CLARK WILSON LLP

Canada's New Anti-Spam Legislation

by

Maggie Cavallin
Clark Wilson LLP
T. 604.891.7748
mac@cwilson.com

CLARK WILSON LLP
Barristers & Solicitors
Patent & Trade-Mark Agents
900 – 885 West Georgia Street
Vancouver, BC V6C 3H1 Canada
T. 604.687.5700 **F.** 604.687.6314
cwilson.com

TABLE OF CONTENTS

Maggie Cavallin, T. 604.891.7748

CLARK WILSON LLP

Canada's New Anti-Spam Legislation

1. CASL OVERVIEW

With the release of the finalized *Electronic Commerce Protection Regulations* by the Canadian Radio-Television and Telecommunications Commission (the "CRTC") last spring, and the publication of a revised draft version of Industry Canada's *Electronic Commerce Protection Regulations* on January 5, 2013, it seems likely that Canada's new Anti-Spam legislation, "*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*", or "CASL" as it is more commonly known, will enter into force sometime in late 2013 or early 2014. CASL seeks to create a more secure online environment as a means of increasing consumer confidence in electronic commerce.

In general terms, CASL will prohibit:

- sending commercial electronic messages ("CEMs"), without a recipient's consent, including CEMs sent to email addresses and social networking accounts, such as Facebook, Twitter or LinkedIn, and text messages sent to cellular phones and other mobile devices;

- altering transmission data in electronic messages which results in messages being delivered to different or additional destinations without express consent;

- installing computer programs (such as spyware and malware, in addition to computer programs with a legitimate business purpose) without the express consent of the owner of the computer or an authorized user;

- using false or misleading representations online (including websites) in the promotion of products or services; and

- collecting electronic addresses by the use of computer programs or the use of such addresses without consent (address harvesting, scraping and hacking).

Because the scope of the new legislation is far reaching and the express consent regime imposed under CASL applies to virtually *all* emails and other electronic messages that are sent for a commercial purpose, subject to limited exceptions, it is advisable that companies and individuals begin to review and carefully consider their current email marketing practices now, and in many instances obtain "fresh" consents to qualify their email and customer lists, to ensure that they are CASL-compliant prior to the coming into force of this new legislation.

This paper is intended to provide an overview of the main requirements, scope and penalties imposed under CASL and provides a number of tips to help ensure that you and your company remain compliant.

Maggie Cavallin, T. 604.891.7748

2. CONSENT

CASL is primarily a permission-based or "opt-in" regime, under which prior express consent must be obtained from a recipient before a CEM may be delivered, before transmission data may be altered and before a computer program may be installed. While there are a number of exceptions under which consent may be implied or is simply not required, the default position under the Act is that consent must be obtained before taking any action which would otherwise be prohibited. Because any person alleging to have obtained consent bears the evidentiary burden of proving such consent,[1] it will be important for all companies to implement clear policies that provide for the proper documentation of consent and frequent and ongoing updating of customer and email lists.

2.1 Express Consent

Where express consent is required, a person seeking such consent must set out "clearly and simply" the purpose or purposes for which consent is being sought, information identifying the person seeking consent (and if the consent is being sought on behalf of another person, prescribed information that identifies that other person), and any other information prescribed by the Act or its Regulations.[2]

The finalized *Electronic Commerce Protection Regulations (CRTC)*, SOR/2012-36, released by the CRTC (the "CRTC Regulations") provide further guidance in this regard and state that consent may be obtained orally or in writing and that separate consents must be obtained for each of the sending of CEMs, the alteration of transmission data and the installation of computer programs. Consent in writing includes both paper and electronic forms of writing. When seeking consent, individuals and other entities must provide recipients with the following information:[3]

- the name by which the person seeking consent carries on business (if different from the person's own name);
- if consent is being sought on behalf of another person, the name by which the person on whose behalf consent is sought carries on business, if different from their own name, if not, the name of the person on whose behalf consent is sought;[4]
- if consent is sought on behalf of another person, a statement indicating which person is seeking consent and which person is the person on whose behalf consent is sought;

[1] Section 13, CASL.
[2] Section 10, CASL.
[3] Section 4, CRTC Regulations.
[4] Under CASL, a person may obtain express consent to send CEMs on behalf of a person whose identity is not known, provided that certain requirements are adhered to. Once such consent has been obtained, the authorized third party may send CEMs to the person from whom consent was obtained, provided that such consent is used in accordance with the terms and conditions set out in CASL and the IC Regulations (see Subsection 10(2), CASL and Section 5, IC Regulations).

Maggie Cavallin, T. 604.891.7748

- the mailing address and either a telephone number (providing access to an agent or a voice messaging system), an email address or a web address of the person seeking consent, and if different, the person on whose behalf consent is being sought; and

- a statement indicating that the person whose consent is sought can withdraw their consent.

Since the release of its finalized Regulations on March 28, 2012, CRTC has provided further clarification and information in relation to the above requirements by way of Compliance and Enforcement Information Bulletin CRTC 2012-548 ("CRTC 2012-548") and Compliance and Enforcement Information Bulletin CRTC 2012-549 ("CRTC 2012-549"). For example, CRTC 2012-548 advises that requests for consent must be clearly identified as such to the persons from whom consent is sought and must not be "subsumed in, or bundled with, requests for consent to general terms and conditions of use or sale."[5] Furthermore, because CASL imposes an opt-in regime, where express consent is obtained electronically, it must consist of a "positive or explicit indication of consent"[6] rather than a default toggling state that assumes consent (i.e. an already checked tick-box or pre-selected icon on a web page). As is noted in CRTC 2012-549, a "default toggle state assumes consent" and puts the responsibility of un-checking the box or de-selecting the icon on the person from whom consent is sought (i.e. is effectively an opt-out mechanism). Under CASL, such a mechanism cannot be used as a means of obtaining express consent for the purposes of sending CEMs, altering transmission data and installing computer programs in the course of a commercial activity.[7]

As will be discussed below, there are additional disclosure requirements where express consent is sought in relation to the installation of computer programs, which requirements may vary depending on the functions to be performed by the computer programs. In addition, as discussed below, there are a number of other circumstances, such as software updates and upgrades, when consent is deemed to have been obtained.

2.2 Implied Consent

CASL provides for a number of circumstances in which the consent to send CEMs may be implied and consequently, express consent is not required. Implied consent may exist in the following circumstances:

(a) where there is an "existing business relationship"[8] between the sender and the recipient. Under CASL, an existing business relationship may include:[9]

[5] Canadian Radio-television and Telecommunications Commission, *Compliance and Enforcement Information Bulletin CRTC 2012-548* (October 10, 2012).
[6] Canadian Radio-television and Telecommunications Commission, *Compliance and Enforcement Information Bulletin CRTC 2012-549* (October 10, 2012).
[7] *CRTC 2012-549*, paras. 4, 6 and 7.
[8] Interestingly, where the seller of a business has an existing business relationship with a recipient, the purchaser acquiring the business is considered to have an existing business relationship with the recipient in respect of the acquired business (Section 10(12), CASL).
[9] Section 10(10), CASL.

Maggie Cavallin, T. 604.891.7748

(i) a relationship arising from the purchase, lease or barter of a product, goods, a service, land or an interest or right in land, *within the previous two-year period*;

(ii) a relationship arising from the acceptance by the recipient of a business, investment or gaming opportunity offered by the sender;

(iii) a relationship arising from an inquiry or application made by the recipient, *within the previous six-month period*, in respect of (i) or (ii) above; or

(iv) a written contract between the recipient and the sender, whether the contract is still in existence or has expired, *within the previous two-year period*;

(b) where there is an "existing non-business relationship"[10] between the sender and the recipient, which may include:

(i) a relationship arising as a result of a donation, gift or volunteer work, by the recipient to a registered charity, a political party or organization or candidate, *within the previous two-year period*; or

(ii) a relationship arising out of the recipient's membership in a club, association, or voluntary organization *in the previous two-year period*. The revised draft Industry Canada *Electronic Commerce Protection Regulations* (the "IC Regulations") describe "membership" as "the status of having been accepted as a member" and provide that a club, association or voluntary organization "is a non-profit organization that is organized and operated exclusively for social welfare, civic improvement, pleasure or recreation or for any other purpose other than profit, if no part of its income is payable to, or otherwise available for the personal benefit of any proprietor, member or shareholder of that organization unless the proprietor, member or shareholder is an organization whose primary purpose is the promotion of amateur athletics in Canada";[11]

(c) where the recipient has "conspicuously published" their email contact information and such publication is not accompanied by a statement that they do not wish to receive unsolicited CEMs at the address *and* the message is relevant to the person's business, role, function or duties in a business or official capacity;[12] or

(d) where the recipient has disclosed his or her email address to the sender, without indicating that he or she does not wish to receive unsolicited CEMs *and* the message is relevant to the person's business, role, function or duties in a business or official capacity.[13]

[10] Section 10(13), CASL.
[11] Subsections 7(1) and (2), IC Regulations.
[12] Section 10(9)(b), CASL.
[13] Section 10(9)(c), CASL.

Maggie Cavallin, T. 604.891.7748

When relying on implied consent in the context of existing business and non-business relationships, it is important to be aware of the dates on which such relationships arose, since implied consent will expire after the time periods set out above (i.e. within two years or six months, as the case may be) if express consent is not obtained during this period of time.

2.3 Exceptions to Consent Requirement

In addition to the circumstances in which consent may be implied, CASL also provides a number of exceptions when express consent is not required prior to the sending of CEMs. Such exceptions include:

(a) where there is an existing personal or family relationship between the sender (or the person on whose behalf the electronic message is sent) and the recipient. The scope of the exception for "family relationships" and "personal relationships" is defined in the IC Regulations. Pursuant to the IC Regulations, "family relationship" is defined as including individuals who are connected by a blood relationship, marriage, common-law partnership and adoption. The definition of "personal relationship" was amended and broadened in the IC Regulations and is now defined as:

> "(b) 'personal relationship' means the relationship between an individual who sends the message and the individual to whom the message is sent, if:
>
> (i) those two individuals have had direct, voluntary, two-way communications and it would be reasonable to conclude that the relationship is personal taking into consideration all relevant factors such as sharing of interests, experiences, opinions and information evidenced in the communications, the frequency of communication, the length of time since the parties communicated and if the parties have met in person, and
>
> (ii) the person to whom the message is sent has not indicated that they no longer wish to receive any commercial electronic messages, or any specified class of such messages from the person who sent the message."[14]

(b) where the electronic message is sent to a person who is engaged in a commercial activity and consists solely of an inquiry or application related to that activity;

(c) where the electronic message provides only a quote or estimate that was requested by the recipient;

(d) where the electronic message facilitates, completes or confirms a pre-existing commercial transaction between the sender and the recipient;

(e) where the electronic message provides warranty, product recall, safety or security information about a product, goods or a service that the recipient uses, has used or has already purchased;

[14] Subsection 2(b), IC Regulations.

Maggie Cavallin, T. 604.891.7748

(f) where the electronic message provides notice of factual information regarding an ongoing subscription, membership, account, loan or similar relationship between the sender and the recipient;

(g) where the electronic message provides information directly related to an employment relationship or related benefit plan;

(h) where the electronic message delivers a product, good or service, including product updates or upgrades, that the recipient is entitled to receive under the terms of a pre-existing transaction with the sender;

(i) where the electronic message is the first CEM sent to an individual on a third-party referral basis, provided that: (1) the individual sending the CEM has an existing business relationship, an existing non-business relationship, a personal relationship or a family relationship with the individual providing the referral, and (2) the individual to whom the CEM is sent has an existing business relationship, an existing non-business relationship, a personal relationship or a family relationship with the individual providing the referral, and (3) the individual sending the CEM discloses the full name of the individual or individuals who made the referral and the CEM states that the message is being sent as a result of a referral;[15] and

(j) where the electronic message communicates for a purpose specified in the Regulations.

In addition to the above, the IC Regulations exempt certain CEMs from application of the anti-spam requirements of CASL. Specifically, such exemption applies to CEMs that are sent:

- by an employee, representative, contractor or franchisee of an organization to another employee, representative, contractor or franchisee of the organization that concerns the affairs of the organization (i.e. intra-business CEMs);

- by an employee, representative, contractor or franchisee of an organization to an employee, representative, contractor or franchisee of another organization if the organizations have a business relationship at the time the CEM is sent and the CEM concerns the affairs of the organization or that person's role, functions or duties within or on behalf of the organization (i.e. inter-business CEMs);

- in response to a request, inquiry or complaint of an individual, or that are otherwise solicited by the person to whom the CEM is sent;

- or caused or permitted to be sent by a person located outside Canada or that are sent from a computer system located outside Canada *and* that relate to a product, good, service or organization located or provided outside Canada that are accessed using a computer system in Canada *if* the person sending the CEM did not know and could not reasonably be expected to know that the message would be accessed by a computer system located in Canada; or

[15] Section 4(1), IC Regulations.

Maggie Cavallin, T. 604.891.7748

- to satisfy a legal or juridical obligation, provide notice of or enforce a right, legal or juridical obligation, court order, judgment or tariff, or enforce a right arising under a law of Canada, of a province or municipality of Canada or of a foreign state.

3. FORMAL REQUIREMENTS FOR UNSOLICITED COMMERCIAL ELECTRONIC MESSAGES

In addition to obtaining the prior consent of a recipient, CASL also requires that that senders of CEMs comply with a number of other formalities.[16] For example, all CEMs which are sent must provide the following prescribed information identifying the sender:[17]

- the name by which the person sending the CEM carries on business (if different from that person's name);

- if the CEM is sent on behalf of another person, the name by which the person on whose behalf the CEM is sent carries on business, if different, and if not, the name of the person on whose behalf the message is sent;

- if the CEM is sent on behalf of another person, a statement indicating which person is sending the CEM and which person is the person on whose behalf the message is sent (note that if a CEM is sent on behalf of multiple persons (i.e. affiliates) all such persons must be identified in the CEM)[18]; and

- the mailing address and either a telephone number (which provides access to an agent or voice messaging system), an email address or a web address of the sender, and if different, the person on whose behalf the CEM was sent.

In addition to the above prescribed information, CASL further requires that all CEMs provide a functioning "unsubscribe mechanism" that allows recipients to indicate that they no longer wish to receive CEMs from the sender.[19] The unsubscribe mechanism must utilize the same electronic means by which the CEM was originally sent, must be capable of being "readily performed" and must function at no cost to the recipients. Where it is not practicable to include the prescribed information and the unsubscribe mechanism in the body of a CEM, the CRTC Regulations state that this information and the unsubscribe mechanism may be posted on a web page that is readily accessible by means of a link that is "clearly and prominently set out" in the CEM.

CRTC advises in CRTC 2012-548 that the unsubscribe mechanism must be consumer-friendly, accessible without difficulty or delay and quick and simple for consumers to use.[20] Such a mechanism may include a link in an email that directs the user to a web page where the user can unsubscribe from receiving some or all types of CEMs, or in the circumstances of a text

[16] Section 6(2), CASL.
[17] Section 2(1), CRTC Regulations.
[18] *CRTC 2012-548*, para. 7
[19] Section 11(1), CASL; Sections 2(2) and 3(1) CRTC Regulations.
[20] *CRTC 2012-548*, para. 11.

Maggie Cavallin, T. 604.891.7748

message received on a cellular phone (SMS), it may consist of providing the user with the option to reply to the text message with the word "stop" or "unsubscribe."[21]

Under CASL, a sender must ensure that the electronic address or website link being provided in a CEM remains valid for a *minimum of 60 days* after each CEM is sent. Where a recipient has expressed a wish to unsubscribe, the sender must give effect to this request without delay, and in any event, *not later than ten business days* after the request is sent.[22]

4. WHAT IS A CEM?

Under the Act, "Commercial Electronic Message"[23] is defined broadly as:

> …an ***electronic message*** that, having regard to the **content of the message**, the **hyperlinks** in the message to content on a website or other database, **or the contact information** contained in the message, **it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a *commercial activity***, including an electronic message that
>
> (a) offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land;
>
> (b) offers to provide a business, investment or gaming opportunity;
>
> (c) advertises or promotes anything referred to in paragraph (a) or (b); or
>
> (d) promotes a person, including the public image of a person, as being a person who does anything referred to in any of paragraphs (a) to (c), or who intends to do so. [Emphasis added]

Consequently, under CASL an electronic message that does not contain any information of a commercial character but which contains a hyperlink to a website that, it would be reasonable to conclude, has the promotion of a commercial activity as *one* of its purposes, would constitute a CEM. In addition to electronic messages that have a commercial purpose, under CASL, an electronic message that contains a request for a recipient's consent to send a CEM is also considered to be a CEM, which further demonstrates the breadth of electronic messages which fall within the scope of the definition of CEM.[24]

"Commercial activity"[25] is defined in a similarly all-encompassing manner and includes "any particular transaction, act or conduct or any regular course of conduct *that is of a commercial character, whether or not the person who carries it out does so in the expectation of profit*…" [Emphasis added]. Accordingly, such activities as contest offers, offers to purchase goods or services, advertising or promotional activities and offers of business and investment opportunities likely fall within the purview of this definition. In its Regulatory Impact Analysis Statement, issued on January 5, 2013, Industry Canada provided further guidance in relation to the scope of the Act, stating that the definition of CEM "is limited in the Act to a message that

[21] *CRTC 2012-548*, para. 12.
[22] Sections 11(2) and (3), CASL.
[23] Section 1(2), CASL.
[24] Section 1(3), CASL.
[25] Section 1(1), CASL.

Maggie Cavallin, T. 604.891.7748

encourages participation in a commercial activity. To the extent that a message is sent in a commercial context but does not fall within the definition of a commercial electronic message provided in CASL, it is not a commercial electronic message for the purposes of the Act." Accordingly, messages such as notifications of successful unsubscribes or courtesy SMS messages sent to roaming customers would not constitute CEMs. In addition, the Regulatory Impact Analysis Statement notes, "[c]urrently, where they are not sent to electronic addresses, the publication of blog posts or other publications on microblogging and social media sites is not within the intended scope of the Act."[26]

It is important to note that "electronic message" and "electronic address"[27] are also defined expansively and in a technology-neutral manner, so as to apply to any means of telecommunication, including text, sound, voice or image messages which are sent via an email account, a social networking account, an instant messaging account, a telephone or similar account.

5. ALTERATION AND REDIRECTION OF ELECTRONIC MESSAGES ("HACKING" AND "PHISHING")

Section 7 of CASL prohibits the alteration of the transmission data contained in an electronic message which results in the delivery of a message to a destination other than or in addition to, the destination that was intended by the sender. This process of interception and rerouting of data is frequently used in "phishing" scams, in which confidential information (such as online banking information and passwords) is sought or where internet users are re-directed to fraudulent websites so that personal information may be obtained directly. CASL seeks to prevent such activities by broadly prohibiting the alteration of transmission data.

An exception to this prohibition exists where the sender or recipient has provided express consent or where the alteration is made in accordance with a court order.[28] Under CASL, any person who alters transmission data with the express consent of either the sender or recipient of the electronic message must ensure that the person providing consent is given an electronic address to send notice of any withdrawal of consent. Where consent is withdrawn it must be carried out *within ten business days* of having received notice of the withdrawal.[29]

Telecommunications service providers are exempted from section 7 where alterations made are for network management purposes.[30] It is important to note that a person contravenes this section only if a computer system located in Canada is used to send or access the electronic message.[31]

---

[26] Industry Canada, Electronic Commerce Protection Regulations, Regulatory Impact Analysis Statement at page 6 "Issues to be addressed in compliance guidelines".
[27] Section 1(1), CASL.
[28] Section 7(1)(a) and (b), CASL.
[29] Section 11(4), CASL.
[30] Section 7(2), CASL.
[31] Section 12(2), CASL.

Maggie Cavallin, T. 604.891.7748

6. INSTALLATION OF COMPUTER PROGRAMS

Section 8 of CASL prohibits the installation of a computer program on another person's computer system as well as causing an electronic message to be sent from a computer system where a computer program has previously been installed, without the express consent of the owner or an authorized user of the computer system or court order. Because CASL does not distinguish between spyware, malicious software and software used for legitimate business purposes, the installation of *all* software must be in compliance with CASL and its Regulations.

A person seeking express consent to install a computer program must comply with the same formality requirements as in other circumstances (described above under the heading "Express Consent"), as well as additional requirements. For example, when seeking consent to install a computer program, the person seeking consent must "clearly and simply" describe the function and purpose of the computer program.[32] In the event that the computer program to be installed performs one or more of the following functions:

(a) collecting personal information stored on the computer system;

(b) interfering with the owner's or authorized user's control of the computer system;

(c) changing or interfering with settings, preferences or commands already installed or stored on the computer system without the knowledge of the owner or authorized user;

(d) changing or interfering with data that is stored on the computer system in a manner that obstructs, interrupts or interferes with lawful access to or use of that data by the owner or authorized user;

(e) causing the computer system to communicate with another computer system or device, without authorization;

(f) installing a computer program that may be activated by a third party without the knowledge of the owner or authorized user; or

(g) performing any other function specified by the regulations,

the person seeking express consent must "clearly and prominently, and separately and apart from the licence agreement" describe the computer program's material elements that perform such functions, including the nature and purpose of those elements and the reasonably foreseeable impact that such functions may have on the operation of the computer system.[33]

The CRTC Regulations provide additional guidance in this regard and require that the material elements that perform these functions be brought to the attention of the person from whom consent is sought and furthermore, that the person seeking consent must obtain an acknowledgement in writing from the person providing consent which states that he or she

[32] Section 10(3), CASL.
[33] Section 10(4) and (5), CASL.

Maggie Cavallin, T. 604.891.7748

understands and agrees that the program performs the specified functions.[34] Compliance and Enforcement Information Bulletin CRTC 2012-548 states that "in writing" in this context includes both paper and electronic forms of writing.[35]

A person who has obtained the express consent of an owner or authorized user must ensure that *for a period of one year* (commencing at the time the computer program begins performing any of the functions noted above), the owner or authorized user is provided with an electronic address to which a request to remove or disable the computer program may be sent. If an owner or authorized user believes that the program was inaccurately described at the time their consent was obtained, the user must be provided with assistance to remove or disable the computer program, at no cost to the user.[36]

6.1 Deemed Consent for Installation of Computer Programs

As noted above, there are several circumstances in which consent is deemed to have been obtained or is simply not required. Further consent is not required where a person that has expressly consented to the installation of a computer program is entitled to receive updates or upgrades as they become available, so long as such updates or upgrades are installed in accordance with the terms of the original express consent.[37]

Express consent is deemed to have been obtained in relation to the installation of a computer program if the computer program is a cookie, HTML code, Java Script, an operating system, any other program that is executable only through the use of another computer program whose installation or use the person has previously consented to, or any other program specified in the Regulations.[38] Pursuant to section 6 of the IC Regulations, express consent is also deemed to have been obtained in relation to the installation of computer programs by or on behalf of telecommunications service providers, if such programs are installed solely to prevent activities that the telecommunications service provider reasonably believes contravene an Act of Parliament and which present an imminent risk of security to the telecommunications service provider's network, or programs that are installed for the purpose of upgrading or updating the network.[39] To fall within these exceptions, it must be reasonable to believe that the owner or authorized user of the computer system would consent to the installation of such programs.

7. AMENDMENTS TO OTHER LEGISLATION

In addition to imposing this new legislative regime, CASL also amends a number of statutes, including the Personal Information Protection and Electronic Documents Act ("PIPEDA"), the Competition Act, the Canadian Radio-Television and Telecommunications Act and the Telecommunications Act.

---

[34] Section 5(1), CRTC Regulations.
[35] *CRTC 2012-548*, para. 30
[36] Section 11(5)(b), CASL.
[37] Section 10(7), CASL.
[38] Section 10(8), CASL.
[39] Section 6, IC Regulations.

Maggie Cavallin, T. 604.891.7748

7.1 PIPEDA

The stated purpose of *PIPEDA*, a federal statute, is to establish rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of private sector organizations to collect, use or disclose personal information. CASL amends *PIPEDA* to prevent the unauthorized collection and use of electronic addresses or personal information using computer programs that are designed to collect such information (i.e. address harvesting in which "web crawlers" locate and collect electronic addresses or "dictionary attacks" in which computer programs generate thousands of variations for valid email domains).

Under *PIPEDA*, the knowledge and consent of an individual whose personal information is being sought is required for the collection, use or disclosure of such personal information, *except where inappropriate*.[40] Clause 4.3 of Schedule 1 and section 7 of *PIPEDA* set out a number of exceptions under which organizations may collect, use or disclose personal information without the knowledge or consent of an individual.

The amendment to *PIPEDA* made under *CASL* (which adds a new section 7.1 to *PIPEDA*) provides that such exceptions *do not apply* in respect of the collection or use of an individual's electronic address, if the address is collected by the use of a computer program that is designed or marketed primarily for use in generating or searching for, and collecting, electronic addresses.[41] *PIPEDA* is further amended such that the exceptions *do not apply* in respect of the collection or use of personal information, through any means of telecommunication, if the collection is made by accessing a computer system or causing a computer system to be accessed in contravention of an Act of Parliament.[42]

7.2 Competition Act

The *Competition Act* is federal legislation which seeks to maintain and encourage competition in Canada and thereby promote the efficiency and adaptability of the Canadian economy. In furtherance of these purposes, the *Competition Act* regulates a variety of commercial activities, including corporate mergers and acquisitions, deceptive marketing practices, and false and misleading representations.

Amendments made to the *Competition Act* under CASL address false and misleading representations contained in three different parts of an electronic message: (1) sender information or subject matter information; (2) content of the electronic message; and (3) locator. These components are defined in the amended section 2(1) of the *Competition Act* as follows:[43]

> "electronic message" means a message sent by any means of telecommunication, including a text, sound, voice or image message;

[40] Schedule 1, Clause 4.3, *PIPEDA*.
[41] Section 82(2), CASL.
[42] Section 82(3), CASL.
[43] Section 70(2), CASL.

Maggie Cavallin, T. 604.891.7748

> "locator" means a name or information used to identify a source of data on a computer system, and includes a URL;
>
> "sender information" means the part of an electronic message – including the data relating to source, routing, addressing or signalling – that identifies or purports to identify the sender or the origin of the message;
>
> "subject matter information" means the part of an electronic message that purports to summarize the contents of the message or to give an indication of them;

The CASL amendment adds section 52.01 to the *Competition Act*, which creates three separate criminal offences to address the sending of a false or misleading representation, whether knowingly or recklessly, when such representation is made to "promot[e], directly or indirectly, any business interest or the supply or use of a product."[44] These new provisions prohibit the use of false or misleading representations in sender information, subject matter information and locater. With respect to the content of electronic messages, the CASL-amended *Competition Act* prohibits any person from knowingly or recklessly sending (or causing to be sent) an electronic message that is false or misleading *in a material respect*, if the direct or indirect purpose of the electronic message is to promote any business interest or supply or use of a product.

For the purposes of section 52.01, an electronic message is considered to have been sent once transmission of the message has been initiated. Accordingly, it does not matter if the electronic message is actually delivered to its intended destination or if the electronic message is sent to an electronic address that does not exist.[45] It is important to note that section 52.01 applies to the person making or sending the representation, as well as anyone who permits the representation to be made or sent,[46] and further, that in establishing that section 52.01 has been contravened, it is not necessary to establish that any person was actually deceived or misled.[47] Where a contravention of this section is alleged, a court will take into account the "general impression conveyed by a representation as well as its literal meaning".[48]

Another provision which the CASL amendment adds to the *Competition Act*, is section 74.011, which creates a civil/reviewable conduct regime for conduct that is substantively the same as that which is prohibited under section 52.01. For example, subsection 74.011(1) states: "a person engages in reviewable conduct who, for the purpose of promoting, directly or indirectly, any business interest or the supply of use of a product, sends or causes to be sent a false or misleading representation in the sender information or subject matter information of an electronic message". Subsections 74.011(2) and (3) are nearly identical to subsections 52.01(2) and (3), respectively.

---

[44] Section 75, CASL (amending Section 52.01 of the *Competition Act*).
[45] Section 75, CASL (amending Section 52.01(9), *Competition Act*).
[46] Section 52(1.2), *Competition Act*.
[47] Section 75, CASL (amending Section 52.01(4), *Competition Act*).
[48] Section 75, CASL (amending Section 52.01(5), *Competition Act*).

Maggie Cavallin, T. 604.891.7748

As is the case for section 52.01, section 74.011 applies to any person who makes or sends such a representation or permits a representation to be made or sent,[49] and liability may arise as soon as the transmission of an electronic message is commenced.[50] Furthermore, similar to section 52.01, in a proceeding under section 74.011, a court will consider the "general impression conveyed by a representation as well as its literal meaning… in determining whether or not the person who made the representation engaged in the reviewable conduct".[51]

8. SUPERVISION AND ENFORCEMENT

Failure to comply with CASL may result in severe penalties, including:

(a) Administrative monetary penalties imposed by the CRTC of up to $1 million (for individuals) and $10 million (for other entities) in respect of a contravention of the Act. Factors considered by the CRTC when determining the appropriate penalty include: the purpose of the penalty; the nature and scope of the violation; whether the person has a history of violations; any financial benefit the person obtained through the violation; the person's ability to pay; and any other relevant factor;[52]

(b) A private right of action for persons (individuals or corporations) that are affected by a contravention of the Act. Persons affected by acts or omissions that contravene CASL (such as spamming, hacking or installation of spyware, malware or another computer program), or CASL-amended *PIPEDA* (such as the unauthorized collection of personal information) and the *Competition Act* (such as the sending of false or misleading electronic messages) may apply to the courts for compensation. It is important to note that there is a three-year limitation period for bringing such actions.[53] Possible remedies include compensation in an amount equal to the loss or damage suffered, or expenses incurred by the applicant, with a maximum penalty of $200 for each contravention with respect to sending CEMs (not to exceed $1 million per day) and $1 million for each day on which a contravention occurs with respect to the alteration of transmission data or the installation of a computer program (hacking, malware and spyware);[54]

(c) Vicarious liability may result for employers where an employee contravenes CASL while acting within the scope of his or her employment. Furthermore, where corporations violate CASL, directors, officers, agents or mandatories of the corporation may be held personally liable if they directed, assented to, acquiesced or participated in the commission of the violation. In such circumstances, employers, directors and officers may be able to avoid liability if they are able to establish that they exercised due diligence in preventing the commission of the violation;[55] and

[49] Section 52(1.2), *Competition Act*.
[50] Section 74.011(5)(a), *Competition Act*.
[51] Section 77, CASL (amending Section 74.011(4), *Competition Act*).
[52] Section 20, CASL.
[53] Section 47(2), CASL.
[54] Section 51, CASL.
[55] Sections 31 to 33, CASL.

Maggie Cavallin, T. 604.891.7748

(d) The obstruction of an investigation under CASL, failure to comply with a demand to preserve transmission data and failure to produce documents when required, constitute criminal offences, punishable by summary conviction under the *Criminal Code*.[56]

9. TIPS FOR COMPLIANCE WITH CASL

Because of the broad scope of this new legislation and the potentially severe penalties that may be imposed, it is important for individuals and businesses to adjust their practices now to ensure that they are CASL compliant when the legislation comes into force. The following tips may assist in ensuring that you and your business remain in compliance of CASL:

1) Review and revise your marketing, advertising and external electronic mailing communication practices to ensure they comply with CASL and the CASL-amended *PIPEDA* and *Competition Act*;

2) Review and update your customer lists and document whether you have obtained express consent or if implied consent exists (noting when consent was obtained). Remove recipients who have not expressly consented to receiving CEMs and those whose implied consent has expired (i.e. after six months or two years, as the case may be). Obtain "fresh" consents, as applicable;

3) Review and update your customer email lists and databases frequently and implement procedures for recording consents that have been obtained (i.e. retain details and evidence of consent, such as the date, time, purpose and manner in which consent was obtained);

4) Do not use computer programs designed to generate, search for or collect electronic addresses;

5) Review and revise processes for obtaining express consent to send CEMs, including company newsletters, and installing software programs. Ensure prescribed information is provided when seeking express consent;

6) Where oral consent has been provided, such consent should be verifiable by an independent third party or a complete unedited audio recording of the consent should be retained;

7) Consent "in writing" includes both paper and electronic forms of writing (i.e. physically filling out a consent form or proactively checking a tick box or clicking an icon on a web page). Ensure that you maintain a database which includes the date, time, purpose and method of consent obtained;

8) Once express consent has been obtained, send an email message asking the recipient to confirm or activate his or her subscription so that consent is verified and documented;

[56] Sections 42, 43 and 46, CASL.

Maggie Cavallin, T. 604.891.7748

9) Ensure that all CEMs sent comply with all formalities required under CASL:

   (a) CEMs must include all prescribed information and clearly identify the sender and the name of the person or company on whose behalf a CEM is being sent (ensure that the sender information, subject line, locator and content of the CEM do not contain any misleading information),

   (b) CEMs must contain the sender's mailing address and either a telephone number (which provides access to an agent or voice messaging system), an email address or a web address of the sender and, if different, the person on whose behalf the CEM was sent (note that this information must remain active for at least 60 days after the CEM is transmitted so that recipients can contact the sender), and

   (c) CEMs must include a functional unsubscribe mechanism that is set out clearly and prominently in the body of the CEM or in a link to the website that allows a recipient to readily unsubscribe from receiving further CEMs at no cost to the recipient. Ensure that the mechanism is tested to ensure functionality each time that CEMs are sent out to those on your customer email lists;

10) Institute procedures and policies to ensure that CEMs sent are not misleading in any way (i.e. sender information, URL, subject line, and content);

11) When a recipient expresses a desire to unsubscribe and not receive further CEMs or withdraws express consent in relation to the installation of computer programs or alteration of transmission data, ensure that such a request is acted on without delay, and in any event, *within not more than ten business days*;

12) When seeking consent where software installation is concerned, provide the prescribed information and ensure that you provide information about the function and purpose of the software prior to its installation and have the recipient acknowledge in writing that he or she understands and agrees that the program performs these functions;

13) If the software to be installed performs one of the functions set out in section 10(5) of CASL (discussed above in Paragraph 6, Installation of Computer Programs), ensure that you also describe the material elements of the software (including its nature and purpose) and the foreseeable impact of such functions;

14) Ensure that separate consents are sought and obtained for the sending of CEMs, the alteration of transmission data and the installation of computer programs;

15) Implement due diligence practices to reduce the risk of liability for directors and officers; and

Maggie Cavallin, T. 604.891.7748

16) Establish policies and guidelines for employees to ensure compliance with CASL and its Regulations.

Acknowledgements

I would like to sincerely thank Larry Munn for his guidance and assistance in the preparation of this paper.

Maggie Cavallin, T. 604.891.7748