creating an "opt-in" consent requirement for almost every commercial electronic message (a "CEM") sent for a commercial purpose, the new legislation will affect virtually every business operating in Canada or communicating with Canadians. Customer consent will now be required not only for email marketing campaigns, but also for newsletters and many other routine paperless communications from both large and small businesses as well as non-profit organizations.

What Do You Need to Know Now?

A more detailed summary of CASL's new requirements for CEMs is set out below. The bottom line is that CASL is certain to affect your business in the near future, so you will need to get ready now by taking stock of your current marketing and electronic communication practices. Depending on your business and the scope of your electronic marketing, this could involve examining your relationship with third party marketing services and agents. Here is a high-level list of the tasks you should be getting started on now:

- Your client, donor and contact databases will need to be reviewed to determine, to the greatest extent possible, the source of the contact and whether express and verifiable consent to receive CEMs from you was ever obtained from that contact.
- If the contact has not given you express consent to receive your CEMs, you will have to consider whether consent can be implied from an existing business relationship, such as if the contact bought or leased any products or services from you, entered into any contracts with you within the last two years or sent you an inquiry or application within the last six months.
- Non-profit organizations will have to consider if consent can be implied from an existing non-business relationship, such as if the contact made a donation to your organization, performed volunteer work or became a member within the last two years.
- You will need to determine the date on which express consent was received or the implied relationship began. Going forward, your contacts will also have to be reviewed every two years to ensure that consents have not expired.
- Your email systems and websites may also have to be overhauled to comply with the new rules, to ensure that you meet the CRTC's content requirements and include an acceptable unsubscribe mechanism for email and text messages.
- You will need to determine how you will obtain and monitor consents from your contacts and begin setting up your email and website response systems.
- Once CASL is in effect, you will have to consider whether every electronic message your organization sends is a CEM (i.e., whether it contains an offer to sell, or advertises or promotes anything or anyone) and whether any of the exceptions to the consent requirement apply.
- If the message is a CEM, you will have to make sure it contains the required contact information and unsubscribe mechanisms (and whether those mechanisms function correctly).
- You will have to ensure that you are complying with unsubscribe requests are being processed properly and on time.
- You will also have to think about internal policies and staff training in this area so that your organization is ready to roll when the new anti-spam regime takes effect.

Although enforcement with the new CASL regime may be several months or even a year away, the scope of the new rules, the severity of the potential penalties and the number of technical issues involved in complying all mean that you should be preparing now.

A Question of Timing

CASL received Royal Assent in December 2010, but the government has held off on proclaiming it into force while regulations are drafted and reviewed through a public consultation process. Regulations from the Canada Radio-television and Telecommunications Commission (the "CRTC") were finalized this spring. A second set of cabinet (Governor in Council) regulations from Industry Canada are not yet finalized. A first discussion draft of the Industry Canada regulations was released for public comment in mid-2011, resulting in the release of a second revised draft in January 2013. A large number of submissions were made by industry groups, legal experts and other stakeholders in response to this second draft (some of which can be downloaded from the Industry Canada website). A final version of the Industry Canada regulations will not be released until the government has had a chance to consider these submissions, likely later in 2013.

Recent public remarks by Industry Canada officials suggest that CASL may not come into force until the second half of 2014. The delay is perceived by many to be attributable to widespread criticism about the scope of the new legislation and its negative impact on the bottom line of most businesses.

What's in the New Rules?

The purpose of CASL is to improve the Canadian economy by prohibiting CEMs from being sent without the prior consent of the recipient, but without discouraging electronic commerce or impeding legitimate business operations. Electronic message is broadly defined to include email and voicemail messages containing text, sounds, voices or images. CEMs include communications which:

- contain offers to purchase, sell or lease a product, goods or a service;
- contain offers to provide a business, investment or gaming opportunity;
- advertise or promote products, services and people;
- promote a person as someone who does anything referred to above or intends to do so; or
- contain a request for consent to send a CEM.

CEMs are permitted under the new legislation if they meet two conditions: first, the recipient must have either expressly or impliedly consented to receiving the message, and second, the message must meet certain content requirements. Consent to receive a commercial electronic message may be implied in certain circumstances, such as where the parties have had a previous business relationship in the last two years, or where message recipients have published or disclosed their email addresses without stating they do not wish to receive unsolicited commercial messages. Implied consent also applies to existing "non-business" relationships, such as those arising from making donations, doing volunteer work or becoming a member of an organization.

What Must Messages Contain?

The content requirements for permitted CEMs include an unsubscribe mechanism and information identifying and providing contact details for the sender. The unsubscribe mechanism must be effective immediately and remain valid for at least 60 days after the message is sent. Contact details to be required on all CEMs include the name by which the sender carries on business; a mailing address and phone number and either an email address or web address for the sender. A request for consent to send CEMs to a person or business must include the same contact information and must state that the consent can be withdrawn.

In October 2012, the CRTC issued advisory bulletins providing more guidelines on the content requirements for CEMs and the acceptable mechanisms for a recipient to provide consent to receiving further messages. The CRTC clarified that an intermediary (such as a marketing campaign service-provider) does not have to provide its contact information on a CEM if it has no role in determining the content or recipients of the message. The entity or entities on whose behalf the CEM is sent must provide a full mailing address.

The New Consent Requirement

Although CASL allows a business to obtain a recipient's

consent to CEMs either orally, electronically or in writing, the CRTC's guidelines state that oral consent must be verifiable, either by an independent third party or by audio recording.

The CRTC also provided examples of acceptable unsubscribe mechanisms, which must be accessible without delay and should be simple, quick and easy for a consumer to use. As well, CEMs sent by text message (SMS) should allow the recipient to unsubscribe by replying "STOP" or "UNSUBSCRIBE" to the message or by clicking a link that will take them to a website form on which subscription choices can be submitted. The CRTC's view is that unsubscribe mechanisms must use an "opt-in" mechanism rather than an "opt-out" mechanism. This means that the default setting on subscription choices must be "no", requiring the recipient of the CEM to proactively click a checkbox to consent to receiving communications , or enter an email address and click a "submit" button. The CRTC has also stated that a confirming email should be sent on receipt of an express consent.

Requests for consent to receive CEMs must be made separately from the general terms and conditions of a sale or use of a product. This means that a user must be able to consent to the terms of sale or use when making a purchase but refuse his or her consent to receiving further CEMs.

Under CASL, certain types of commercial messages are exempt from the consent requirement: e.g., those providing quotations or information about previously completed transactions, messages completing or confirming transactions and messages related to an employment relationship. The revised draft Industry Canada regulations provide several additional exceptions for business communications that do not represent the types of threats that CASL was intended to address. The following types of messages would not be subject to the requirement to obtain the recipient's advance consent:

- CEMs sent between businesses that already have a business relationship, if the message is sent by an employee or other representative and is relevant to the recipient's business, function or duties;
- CEMs sent in response to a request, complaint or inquiry (presumably because consent can be clearly implied under those circumstances);
- CEMs sent because of a legal obligation or to enforce a legal right;
- CEMs from organizations outside Canada that are accessed while the recipient was only visiting here.

Messages sent to someone with whom the sender has a personal or family relationship are also exempt, but the precise definitions of such relationships will not be known until the final Industry Canada regulations are filed. The revised draft regulations define family relationship narrowly to include only relatives connected by blood, marriage, common-law partnership or adoption.

A personal relationship is defined in the revised draft regulations as one in which the sender and receiver have previously had direct, voluntary, two-way communications and it would be reasonable to conclude that the relationship is personal considering a number of factors such as sharing of interests, opinions and information and the length of time since the parties have communicated. This definition has been significantly revised from the previous version, which defined a personal relationship as one in which the parties had met face-to-face within the past two years. The change is intended to permit "virtual relationships" such as Facebook friends, and reflects stakeholder concerns that the previous definition was too narrow.

Penalties and Problems

CASL gives the government broad investigative and administrative powers and imposes substantial penalties for breaches of the rules: up to $100,000 for a first offence by a corporation and $250,000 for a second ($10,000 and $25,000 for offences by an individual), with maximum penalties of $1,000,000 for individuals and $10,000,000 for corporations. Directors of a corporation may be held personally liable for violations of CASL, unless a director can successfully prove a due diligence defence. CASL provides individuals with a private right of action against those engaging in, for example, spamming and hacking and installing malware and spyware. CASL also permits government officials to order third parties (such as internet service providers) to produce or preserve documents as evidence for investigations or complaints made under the new legislation.

Given the severity of these administrative penalties, and the

onerous technical requirements of complying with the CRTC's new guidelines on unsubscribe mechanisms, a number of large and small Canadian businesses and business advisors have expressed concerns about how CASL will dramatically impair their ability to communicate electronically with customers. The CRTC content regulation, for example, effectively requires all messages, even texts, to contain a link to a website on which recipients can unsubscribe from further messages. This means that, once CASL takes effect, even very small and home-based businesses will have to have set-up a fairly sophisticated website before they can send a sales message. Requiring an audio recording for oral consents is also impracticable for small businesses and for many retailers who obtain consent at the point of sale.

Another potentially burdensome requirement imposed by the CRTC guidelines is the confirming email which must be sent when the recipient of a CEM provides his or her express consent to receiving further messages. Confirmation is not required by CASL or the CRTC regulation and many consumers may be irritated at receiving these additional emails.

If you need help with preparing for CASL, reviewing your existing and proposed practices with respect to electronic communications or delivering staff training, the members of our Privacy Practice Group would be pleased to assist you.

The authors would like to thank Steven Pordage, Student-at-Law, for his assistance in preparing this bulletin.

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 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* and the *Municipal Freedom of Information and Protection of Privacy Act*.

Contact Members of the Privacy Law Group

Greg Azeff gazeff@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 264

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

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

Helen Ferrigan hferrigan@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 211

Greg Azeff is a member of the Privacy Law Group.

Andy Balaura is a member of the Privacy Law Group.

Joe Conte is a member of the Privacy Law Group.

Helen Ferrigan is a member of the Privacy Law Group.