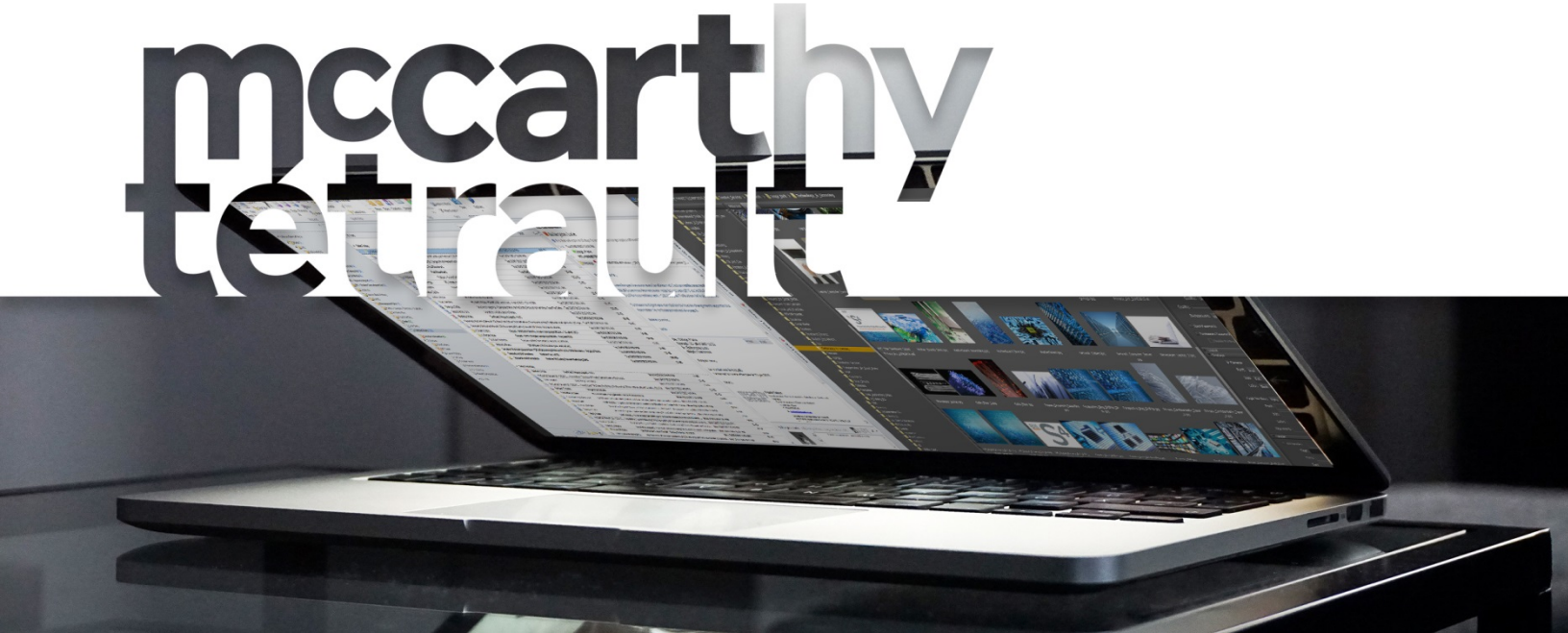
mccarthy tetrault

# Anti-Spam Toolkit

LAST UPDATED: FEBRUARY 2018



mccarthy tetrault

# Table of Contents

# Anti-Spam Toolkit

## Introduction

The purpose of this toolkit is to help organizations navigate Canada's anti-spam law. The anti-spam law does not have a formal shorthand name. The official name would take up the space of a long paragraph to print each time. For the sake of brevity, this toolkit will refer to the law by the commonly used name "Canada's Anti-Spam Legislation", or "CASL".[1]

Parliament passed CASL on December 15, 2010. Most of CASL is already in force. There is one exception: the private right of action. The coming into force of the private right of action provisions has been postponed indefinitely while a parliamentary committee reviews the legislation.[2]

CASL is arguably the toughest anti-spam/malware law in the world. In order to ensure compliance, organizations that send commercial electronic messages to Canadians will need to examine the way they electronically communicate. Those who violate CASL could face fines of up to $10 million.[3] Officers and directors are also exposed to personal liability if they authorize, acquiesce in or participate in offending conduct.

Although many organizations are familiar with the requirements of the US anti-spam law, the CAN SPAM Act of 2003, the Canadian law is more complicated and more onerous. In most cases, compliance with the US requirements will not be sufficient for Canadian purposes.

CASL's reach extends far beyond typical "spam" emails, and potentially applies to what most people consider ordinary electronic communications. As a result, organizations will need to carefully scrutinize their use of messages sent using email, SMS and other electronic messaging systems including certain messages sent using social networks and online portals. The simple act of sending an electronic message with any degree of commercial content to someone without prior consent presents significant risks for organizations.

CASL prohibits organizations from sending commercial electronic messages unless the recipient has given express consent or the message falls into one of the closed categories where consent is implied. A "commercial electronic message" is an electronic message that is sent to an electronic address which has as one of its purposes to encourage participation in commercial activity. The term "electronic message" is defined broadly to include any "message sent by any means of telecommunication, including a text, sound, voice or image message." An "electronic address" is an email account, an SMS account, an instant messaging account or any similar account.

CASL also requires that all commercial electronic messages identify the sender, include the sender's contact information, and provide an "unsubscribe" mechanism so that a recipient can opt out of receiving future communications. These requirements become more complicated in situations where service

---

1 The full text of CASL can be found at http://laws-lois.justice.gc.ca/eng/acts/E-1.6/index.html.

2 For more details, see Barry Sookman, CASL Private Right of Action delayed and Government to review CASL at http://www.canadiantechlawblog.com/2017/06/07/casl-private-right-of-action-delayed-and-government-to-review-casl/

3 The largest CASL-related penalties issued to date involved a Competition Bureau settlement against rental car companies for $3 million; on the side of commercial electronic messaging, the CRTC has issued notices of violation for amounts as high as $1.1 million.

providers or co-promoters are involved in creating the content of a message or deciding on the list of recipients.

CASL amends the *Competition Act* to prohibit false or misleading representations in the sender description, subject matter field or message field of an electronic message, or in the URL or other locater on a webpage. Senders will have to be particularly wary of making overly boastful or factually incomplete statements in subject matter lines in an attempt to catch readers' attention, as *any* misleading element can lead to significant liability.

The law also amended Canada's federal privacy legislation (the *Personal Information Protection and Electronic Documents Act* or "PIPEDA"). These amendments prohibit the use of computer programs known as "address harvesters" and extend to both the use of address harvesting programs and using electronic addresses that were obtained through the use of such programs. The latter prohibition creates issues for persons who have obtained or are using third-party address lists.

To combat spyware, malware and other malicious software, CASL prohibits the installation of computer programs without the consent of the computer's user or owner. However, the computer program provisions in CASL go beyond malicious software and have the potential of affecting routine computer program installations for innocuous purposes.

CASL creates a private right of action that allows a person to take civil actions against anyone who violates CASL or the new false or misleading representations provisions of the *Competition Act*. The potential remedies could amount to as much as $1 million per day per category of violation plus compensation for actual damages or losses. As mentioned above, while the private right of action is not yet in force, it could be resurrected pursuant to the government's review.

This toolkit provides basic guidance for organizations that communicate electronically and wish to address the requirements in CASL. Appendix A set out a list of information to gather for an audit. It also includes in Appendix B an audit checklist that covers the key points of compliance that organizations should consider and revisit on a regular basis.

This toolkit should not be taken as formal legal advice.

## ADDITIONAL RESOURCES AND GUIDANCE

Many of CASL's provisions are impacted by two sets of government regulations; one established by the CRTC and the other by Industry Canada. The CRTC published its final regulations in March 2012. Industry Canada published its final regulations in December 2013.[4] References in this toolkit to CRTC regulations refer to the final CRTC regulations. References in this toolkit to the IC regulations refer to the final regulations published in December 2013 by Industry Canada.[5]

In addition, the CRTC has published three compliance and enforcement information bulletins related to CASL:

[4] For a summary of the IC regulations see, Barry Sookman, CASL Industry Canada regulations: summary and comments at http://www.barrysookman.com/2013/12/04/casl-industry-canada-regulations-summary-and-comments/ and Barry Sookman, The Industry Canada CASL Regulations and RIAS: a Lost Opportunity at http://www.barrysookman.com/2013/12/16/the-industry-canada-casl-regulations-and-rias-a-lost-opportunity/

[5] The CRTC regulations can be found at http://www.crtc.gc.ca/eng/archive/2012/2012-183.htm, the IC regulations can be found at http://fightspam.gc.ca/eic/site/030.nsf/eng/00273.html and the Compliance Program Guideline can be found at http://crtc.gc.ca/eng/archive/2014/2014-326.htm

- CRTC 2012-548 Guidelines on the interpretation of the Electronic Commerce Protection Regulations (the "General Guideline")

- CRTC 2012-549 Guidelines on the use of toggling as a means of obtaining express consent under Canada's anti-spam legislation (the "Toggling Guideline")

- CRTC 2014-326 Guidelines to help businesses develop corporate compliance programs (the "Compliance Program Guideline")

The CRTC regulations prescribe the form of, and content to be included in, commercial electronic messages and requests for consent to send commercial electronic messages, to alter transmission data in electronic messages, and to install computer programs. The CTRC Guidelines focus on the CRTC's interpretation of the CRTC regulations and the related provisions of CASL and provide examples of what the CRTC considers to be compliant behavior.[6]

Aside from the legislation, regulations and compliance and enforcement information bulletins, the CRTC, Industry Canada and the Competition Bureau have provided guidance in a range of different forms (the "Additional Guidance Documents"), including:

- a regulatory impact analysis statement (the "RIAS"),[7] published by Industry Canada when the IC regulations came into force. The RIAS contains somewhat helpful explanations of key aspects of CASL and the regulations;

- the CRTC's frequently asked questions regarding CASL; (the "CRTC FAQs")[8]

- additional FAQs published on the fightspam.gc.ca website;[9]

- the Competition Bureau's FAQs;[10]

- a Video Transcript of the CRTC's information session on CASL;[11]

- the CRTC's information sheet *Canada's Anti-Spam Legislation Requirements for Installing Computer Programs* (the "Installing Computer Programs Guidelines");[12]

- the CRTC's *Enforcement Advisory - Notice for Businesses and Individuals on how to Keep Records of Consent*;[13] and

---

6 For a full analysis of the CRTC Guidelines see, Barry Sookman CRTC Issues CASL (Canada's Anti-Spam Law) Guidelines, background and commentary at http://www.barrysookman.com/2012/10/16/crtc-issues-casl-canadas-anti-spam-law-guidelines-background-and-commentary/

7 The RIAS can be found at http://fightspam.gc.ca/eic/site/030.nsf/eng/00271.html. For analysis and commentary regarding the RIAS see, Barry Sookman, The Industry Canada CASL Regulations and RIAS: a Lost Opportunity at http://www.barrysookman.com/2013/12/16/the-industry-canada-casl-regulations-and-rias-a-lost-opportunity/. For additional commentary on the FAQs see Barry Sookman, CRTC FAQ on CASL at http://www.barrysookman.com/2013/12/18/crtc-faq-on-casl/

8 The CRTC FAQs can be found at http://crtc.gc.ca/eng/com500/faq500.htm

9 The fightspam.gc.ca FAQs can be found at http://fightspam.gc.ca/eic/site/030.nsf/eng/00304.html

10 The Competition Bureau's FAQs can be found at http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03765.html

11 The transcript can be found at http://www.crtc.gc.ca/eng/com500/videot1.htm

12 The Installing Computer Programs Guidelines can be found at http://crtc.gc.ca/eng/internet/install.htm. We recommend that these Guidelines be assessed with care, as it adopts certain interpretations regarding installations that do not appear to be grounded in the language of CASL.

- the CRTC's guidance on implied consent ("Implied Consent Guidance").[14]

**IMPORTANT:** Guidance in the Additional Guidance Documents set out above may be taken into consideration when the CRTC or a court determines the appropriate remedy for violating CASL. These documents may also possibly be helpful in establishing due diligence defenses. The value of these documents, however, is subject to the significant caveat that a mistake of law, that is, a mistake as to what the law is, has been rejected as a defence to regulatory offenses. Therefore, organizations cannot merely rely on statements in the Additional Guidance Documents without making their own assessments that the guidance provided is right.[15]

**GUIDANCE FROM ENFORCEMENT DECISIONS:** While the CRTC has published a range of material regarding how it has enforced CASL to date, that material provides little additional guidance on future applications.[16] The CRTC has issued several notices of violation, which have tended to result in the accused party agreeing to an undertaking. So far, each of the undertakings has involved a monetary payment and a commitment to undertake a compliance program. In such cases, there is very little guidance as to the nature of the offence and the manner in which the CRTC has interpreted key ambiguous provisions of CASL. However, there have been at least three published decisions in which administrative monetary penalties (AMPs) have been issued.[17] These decisions provide some guidance as to how the CRTC interprets CASL and its regulations.

**NOTE ON ENFORCEMENT:** The CRTC is the authority primarily responsible for administration and enforcement of CASL. The Commissioner of Competition and the Privacy Commissioner of Canada is responsible for the administration and enforcement of the amendments made in CASL to the *Competition Act* and to PIPEDA. The Commissioner of Competition also has both civil and criminal enforcement responsibilities under CASL and the Competition Act. Each of the CRTC, the Commissioner of Competition and the Privacy Commissioner of Canada are obligated to consult with each other and have together entered into an MOU to "facilitate cooperation, coordination and information sharing" for purposes of administration and enforcement of CASL.[18]

---

[13] The enforcement advisory can be found at https://www.canada.ca/en/radio-television-telecommunications/news/2016/07/enforcement-advisory-notice-for-businesses-and-individuals-on-how-to-keep-records-of-consent.html

[14] The guidance on implied consent can be found at http://www.crtc.gc.ca/eng/com500/guide.htm

[15] See Barry Sookman, The Industry Canada CASL Regulations and RIAS: a Lost Opportunity at http://www.barrysookman.com/2013/12/16/the-industry-canada-casl-regulations-and-rias-a-lost-opportunity/

[16] For all current enforcement decisions, administrative monetary penalties, notices of violation and undertakings, see: http://www.crtc.gc.ca/eng/dncl/dnclce.htm

[17] See http://www.crtc.gc.ca/eng/archive/2017/2017-368.htm, https://www.crtc.gc.ca/eng/archive/2017/2017-65.htm, and https://www.crtc.gc.ca/eng/archive/2016/2016-428.htm

[18] See http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03643.html

# Sending Commercial Electronic Messages

The main focus of CASL's anti-spam provisions is to prevent Canadian "inboxes" from being filled with commercial electronic messages that are sent without consent and without compliance with the other formalities. This document provides an overview of CASL's main provisions. Representatives of organizations involved in sales, marketing or other external-facing roles should be made aware of and should pay particular attention to these requirements.

From an enforcement perspective, organizations must ensure that they take demonstrable efforts to address the consent and other formalities associated with CASL. The steps that an organization takes to prevent its employees and/or other representatives from sending unsolicited commercial messages can help to establish or bolster the due diligence defense and can factor in determining the amount of administrative monetary penalties (AMPs) or damage awards applicable in the event of a CASL breach. Accordingly, developing and implementing a CASL compliance program is essential for limiting an organization's liability and exposure to CASL.

## IS THE MESSAGE AN "ELECTRONIC MESSAGE"?

CASL applies to "electronic messages" sent to an "electronic address". The term "electronic message" is defined to mean a message sent by *any* means of telecommunication, including a text, sound, voice or image message. But, it excludes interactive two-way voice communication between individuals, fax messages to a telephone account, voice recordings to a telephone account.

The addresses covered by CASL are addresses "used in connection with the transmission of an electronic message to (a) an electronic mail account; (b) an instant messaging account; (c) a telephone account; or (d) *any similar account*." This includes many forms of electronic messaging systems such as email, SMS, instant-messaging, and some online services where users hold an account, including some social networking sites and certain online forums, and portals.

**NOTE**: The IC regulations established exemptions for messages sent to secure e-commerce portals and to certain messaging systems. For further details on these exemptions, see below under "Is the Message Subject to a Complete Exemption." In addition, the RIAS offers some guidance with respect to whether messages sent to Internet Protocol (IP) addresses or as part of behavioural advertising are sent to "electronic addresses". The RIAS states that "insofar as (IP) addresses are not linked to an identifiable person or to an account, IP addresses are not electronic addresses for the purposes of CASL. As a result, banner advertising on websites is not subject to CASL."

## IS THE MESSAGE A "CEM"?

CASL only applies to commercial electronic messages ("CEMs"). The law defines a commercial electronic message 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)

The term “commercial activity” is also very broadly defined as: “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*, other than any transaction, act or conduct that is carried out for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs of the defence of Canada.” (emphasis added)

In the Additional Guidance Documents, the CRTC and Industry Canada made statements intended to clarify the definition of CEM. While somewhat helpful, the explanations are sometimes contradictory and still leave open substantial questions about whether particular messages are CEMs. Further, the published enforcement decisions and CRTC undertakings summaries have fallen short of providing clarity on common questions of organizations trying to understand CASL.

The CRTC FAQs state:

> “A key question to ask yourself is the following: Is the message I am sending a CEM? Is one of the purposes to encourage the recipient to participate in commercial activity?
>
> When determining whether a purpose is to encourage participation in commercial activity, some parts of the message to look at are:
>
> - the content of the message
> - any hyperlinks in the message to website content or a database, and
> - contact information in the message.
>
> These parts of the message are not determinative.”

The RIAS states:

- “The mere fact that a message involves commercial activity, hyperlinks to a person's website, or business related electronic addressing information does not make it a CEM under the Act if none of its purposes is to encourage the recipient in additional commercial activity. If the message involves a pre-existing commercial relationship or activity and provides additional information, clarification or completes the transaction involving a commercial activity that is already underway, it would not be considered a CEM since, *rather than promoting commercial activity, it carries out that activity*.” (emphasis added)
- “Moreover, surveys, polling, newsletters, and messages soliciting charitable donations, political contributions, or other political activities that do not encourage participation in a commercial activity would not be included in the definition.”
- “However electronic messages may come within the definition of a CEM if it would be reasonable to conclude that one of the purposes is to encourage the recipient to engage in additional commercial activities, based on, for example, the prevalence and amount of commercial content, hyperlinks or contact information.”
- “To be clear, if the purpose or one of the purposes is to advertise, promote, market or otherwise offer a product, good, service, business or gaming opportunity or interest in land, these messages are clearly CEMs. Most notably, *the Act aims to limit the opportunity to advertise, market, promote, or otherwise offer products or services under the guise of a non-commercial electronic message.* If it is reasonable to conclude that the message has one of those purposes, then the message would be considered to be a

> CEM and, subject to exclusions, the requirements of the Act would apply."(emphasis added)

The written decision in Compliance and Enforcement Decision CRTC 2016-428 ("*Blackstone*")[19] explained that a message can still be a CEM without a clear offer of a purchase or sale:

> "The messages sent referred to and promoted educational and training programs in areas such as technical writing, grammar, and stress management. The cost of these programs was not specifically discussed; however, the nature of the language used, including references to various discounts and group rates, conveyed that these courses were services available for purchase from Blackstone. The Commission thus determines that the messages were sent for the purpose of advertising and promoting services commercially available from Blackstone, and were commercial electronic messages within the meaning of subsection 1(2) of the Act."

## IS THE MESSAGE SUBJECT TO A COMPLETE EXEMPTION?

CASL provides several complete exemptions from all of its provisions. These are:

1. Where sender and recipient have a personal or family relationship as established by the regulations (s.6(5)(a)); and
2. An inquiry or application related to a person engaged in a commercial activity. (s.6(5)(b)).

Nine additional exemptions are set out in the IC regulations. These exemptions, which are further described below, are:

1. Messages sent within an organization that concern the activities of that organization (IC Regs - 3(a)(i));
2. Messages sent between organizations with a relationship that concern the activities of the recipient organization (IC Regs - 3(a)(ii));
3. Messages sent in response to requests, inquiries or complaints (IC Regs - 3(b));
4. Messages sent in response to a legal or juridical obligation, including to provide notice of a pending right and to enforce a right (IC Regs - 3(c));
5. Messages sent on an electronic messaging service if (i) the required form, content and unsubscribe mechanism are available on the service's user interface, and (ii) the recipient has consented to receive such messages expressly or by implication. (IC Regs – 3(d));
6. Messages sent to a limited-access secure and confidential account to which messages can only be sent by the person who provides the account (IC Regs – 3(e));
7. Messages that (i) a sender reasonably believes will be accessed in a listed foreign state, and (ii) conform to the laws of such foreign state addressing conduct similar to CASL. (IC Regs – 3(f));
8. Messages sent by or on behalf of a registered charity as defined in s.248(1) of the ITA, and have as their primary purpose raising funds. (IC Regs – 3(g)); and

[19] See: http://www.crtc.gc.ca/eng/archive/2016/2016-428.htm

9. Messages sent by or on behalf of a political party or organization or a person who is a candidate for publicly elected office that has as its primary purpose soliciting a contribution. (IC Regs – 3(h)).

### *Business to Business*

There are two business to business exemptions:

The first is an exemption for messages sent within an organization by an employee, representative, consultant or franchisee to another employee, representative, consultant or franchisee of that organization and that concerns the activities of that organization.

The second is an exemption for messages sent by an employee, representative, franchisee or contractor of an organization to another employee, representative, franchisee or contractor from another organization, to the extent that the organizations "have a relationship" at the time the message was sent and the message concerns the activities of the recipient organization.

### *Messages Sent in Response to a Request*

Messages sent in response to requests, inquiries or complaints, or otherwise solicited by the recipient are exempt from CASL. This exemption fixes an unintended problem in s.6(5) of CASL which would have made it illegal to send consumers messages in response to a request for information without obtaining additional consent.

### *Messages Sent to Enforce a Legal Right*

The IC regulations exempt CEMs that are sent to a person (i) to satisfy a legal or juridical obligation, (ii) to provide notice of an existing or pending right, legal or juridical obligation, court order, judgment or tariff, (iii) to enforce a right, legal or juridical obligation, court order, judgment or tariff, or (iv) to enforce a right arising under a law of Canada, of a province or municipality of Canada or of a foreign state.

### *Messages Sent and Received on an Electronic Messaging Service*

Messages sent and received on an electronic messaging service are exempt so long as the form and content and unsubscribe requirements of CASL are *conspicuously published* and *readily available* on the user interface through which the messages are accessed and the recipient consents to receive the messages expressly "*or by implication*."

### *Messages Sent to E-Commerce Portals*

Messages sent "to a limited-access secure and confidential account to which messages can only be sent by the person who provides the account" are also exempt from CASL. The application of this exemption will allow banks, for example, to continue sending messages to users of online banking services, through accounts established by the bank and accessible through such services.

### *Messages "Reasonably Believed" to be Accessed in a Foreign State*

Messages that the sender reasonably believes will be accessed in a foreign state that is expressly listed in an annex to the regulations are exempt from CASL so long as that message conforms to the law of that state that addresses conduct similar to conduct prohibited under CASL. The effect of this regulation is to make senders of CEMs from Canada liable for violating CASL if the message sent to the foreign jurisdiction violates the applicable anti-spam law of the foreign jurisdiction.

### *Registered Charities and Political Parties, Organizations and Candidates*

Messages that are primarily fundraising solicitations by registered charities and by political parties, organizations and candidates are exempt from CASL. The exemptions apply only to registered charities under section 248(1) of the *Income Tax Act* and to political entities, leaving all other non-profits subject to the requirements of CASL.

The CRTC has provided some further guidance for charities, taking the position that it will only focus on charities where there is an attempt to subvert the law. The CRTC FAQs state that "[g]iven that legitimate messages sent by registered charities raising funds are exempt under the Act, the CRTC will focus on messages sent by those attempting to circumvent the rules under the guise of a registered charity."[20]

## HAS THE RECIPIENT CONSENTED TO THE MESSAGE?

The goal of CASL is to ensure that recipients of commercial electronic messages have consented to receiving such messages. The consent can be either express or implied. The requirements under CASL for express and implied consent, and exceptions to the consent requirements, are set out below. Obtaining consent is critical. In fact, the first three enforcement decisions that resulted in administrative monetary penalties involved a lack of recipient consent.

### *Express Consent*

The CRTC regulations state that a request for consent to send commercial electronic messages may be obtained orally or in writing. Although there is no requirement that the act of consent itself be in writing, organizations will invariably prefer to obtain the consent in writing in order to be able to prove the existence of the consent. The CRTC Guideline provides some guidance on the types of evidence it would consider sufficient to demonstrate oral consent. We have summarized its recommendations under "Obtaining Consent" below.

**NOTE**: An electronic message that requests consent to send a commercial electronic message is deemed to be a commercial electronic message. Thus any such requesting message must comply with appropriate consent requirements before it is sent unless it is subject to one of the exemptions from the consent requirement discussed below.

**COMPLIANCE NOTE**: Both the RIAS and the CRTC FAQs provide that express consents, obtained before CASL comes into force, to collect or to use electronic addresses to send commercial electronic messages will be recognized as being compliant with CASL even if the requests for consent did not include requisite form and content requirements under CASL (see below under "Obtaining Consent").[21] However, other consents such as those that would be compliant with PIPEDA will not be considered compliant with CASL, whether obtained before CASL came into force or after. Inferred consents that are recognized as valid in Australia are not express consents for the purposes of CASL.

### *Implied Consent*

CASL implies consent to send a commercial electronic message in three situations:

1. where there is an "*existing business relationship*" or an "*existing non-business relationship.*"
2. where the recipient has "*conspicuously published*" the electronic address without a statement that the person does not wish to receive unsolicited CEMs AND the message is relevant to the person's business, role, functions or duties in a business or official capacity; and
3. where the recipient has disclosed, to the person who sends the message, the electronic address without indicating a wish not to receive unsolicited CEMs, AND the message is relevant to the person's business, role, functions or duties in a business or official capacity.

---

[20] For a more detailed discussion of CASL and charities, see Meghan Waters, CASL Guidance for Registered Charities at https://www.mccarthy.ca/en/insights/blogs/snipits/casl-guidance-registered-charities

[21] The CRTC does not regard a consent obtained using a pre-checked box to be an express consent. See the Toggling Guidelines. Accordingly, there is uncertainty about whether these consents remain valid.

A person has "an existing business relationship" with a recipient if it arises from:

> (*a*) the purchase or lease of a product, goods, a service, land or an interest or right in land, within the two-year period immediately before the day on which the message was sent, by the person to whom the message is sent from any of those other persons;
>
> (*b*) the acceptance by the person to whom the message is sent, within the period referred to in paragraph (*a*), of a business, investment or gaming opportunity offered by any of those other persons;
>
> (*c*) the bartering of anything mentioned in paragraph (*a*) between the person to whom the message is sent and any of those other persons within the period referred to in that paragraph;
>
> (*d*) a written contract entered into between the person to whom the message is sent and any of those other persons in respect of a matter not referred to in any of paragraphs (*a*) to (*c*), if the contract is currently in existence or expired within the period referred to in paragraph (*a*); or
>
> (*e*) an inquiry or application, within the six-month period immediately before the day on which the message was sent, made by the person to whom the message is sent to any of those other persons, in respect of anything mentioned in any of paragraphs (*a*) to (*c*). (s.10(10)).

In relation to the purchase or lease of a product, goods, a service, land or an interest or right in land, if it involves an ongoing use or ongoing purchase under a subscription, account, loan or similar relationship, the period is considered to begin on the day that the subscription, account, loan or other relationship terminates. This effectively lengthens the two year period for customers of a business that have an ongoing subscription, account or loan or other qualifying relationship. (s.10(14)).

A person has "an existing non-business relationship" with a recipient if it arises from:

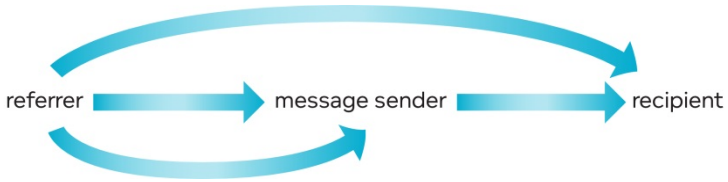
> (*a*) a donation or gift made by the person to whom the message is sent to any of those other persons within the two-year period immediately before the day on which the message was sent, where that other person is a registered charity as defined in subsection 248(1) of the *Income Tax Act*, a political party or organization, or a person who is a candidate — as defined in an Act of Parliament or of the legislature of a province — for publicly elected office;
>
> (*b*) volunteer work performed by the person to whom the message is sent for any of those other persons, or attendance at a meeting organized by that other person, within the two-year period immediately before the day on which the message was sent, where that other person is a registered charity as defined in subsection 248(1) of the *Income Tax Act*, a political party or organization or a person who is a candidate — as defined in an Act of Parliament or of the legislature of a province — for publicly elected office; or
>
> (*c*) membership, as defined in the regulations, by the person to whom the message is sent, in any of those other persons, within the two-year period immediately before the day on which the message was sent, where that other person is a club, association or voluntary organization, as defined in the regulations. (s.10(13)).

Where a period is specified above in relation to a donation, gift or membership, (a) in the case of a donation or gift, if it involves an ongoing use or ongoing purchase under a subscription, account, loan or similar relationship, the period is considered to begin on the day that the subscription, account, loan or other relationship terminates; and (b) in the case of a membership, the period is considered to begin on the day that the membership terminates. (s.10(14)).

Even though consent may be implied to send messages in these circumstances, it is still recommended that organizations make efforts to obtain express consents to send commercial electronic messages. Where a business has obtained express consent, it does not have to worry about satisfying the conditions

for implied consent, such as monitoring whether the business or non-business relationship continues to exist, when the two year or other period begins and ends, or if the message is relevant to the recipient's business.

### *Third Party Referrals*




The IC regulations provide a limited exemption to the consent provisions of CASL permitting third party referral messages to be sent. Under this exemption, the consent provisions of CASL do "not apply to the first commercial electronic message that is sent by a person for the purpose of contacting the individual to whom the message is sent following a referral by any individual who has an existing business relationship, an existing non-business relationship, a family relationship or a personal relationship with the person who sends the message as well as any of those relationships with the individual to whom the message is sent and that discloses the full name of the individual or individuals who made the referral and states that the message is sent as a result of the referral."

These individuals have an existing business relationship or an existing non-business relationship. Accordingly, while the consent provisions of CASL do not apply to the first message, the form and unsubscribe formalities of CASL do apply.

### *Exceptions from the Consent Requirement*

Certain classes of commercial electronic messages are exempt from CASL's consent requirements, but must comply with the form and unsubscribe requirements. These are CEMs that are listed in s.6(6) that *solely*:

> (*a*) provides a quote or estimate for the supply of a product, goods, a service, land or an interest or right in land, if the quote or estimate was requested by the person to whom the message is sent;
>
> (*b*) facilitates, completes or confirms a commercial transaction that the person to whom the message is sent previously agreed to enter into with the person who sent the message or the person — if different — on whose behalf it is sent;
>
> (*c*) provides warranty information, product recall information or safety or security information about a product, goods or a service that the person to whom the message is sent uses, has used or has purchased;
>
> (*d*) provides notification of factual information about
>
> > (i) the ongoing use or ongoing purchase by the person to whom the message is sent of a product, goods or a service offered under a subscription, membership, account, loan or similar relationship by the person who sent the message or the person — if different — on whose behalf it is sent, or

(ii) the ongoing subscription, membership, account, loan or similar relationship of the person to whom the message is sent;

(*e*) provides information directly related to an employment relationship or related benefit plan in which the person to whom the message is sent is currently involved, is currently participating or is currently enrolled;

(*f*) delivers a product, goods or a service, including product updates or upgrades, that the person to whom the message is sent is entitled to receive under the terms of a transaction that they have previously entered into with the person who sent the message or the person — if different — on whose behalf it is sent; or

(*g*) communicates for a purpose specified in the regulations.

There is some uncertainty about the meaning of the term ”solely” at the beginning of the list of partially exempted messages. Representatives of the CRTC, in unofficial remarks, have stated that the listed messages are not deemed to be CEMs. Rather the word “solely” exempts the messages listed above from the consent requirements of CASL if the messages need such exemption because the contents of the messages would otherwise make them CEMs. The RIAS, quoted above, also attempted to clarify the interpretation of this provision.

## DOES THE MESSAGE COMPLY WITH THE FORM AND UNSUBSCRIBE REQUIREMENTS?

Even if the consent requirements under CASL have been satisfied, commercial electronic messages (with the few exceptions discussed above) must contain certain specific information and must allow the recipient to “opt-out” or unsubscribe from receiving future messages from the sender.

### *Prescribed Information in Messages*

Under CASL, commercial electronic messages must include prescribed information that identifies the sender. This toolkit also contains guidelines to assist companies in updating their standard form signatures and email disclaimers in order to comply with these new requirements. It is also important to note that these requirements not only apply to email communications, but every form of commercial electronic messaging as described above.

### *Unsubscribe Mechanism*

CASL requires every commercial electronic message to include a mechanism which would “enable the person to whom the commercial electronic message is sent to indicate, at no cost to them, the wish to no longer receive any commercial electronic messages” from the sender. This toolkit contains further information on implementing an unsubscribe system that complies with CASL.

## HAS THE RECIPIENT UNSUBSCRIBED FROM RECEIVING COMMERCIAL ELECTRONIC MESSAGES?

Organizations should implement an efficient method that allows employees and other representatives to check whether a potential message recipient has unsubscribed or “opted-out” of receiving commercial messages from the business. This process can be automated through technical measures on enterprise outgoing messaging systems or Customer Relationship Management (CRM) systems. This toolkit provides further information on setting up an effective system to receive and record message unsubscriptions.

# Obtaining Consents

Since obtaining consents is a key component of CASL, it is important to know how these should be obtained.

### *Ways to Obtain Consent*

As noted above, CASL deems an electronic message that contains a request for consent to send a CEM as a CEM. This means individuals with whom a business has had no previous contact cannot be sent an electronic message with a request for consent to send further messages in most circumstances. Where the company already has an existing business or non-business relationship with the recipient, or the recipient otherwise satisfies the implied consent requirements, organizations may send a request for consent electronically; in fact, they are encouraged to do so in order to "convert" an implied consent (which may expire) into an express consent which only expires when consent is revoked.

Where a business does not have an existing relationship or other form of implied consent, consent to send commercial electronic messages must be obtained through other means.

Requests for consent may be obtained orally or in writing. Senders of CEMs have the onus of proving consent.

The CRTC considers the following forms as sufficient, but not the only ways, to discharge the onus of demonstrating oral consent:

- where oral consent can be verified by an independent third party; or
- where a complete and unedited audio recording of the consent is retained by the person seeking consent or a client of the person seeking consent.

The CRTC adds: "For example, a person may request and obtain oral consent in situations where information is collected over the phone (e.g. call centres) or consent may be given at the time that individuals use a product or service (e.g. point of sale purchases)."

The CRTC considers that the requirement for consent in writing is satisfied by information in electronic form if the information can subsequently be verified. Examples of acceptable means of obtaining consent in writing provided by the CRTC include checking a box on a web page to indicate consent where a record of the date, time, purpose, and manner of that consent is stored in a database; and filling out a consent form at a point of purchase. The CRTC's Toggling Guideline suggests that clicking agree to a pre-checked box is not an express consent.

Consent must be sought separately for each act covered by CASL (i.e. the sending of commercial electronic messages, the alteration of transmission data, and the installation of computer programs), but not for each instance of each act. In addition, separate consent is required for each organization or affiliate that wants to send messages to the recipient.

As noted above, senders of CEMs have the onus of proving consent. Accordingly, a company's compliance work should include ensuring that adequate processes and the necessary facilities exist to prove consent and to satisfy this onus. With this in mind, companies seeking consent may choose to do so "in writing," rather than orally, in order to ensure that they are able to prove the existence of the consent.

### *Prescribed Information when Obtaining Consent*

Under the CRTC regulations, when obtaining express consent to send CEMs, the request must set out the following information:

(a) the purpose or purposes for which the consent is being sought;

(b) the name of the person seeking consent and the name of the person, if different, on whose behalf consent is sought;

(c) if the consent is sought on behalf of another person, a statement indicating which person is seeking consent and which person on whose behalf consent is sought;

(d) if the person seeking consent and the person, if different, on whose behalf consent is sought carry on business by different names, the name by which those persons carry on business;

(e) the physical 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 sought; and

(f) a statement indicating that the person whose consent is sought can withdraw their consent by using any contact information referred to above.

### *Using a 3rd Party to Obtain Consent*

When using a third party to obtain consents, or when purchasing "mailing lists" from third party marketing agencies, Canadian business must ensure that the formalities for obtaining and using the consent are followed. The requirements are set out in the IC regulations which state the following:

> 5. (1) For the purposes of paragraph 10(2)(b) of the Act, a person who obtained express consent on behalf of a person whose identity was unknown may authorize any person to use the consent on the condition that the person who obtained it ensures that, in any commercial electronic message sent to the person from whom consent was obtained,
>
> (*a*) the person who obtained consent is identified; and
>
> (*b*) the authorized person provides an unsubscribe mechanism that, in addition to meeting the requirements set out in section 11 of the Act, allows the person from whom consent was obtained to withdraw their consent from the person who obtained consent or any other person who is authorized to use it.
>
> (2) The person who obtained consent must ensure that, on receipt of an indication of withdrawal of consent by the authorized person who sent the commercial electronic message, that authorized person notifies the person who obtained consent that consent has been withdrawn from, as the case may be,
>
> (*a*) the person who obtained consent;
>
> (*b*) the authorized person who sent the commercial electronic message; or
>
> (*c*) any other person who is authorized to use the consent.
>
> (3) The person who obtained consent must without delay inform a person referred to in paragraph (2)(*c*) of the withdrawal of consent on receipt of a notification of withdrawal of consent from the person referred to in that paragraph.

(4) The person who obtained consent must give effect to a withdrawal of consent in accordance with subsection 11(3) of the Act, and, if applicable, ensure that a person referred to in paragraph (2)(*c*) also gives effect to the withdrawal in accordance with that subsection.

### *Sharing or Obtaining Consent Amongst Affiliates*

CASL does not distinguish between affiliated and non-affiliated organizations. Therefore, if a business wants to rely on consents obtained by an affiliate to send commercial electronic messages, the requirements noted above with respect to third parties must be followed. The organization has three choices:

- Each affiliate can obtain its own consent.
- One affiliate can obtain consent on behalf of other affiliates as long as the other affiliates are identified and the prescribed information is provided for each affiliate when requesting consent. The RIAS states that "where it is not practicable to include this information in the body of a CEM, a hyperlink to a page on the World Wide Web containing this information that is readily accessible at no cost to the recipient may be included in the CEM."
- The entity can rely on the IC regulation which permits consents to be obtained on behalf of unidentified third parties, as long as the other requirements of the regulations are met.

The management of consents will be a challenge for organizations with multiple affiliates. The challenges will be even greater when an affiliate is sold, as the consents can form an important part of the assets of both the transferred business and the affiliates that remain behind. Proper arrangements will need to be struck that allow both organizations to carry on their respective businesses.

# Transferring Consents in Business Transactions

It is theoretically possible for one business to transfer its consents to another business in the context of the sale of the transferring business. However, doing so is likely to be a complicated exercise.

With respect to express consent, the RIAS states that "express consents will transfer upon the sale of a business, should the contract of sale include a provision transferring these as a business asset." It must be noted, however, that the RIAS only provide guidance on the transfer of express consents; the direct transfer of implied consents (such as those arising from an existing business relationship) is not addressed.

In the context of implied consent on the basis of a business relationship, CASL provides for the existing business relationship to be transferred following the sale of a business to a purchaser. However, it does not specifically state that the consents that flow from that relationship and held by the business may be transferred as well. Therefore, a significant CASL issue to be addressed when dealing in an asset acquisition involves obtaining and maintaining the consents of customers to receiving CEMs on this basis. When purchasing private information used to distribute CEMs, the purchaser must ensure that the consents being purchased from the seller are validly held and transferrable under CASL (and privacy laws).

The Implied Consent Guidance adds a further layer of interpretation:

> "When a business is sold, the purchaser can rely upon express consents obtained by the seller if the contract of sale of the business includes a provision transferring the list of email addresses for which consents have been obtained as part of all its assets. Therefore, the new owner will be able to continue sending CEMs to the recipients that gave express consent, as long as the other requirements of CASL are met. CASL also specifically indicates, at section 10(12) that, with the sale of a business, any existing business relationships (EBR) are considered to now be with the new owner of the business."

The Implied Consent Guidance seems to suggest implied consents do not transfer *per se*, but rather the exemption from consent created by a valid existing business relationship may be relied upon by an acquiring business. However, the onus is on the purchaser to ensure such underlying business relationships are, in fact, valid.

An important consideration here will also be which entity gets the benefit of the existing business relationship – the Implied Consent Guidance states that "with the sale of a business, any existing business relationships (EBR) are considered to now be with the new owner of the business". In other words, such relationships are not divisible, creating an all-or-none situation.

There is limited guidance with respect to the transfer of other forms of implied consent, such as implied consent arising from the conspicuous publication of an electronic address.

Based on the current available guidance, the transfer of consents is something that will need to be carefully considered on a case-by-case basis. This is particularly true where the consents being transferred are implied consents.

# Message Formalities

Organizations sending CEMs have to review the information that is included within all external commercial electronic communications that are CEMs.

These requirements apply to all CEMs (with limited exceptions discussed above), even if the recipient has consented to receiving the class of messages or the message is in response to a customer inquiry.

### *Formalities*

CASL requires that all commercial electronic messages contain the following information:

(a) the name of the person sending the message and the person, if different, on whose behalf it is sent;

(b) the name by which those persons carry on business;

(c) the physical and mailing address of those persons; and

(d) a telephone number of those persons, an email address of those persons, or, a web address of those persons.

Where it is impractical to include all of this information in the message (for instance, if the messaging medium limits the number of characters in the message), the regulations allow this information to be provided on a website, with a hyperlink to the website that is clearly and prominently set out in the message.

It is important that organizations review all forms of electronic messages that are used to communicate with third parties to ensure that each communication method is set up to comply with these form requirements.

**TIP:** Many email systems are set up to include signature information only with the first message in an email chain. In order to preserve space, all other replies in the chain do not include the senders' signatures. Such a practice may no longer comply with CASL. The first commercial electronic message from a party as a reply to an earlier message must now abide by these form requirements so that the prescribed information is included at least once in the email chain.

### *Unsubscribe Mechanism*

CASL requires every CEM to include a mechanism by which a recipient can opt-out of receiving future messages. The unsubscribe mechanism must:

(*a*) enable the person to whom the commercial electronic message is sent to indicate, at no cost to them, the wish to no longer receive any commercial electronic messages, or any specified class of such messages, from the person who sent the message or the person — if different — on whose behalf the message is sent, using (i) the same electronic means by which the message was sent, or (ii) if using those means is not practicable, any other electronic means that will enable the person to indicate the wish; and

(*b*) specify an electronic address, or link to a page on the World Wide Web that can be accessed through a web browser, to which the indication may be sent.

The unsubscribe mechanism specifies that two methods must be provided to message recipients to enable them to unsubscribe from receiving further messages. For some types of messages one

unsubscribe mechanism may satisfy both requirements. For example, an email message that specifies a return electronic address would satisfy both requirements in paragraph (a) and (b) above.

The CRTC regulations specify that an unsubscribe mechanism must be able to be "readily performed". The General Guideline has interpreted this to mean that "it must be accessed without difficulty or delay, and should be simple, quick, and easy for the consumer to use." The CRTC considers "a link in an email that takes the user to a web page where he or she can unsubscribe from receiving all or some types of CEMs from the sender" to be an example of an unsubscribe mechanism that can be readily performed. In the case of a short message service (SMS), the user should have the choice between replying to the SMS message with the word "STOP" or "Unsubscribe" and clicking on a link that will take the user to a web page where he or she can unsubscribe from receiving all or some types of CEMs from the sender.

Companies are permitted to create an unsubscribe mechanism that would allow recipients to opt-out of only certain classes of CEMs received from the company, although they must also provide an option to "unsubscribe from all CEMs."

# Updating Messaging Systems

As part of complying with CASL, organizations will need to implement systems to track recipient consents and give effect to unsubscribe requests.

Ideally these systems can be integrated directly into the messaging systems themselves or existing CRM systems. Employees who attempt to send CEMs to external electronic addresses where the intended recipient has either opted-out through the unsubscribe mechanism or has not consented in the first place should either be blocked from sending the message or subject to a warning that the company does not have the consent of the recipient.

Even if this kind of integration would be too onerous for many, organizations will nonetheless need to ensure that their consent and unsubscribe systems are functional, up-to-date and consistently utilized.

### *Tracking Consent*

A system to track recipient consents can be as simple as a spreadsheet for smaller organizations and as complex as a fully integrated database for larger enterprises.

For organizations that intend to rely on the implied consent provisions of CASL in order to send commercial electronic messages, the consent tracking system must be able to track the “expiry” dates of the implied consent categories. For instance, where a company received an inquiry on a certain product from a potential customer, the consent tracking system should take into account that follow-up replies to that potential customer can only be sent within six months of receiving the inquiry.

Once again, along with a system that tracks both situations of implied and express consent within a contacts database, it is recommended that organizations make efforts to “convert” the implied consents to express consents within the applicable timeframe when the implied consents are still “active”.

### *Respecting Unsubscribe Requests*

Significant liability could potentially arise for organizations that fail to respect unsubscribe requests. For this reason, it is important for every business to implement a system that tracks which electronic addresses cannot be sent CEMs. Ideally, the system will also work to prevent messages from being sent to these addresses. Note as well that certain customers may “re-consent” to receiving messages and in this case it would be appropriate to remove that address from the unsubscribe list in addition to adding it to the consent list.

Senders must give effect to unsubscribe requests within 10 business day of the request being made. For more on the technical requirements of the unsubscribe mechanism, see the discussion earlier.

# Proving Compliance

Being compliant with CASL is not enough. Your organization must be in a position to prove compliance with well-documented records. The CRTC has issued significant guidance on the level of record keeping it expects. Keeping with the general theme of CASL, the CRTC's expectations are onerous.

Continuing this theme, in its early decisions, the CRTC has highlighted that CASL's burden of proof falls on the person alleging consent and has insisted that proof be provided for each and every message that is the subject of a given investigation.[22] Organizations which are unable to provide proof at a granular level will face significant concerns.

The CRTC's Compliance Program Guideline states that your written corporate compliance policy should "address record keeping, especially with respect to consent". It goes on to explain the benefits of keeping records:

> "Good record-keeping practices may help businesses (i) identify potential non-compliance issues, (ii) investigate and respond to consumer complaints, (iii) respond to questions about the business's practices and procedures, (iv) monitor their corporate compliance program, (v) identify the need for corrective actions and demonstrate that these actions were implemented, and (vi) establish a due diligence defence in the event of complaints to the Commission against the business."

The Implied Consent Guidance list the basic set of records that organizations should retain:

- "commercial electronic message policies and procedures;
- all contemporaneous unsubscribe requests and resulting actions;
- all evidence of express consent (e.g. audio recordings or completed forms) from consumers who agree to receive commercial electronic messages;
- commercial electronic message recipient consent logs;
- commercial electronic message scripts;
- CEM campaign records;
- staff training documents;
- other business procedures; and
- official financial records."

The Implied Consent Guidance also addresses how to prove implied consent through a series of lengthy examples. One example addresses a common scenario where consent is implied by the publication of an electronic address online:

[22] Compu-Finder decision (CRTC 2017-368) at para. 67: "As the Commission noted in Compliance and Enforcement Decision 2016-428, the conspicuous publication exemption and its requirements set a higher standard than the simple public availability of electronic addresses. These conditions do not create broad licence for the senders of CEMs to contact any electronic address found online, but rather provide limited circumstances in which consent can be reasonably inferred, to be evaluated on a case-by-case basis."

> “A company collects email addresses from websites or other media publications. If the company wants to rely on conspicuous publication as a form of implied consent, then the company must be able to prove that there were no statements against receiving CEMs on the website or in the advertisement where the email addresses were collected, and must demonstrate how the CEMs were relevant to the recipients' business, role, functions or duties in a business or official capacity. For example, to prove there were no statements against receiving CEMs a company could record screenshots or have a contemporaneous record of the publication where the address was listed, including information such as the date, email address and URL.”

Detailed records of compliance will also be useful in proving due diligence if the CRTC investigates an unintentional breach (as discussed later in this toolkit).

# Older Consents

S.66 of CASL provided for a three-year transitional period for certain consents that could be implied based on a relationship with the recipient. This transitional period ended in July 2017. Organizations should be very careful to ensure that they are not relying on expired transitional consents, as these may form a hidden liability if they have not been converted into a valid consent during the transitional period.

The CRTC FAQs and the RIAS suggest that express consents received prior to July 1, 2014 will suffice for CASL purposes. However, there is no further “grandfathering” of other forms of existing consents, including implied consents, consents that were “bundled” into terms and conditions, or consents that contained pre-checked “I agree” boxes.

Now that the transitional period has expired, organizations will want to revisit the question of whether some or all of their historical bases for consent remain valid.

# Malware and Spyware

CASL's provisions potentially apply to all computer programs that are installed on any type of computer, system, machine, appliance or device as part of a commercial activity.[23] They do not have to be harmful in any way. The programs covered by the "malware/spyware" provisions could range from applications on personal computers, tablets and mobile devices to programs that are embedded in consumer products such as automobiles, TV sets, PVRs, home audio systems, household appliances and devices used in homes such as thermostats, security systems, lighting controls, and home networking systems, and an endless variety of other devices including watches, toys, learning systems, hearing aids and other medical devices and so forth. They are also ubiquitous in industrial and business applications.

These provisions must be considered with especial care, as the CRTC Installing Computer Programs Guidelines appear to introduce interpretive concepts that may be at odds with the actual language of CASL. For example, the CRTC suggests that "self-installed software is not covered under CASL", but then suggests that a person may "cause" a program "to be installed" through incomplete disclosure. These concepts do not closely track the language of CASL itself and could cause false comfort in future if the CRTC changes its views or the private right of action comes into force.

It is illegal under CASL to install or cause to be installed a computer program on any other person's computer system or, having so installed or caused to be installed a computer program, cause an electronic message to be sent from that computer system, unless (a) the person has obtained the express consent of the owner or an authorized user of the computer system and complies with the disclosure requirements of section 11(5); or (b) the person is acting in accordance with a court order (s. 8(1)).

When seeking consent, the purpose of the consent must be disclosed clearly and simply. This includes in general terms the function and purpose of the computer program that is to be installed if the consent is given (ss. 10(1), (3)).

If the program performs one of the malware or spyware functions listed in section 10(5), the person seeking express consent must, when requesting consent, clearly and prominently, and separately and apart from the licence agreement, (a) describe the program's material elements that perform the function including the nature and purpose of those elements and their reasonably foreseeable impact on the operation of the computer system; and (b) bring those elements to the attention of the person from whom consent is being sought in the prescribed manner (s. 10(4)). The CRTC says an acknowledgement from the user is required in such circumstances.

The basic consent and disclosure requirements do not apply to an update or upgrade if (a) there was an original express consent to the program installation or use, (b) if the person who gave the consent is entitled to receive the update or upgrade under the terms of the express consent and, (c) the update or upgrade is installed in accordance with those terms (s. 10(7)). The update or upgrade cannot be installed without obtaining a new express consent if the update or upgrade has one of the malware or spyware features listed in section 10(5).

[23] For a more complete analysis of the computer program provisions in CASL and the related regulations, see Barry Sookman, The Industry Canada CASL regulations and RIAS: a lost opportunity at http://www.barrysookman.com/2013/12/16/the-industry-canada-casl-regulations-and-rias-a-lost-opportunity/

A person is considered to expressly consent to the installation of a computer program if (a) the program falls into one of the listed categories in section 10(8) e.g., it is a cookie, HTML code, Java Scripts, an operating system, or is any other program that is executable only through the use of another computer program whose installation or use the person has previously expressly consented to, but only if (b) the user's conduct is such that it is reasonable to believe that they consent to the program's installation.

The list of programs for which express consent is deemed to exist can be expanded through regulations, but any addition to the list is still subject to the caveat that the user's conduct is such that it is reasonable to believe that they consent to the program's installation.

The prohibitions apply to programs installed from Canada in another country or vice versa.

### *Operating Systems and Cookies*

As noted above, a person is considered to expressly consent to the installation of a computer program if (a) the program falls into one of the listed categories in section 10(8) (e.g., it is a cookie, HTML code, Java Scripts, an operating system, or is any other program that is executable only through the use of another computer program whose installation or use the person has previously expressly consented to), but only if (b) the user's conduct is such that it is reasonable to believe that they consent to the program's installation.

The line between an application program and an operating system program may be a difficult one to apply. In the RIAS Industry Canada suggested that a braking system might be an operating system. It also provided guidance that section 10(7) does not apply to updates or upgrades to software of the type listed in section 10(8). This guidance confirms that an update to a program for which express consent is deemed to exist also applies to the update, as long as the user's conduct is such that it is reasonable to believe that they consent to the program's installation.

In the RIAS, Industry Canada also suggested that notwithstanding that section 10(8) deems an express consent to install "cookies", they are likely not programs covered by the Act.

### *Network security and TSPs*

Industry Canada noted in the RIAS that stakeholders expressed concern that CASL would impair their ability to take action to address threats to the security of their networks, which would be counter to the purposes of the Act. To address this concern, using the regulatory making power in under section 10(8)(a)(vi) of the Act, the IC regulations amended the previous draft language to provide for deemed consent for a Telecommunications Service Provider (TSP) to install computer programs to protect the security of the network from a current and identifiable threat to the availability, reliability, efficiency or optimal use of its network.

The new exception specifies the following programs:

> a program that is installed by or on behalf of a telecommunications service provider solely to protect the security of all or part of its network from a current and identifiable threat to the availability, reliability, efficiency or optimal use of its network;

### *Network updates*

As noted by Industry Canada in the RIAS, stakeholders expressed concern that CASL would impair their ability to update or upgrade their networks. To address this concern, the regulations also provide deemed consent for TSPs to install software on devices across all or part of a network for update and upgrade purposes.

The new exception specifies the following programs:

> a program that is installed, for the purpose of updating or upgrading the network, by or on behalf of the telecommunications service provider who owns or operates the network on the computer systems that constitute all or part of the network;

### *Correcting Program Failures*

The IC regulations also introduced a limited exception for correcting program failures. It exempts the following programs:

> "a program that is necessary to correct a failure in the operation of the computer system or a program installed on it and is installed solely for that purpose."

### *Public Safety*

The RIAS points out that even if programs are installed as part of a commercial activity, they will be excluded from CASL if required for reasons of public safety. According to the RIAS:

> "Note that the Act only applies to computer programs installed in the course of commercial activity, a defined term that excludes public safety and other purposes, so issues of public safety. However, for software issues that are not matters of public safety, the Regulations provide for deemed consent for the installation of computer programs that are necessary to correct a failure in the operation of a computer system or program that is already installed."

### *Form of Consent for Updates and Upgrades*

The RIAS also provides guidance on the form of consent required to install an update or upgrade. According to the RIAS:

> "For updates and upgrades to computer programs installed after CASL comes into force, the Act allows companies to get the consent of the owner or authorized user for future updates or upgrades to the computer program at the same time they obtain consent for the original installation, or when the user is downloading. That is, when a computer program is installed, consent must in general be requested in accordance with the Act, but there are no requirements for the form of a request for consent to install updates and upgrades, whether that consent is requested in advance or when the update or upgrade is installed."

Although not specifically referenced, the statement appears to reflect the provisions of section 10(7)(b) which states that an update or upgrade can be installed if there is an express consent if the person who gave the consent is entitled to receive the update or upgrade under the terms of the express consent and, the update or upgrade is installed in accordance with those terms. This approach is supported by the Installing Computer Programs Guidelines, which state the following:

> "An update or upgrade is generally a replacement of software with a newer or better version, in order to bring the system up to date or to improve its characteristics. Usually the update or upgrade will have new features. Common software updates or upgrades include changing the version of an operating system, an office suite, an anti-virus program, or various other tools.
>
> An update or upgrade makes changes to or replaces previously installed software. Retrieving current information and displaying it within a program is not considered to be updating the program within the context of CASL. For example, updating or refreshing information displayed in a program, such as

> refreshing the weather forecast in a weather app, or refreshing television listings in an electronic programming guide are not updates or upgrades for the purposes of CASL."

### *When the "Malware" and "Spyware" Features of a Program Must be Disclosed*

Under section 10(4), if the program performs one of the malware or spyware functions listed in section 10(5), the person seeking express consent must, when requesting consent describe the program's material elements that perform the function including the nature and purpose of those elements and their reasonably foreseeable impact on the operation of the computer system.

The section 10(5) functions are described as follows:

> (5) A function referred to in subsection (4) is any of the following functions that the person who seeks express consent knows and intends will cause the computer system to operate in a manner that is contrary to the reasonable expectations of the owner or an authorized user of the computer system:
>
> (a) collecting personal information stored on the computer system;
>
> (b) interfering with the owner's or an 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 an authorized user of the computer system;
>
> (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 an authorized user of the computer system;
>
> (e) causing the computer system to communicate with another computer system, or other device, without the authorization of the owner or an authorized user of the computer system;
>
> (f) installing a computer program that may be activated by a third party without the knowledge of the owner or an authorized user of the computer system; and
>
> (g) performing any other function specified in the regulations.

The combined wording of sections10(4) and 10(5) strongly suggests that disclosure was only required both when one of the listed items in paragraphs (a) to (g) existed and if the person seeking express consent knows and intends to cause the computer system to operate in that manner contrary to the reasonable expectations of the owner. This was confirmed in the RIAS which stated the following.

> Note that the reasonability test that is built in to the deemed consent provision of CASL also applies as a mechanism to reduce the risk of abuse of deemed consent in these Regulations. In addition, the requirements of section 10(4) of the Act to describe functions in section 10(5) only come into play when consent has to be requested. Furthermore, the notice requirements in section 10(4) only apply when the person seeking consent knows and intends for the function listed in section 10(5) to cause the computer system to operate in a manner that is contrary to the reasonable expectations of the owner or authorized user of the computer system

### *Existing Programs and Transitional Provisions*

There are hundreds of thousands, if not millions, of computer programs already installed on systems throughout Canada. CASL applies to all of these programs for at least two reasons. It is illegal to install updates or upgrades to them unless there is an original express consent to install the programs that included a consent to install the update or upgrade or unless a new express consent is obtained. Secondly, it is illegal for a person that installed a program to have that program transmit information to the person without having obtaining an express consent to do so. Many existing programs are regularly updated automatically (as desired by consumers) or require the transmission of information to a person for the program to continue to operate.

For the vast majority of programs currently in use the users would not have provided express consents to receive updates or upgrades. Moreover, the original suppliers of the programs often would not have any records including contact information such as email addresses of the persons receiving the updates or upgrades. Nor could emails even be sent out to many users asking for consent if this is done as part of a commercial activity without violating the anti-spam portions of CASL.

The transitional provisions were designed to temporarily alleviate these problems. The wording of section 67 reads as follows:

> If a computer program was installed on a person's computer system before section 8 comes into force, the person's consent to the installation of an update or upgrade to the program is implied until the person gives notification that they no longer consent to receiving such an installation or until three years after the day on which section 8 comes into force, whichever is earlier.

Under CASL there appeared to be only two ways in which a new update or upgrade could be installed for an existing program. If the update or upgrade is treated as a new program, then express consent would be required. If reliance was going to be placed on a prior consent associated with the first installation, then there would need to be (a) an original express consent to the program installation or use, (b) an entitled to receive the update or upgrade under the terms of the express consent and, (c) the update or upgrade has to be installed in accordance with those terms.

On its face, section 67 did not appear to meet the standards required to permit updates or upgrades to be installed for legacy programs because only implied and not express consent is deemed to be given. However, in the RIAS Industry Canada takes the position that there is a three year transitional period allowing updates and upgrades to programs installed prior to the coming-into-force of CASL.

# False or Misleading Statements

CASL also amended the federal *Competition Act* to prohibit false and misleading statements in electronic messages in order to promote a business interest or a product. The *Competition Act* has long contained provisions relating to false and misleading representations to the public (i.e. misleading advertising), and CASL added specific prohibitions to the realm of emails and other electronic messages.

Under the CASL amendments, it is contrary to the *Competition Act* to make false or misleading representations in any of an electronic message's sender description, subject matter field or message field, or in the URL or other locater in an electronic message or on a webpage.

These amendments came into the spotlight in March 2015, when the Competition Bureau launched a $30 million claim against three related car rental agencies for false or misleading representations in various marketing materials directed at the Canadian public. The charges made against the agencies included claims under the CASL amendments. The matter was subsequently settled at a cost of $3 million to the agencies.[24] Subsequently, in 2017, the Competition Bureau entered into a $1.25 million settlement with a pair of other car rental agencies in a case that touched upon email and mobile applications.[25]

CASL-compliant organizations will ensure that their employees and other representatives are aware that CASL creates separate offences for each of these headings. Sales representatives and marketers can no longer rely on statements in the body of a message to qualify claims found in the subject matter field. If a representation made in the subject field is found, on its own, to be false or misleading, the sender will have contravened the *Competition Act* regardless of the fine print found in the body of the message.

### *False and Misleading Electronic Messages*

CASL prohibits, for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product, sending or causing to be sent an electronic message that contains a representation that is false or misleading in a material respect. The "electronic message" in this case is the entirety of the message.

**TIP:** The requirement that the message be false or misleading "in a material respect" contemplates that some false or misleading representations, i.e. those which are not enough to reach the materiality threshold, may be acceptable. Note, however, that this "in a material respect" qualification does not apply for false or misleading representations applicable to subject matter information, sender information or a locater. Hence, false or misleading representations in these elements will be treated more strictly.

### *False or Misleading Subject Matter Information*

CASL's prohibition against false and misleading subject matter information is where CASL will create the largest gap between physical and electronic marketing. Where a physical flyer or advertisement poster can include a boastful title that is qualified within the body of the advert, CASL creates a distinct offence for a false or misleading subject matter line without regard to the body of the message or other elements.

[24] See http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03885.html and https://www.canada.ca/en/competition-bureau/news/2016/06/avis-and-budget-to-ensure-prices-advertised-are-accurate.html

[25] https://www.canada.ca/en/competition-bureau/news/2017/04/hertz_and_dollarthriftytopay125millionpenaltyforadvertisingunatt.html and http://www.ct-tc.gc.ca/CMFiles/CT-2017-009_Registered%20Consent%20Agreement_2_66_4-24-2017_7054.pdf

For instance, consider an email that an airline sends to its mailing list promising to provide "Flights from Ottawa to Calgary for $299 return". Where a physical poster or flyer with the same title could qualify that this stated price is subject to the myriad of fees, taxes and eligibility conditions associated with airfare, statements made in electronic message subject lines must stand on their own. Accordingly, aggressive email subject matter language poses substantial risk to senders.

**TIP:** CASL does not impose a size or character limit on what would be considered the "subject matter information" of a message. Organizations should therefore consider including a disclaimer such as "(some conditions apply)" or "(see message below for details and conditions)" at some point in the subject line in order to help with compliance with these new *Competition Act* requirements.

### *False and Misleading Sender Information*

The prohibition against false and misleading sender information should not be a significant concern to legitimate organizations. This would generally apply to information found in the "From:" field of an email and the purpose of this prohibition is to create an offence for sending messages under a false name.

### *False and Misleading Locator*

A common technique among malicious spammers is to create a URL that appears, at first glance, to represent a legitimate business. For instance, by adding another "c" to create the web address http://www.mcccarthy.ca, many email recipients could be fooled into believing this link will lead to the McCarthy Tétrault LLP website. CASL creates a prohibition against such practices and makes it an offence to send false or misleading URLs or other electronic locators for the purpose of promoting a business interest or product. This new provision is unlikely to be a concern to legitimate organizations.

### *Private Right of Action*

It is worth noting that the private right of action will also apply to breaches of S. 74.011, making it the only provision of the *Competition Act* that is subject to a private right of action.[26] As noted above, no new date has been scheduled for the private right of action to come into force.

[26] For a discussion of the problems presented by the private right of action in the context of the *Competition Act* provisions, see Donald Houston and Jonathan Bitran, Misguided Policy: CASL's Private Right of Action for Competition Act Reviewable Conduct at https://www.mccarthy.ca/en/insights/blogs/snipits/misguided-policy-casls-private-right-action-competition-act-reviewable-conduct

# Technical Compliance

Aside from the anti-spam and anti-spyware prohibitions, CASL prohibits other forms of malicious activity that is commonly conducted through the Internet and other digital networks. While most legitimate organizations would not intentionally engage in these sorts of activities, the provisions in CASL are sufficiently broad that they are worth paying attention to.

### *Altering Transmission Data*

CASL prohibits altering the transmission data in an electronic message so that the message is delivered to a destination other than or in addition to that specified by the sender. The purpose of this provision is to ensure that emails and other electronic messages are not sent or copied anywhere other than where the sender thinks they are going. Although it is unlikely any legitimate Canadian business is surreptitiously forwarding or copying messages by altering transmission data, some auto-forwarding and other technical processes may nonetheless fall offside of this provision.

CASL broadly defines “transmission data” as data that:

(a) relates to the telecommunications functions of dialing, routing, addressing or signaling;

(b) either is transmitted to identify, activate or configure an apparatus or device, including a computer program, in order to establish or maintain a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and

(c) does not reveal the substance, meaning or purpose of the communication.

### *Email Harvesting*

CASL amends PIPEDA, Canada’s privacy law, to prohibit the use of computer programs known as “address harvesters”. These are programs that are designed to generate or search for email and other electronic addresses to create mailing lists. The prohibition extends to both the use of address harvesting programs and to using electronic addresses that were obtained through the use of such programs. Therefore, it is important that organizations that obtain mailing lists from third parties ensure that these lists were obtained in full compliance with these and other CASL requirements. Although CASL does not prevent companies from obtaining mailing lists from third parties, it is highly recommended that organizations only obtain such lists from very reputable vendors with appropriate safeguards. This toolkit contains further advice on working with third parties.

Note that the simple use of address harvesting programs is contrary to CASL’s provisions. The prohibition against the automated collection of electronic addresses does not necessarily need to be tied to any spam-related activity.

### *Personal Information Harvesting*

CASL also prohibits using computer systems to collect personal information in the broader sense in addition to the address harvesting provisions.

CASL includes a broad prohibition against the collection of personal information, through any means of telecommunication, if the collection is made by accessing a computer system in contravention of an Act of Parliament. In other words, where someone has unlawfully hacked into a computer system, network or database, CASL makes it an offence to collect any personal information found therein, or using such personal information for any purpose. Once again, this emphasizes the importance of obtaining customer

lists or contact lists only from reputable sources and creating contractual safeguards to limit potential exposure to unlawfully acquired personal data.

### *Botnet Scan*

Very few legitimate organizations are engaged in what would normally be thought of as mass spamming. However, the truly malicious entities engaged in spamming will often gain control of computer systems owned by legitimate parties to facilitate their illicit activities. Computer systems that have been compromised through viruses and other malware are known as “bots” or “zombies”, as spammers are able to use large networks of these systems, called “botnets”, to send billions of spam emails.

Organizations should ensure their systems are not being used as part of these botnets. Before CASL comes into effect, companies should perform a technical sweep of their systems, paying particular attention to mail servers, with leading, up-to-date anti-virus and anti-malware programs. Doing so will lessen the likelihood of becoming involved in a spam-related investigation – which can be expensive and time-consuming. Also, if questions are asked about botnet activities emanating from a company computer, the company will want to be able to respond that it has taken reasonable steps to avoid such activities.

# Working with Third Parties

Many organizations often employ third party providers to assist with email marketing and other online outreach programs. Some third party providers will offer to completely outsource a company's digital marketing initiatives. Others will sell contact lists of prospective customers to businesses looking to broaden their client base.

Organizations that rely on third parties will not have the luxury of ignoring the new requirements in CASL since CASL imposes requirements both on senders of commercial electronic messages and the person on whose behalf those messages are sent. This means that companies that use third party providers to send messages can be held responsible if those messages were sent by the provider in violation of CASL's anti-spam provisions. CASL also creates additional disclosure requirements where the person sending the message is not the same entity as the person on whose behalf the message is sent.

### *Double Disclosure Requirements*

Earlier, this toolkit discussed the information that organizations must disclose about themselves in all commercial electronic messages, and the information that organizations must disclose when obtaining consents to send commercial electronic messages. In both of these cases, where the business has used a third party to either send the messages or obtain the consents, CASL imposes a "double disclosure" requirement – all of the information with respect to the sender that must be set out in commercial electronic messages or consent requests must also be set out with respect to the company on whose behalf the consent is sought.

It is the responsibility of both parties to ensure that all of this information remains valid for at least 60 days after the date the messages are sent.

### *Unsubscribe Requirements When Using a 3rd Party to Obtain Consent*

CASL creates additional requirements with respect to the unsubscribe requirements for organizations that have hired a third party to obtain consents from individuals to receive commercial messages. These requirements will apply if the third party was hired by the business to obtain specific consent only for itself, or if the business simply purchased a contact list where the individuals have presumably provided their general consent to the third party. For more details on these requirements, see the discussion earlier in this toolkit.

### *Contractual Terms*

When a business hires a third-party to handle aspects of its digital marketing strategy, it should be expected that this third party is aware of and is in compliance with all applicable laws, including anti-spam laws and regulations. Nevertheless, when hiring such third-party providers, it is recommended to contractually stipulate that they bear the burden of complying with these requirements and that they will indemnify the business for any breach.

Liability for a breach of CASL can arise from both a government body, primarily the CRTC, or through persons using the private right of action (either individually or collectively through class actions). As such, contracts for outside services should include protections for clients for breaches of the law by the service provider, for example:

- Representations and warranties that the services provided are and will continue to comply with the requirements in CASL and related regulations; and
- Indemnification against losses or damages from alleged or actual breach of CASL.

# Remedies, Penalties and Rights of Action

One reason why organizations need to be diligent about CASL compliance efforts is that the penalties for failing to comply with CASL's requirements have the potential to be large. CASL allows for the imposition of significant "administrative monetary penalties" that are not tied to the damage caused by the infraction. In addition, CASL also allows persons to seek monetary penalties beyond damage awards under CASL's private right of action. The potential for large administrative fines and the looming threat of private class actions reinforce the seriousness of CASL and the failure to abide by its provisions.

**NOTE**: The provisions establishing the private right of action will be the last of CASL's provisions to come into force. These provisions were originally scheduled to come into force in July 2017. However, an Order in Council suspended the private right of action and a new date has not yet been scheduled.

## ADMINISTRATIVE PENALTIES BY THE CRTC

Any contravention of the anti-spam or anti-spyware provisions of CASL (the latter of which is not covered under this toolkit) is a "violation" of the law, subject to an "administrative monetary penalty". These are, in essence, fines ranging from zero up to a maximum of $1,000,000 for an individual, or $10,000,000 for businesses. These fines can be imposed by the CRTC. Examples of possible violations include:

- sending a commercial email without the express or implied consent of the recipient;
- sending a commercial SMS message that does not identify the sender, or provide a compliant unsubscribe mechanism; or
- operating a message forwarding or re-direction service, or a proxy service, that causes a commercial email message to be sent to a person other than the original addressee, without the express consent of the sender or addressee.

In the written compliance and enforcement decision in *Blackstone*,[27] the CRTC set out a series of consideration for the assessment the administrative monetary penalty (AMPs) issued in that case:

- "that compliance with the Act can be promoted through the general deterrence associated with the AMP;
- that the non-compliant conduct reflected a large number of commercial electronic messages sent to recipients at a range of organizations, over approximately five months, and had not ceased as of the day before the notice of violation was issued;
- that some individuals did purchase services from Blackstone during the period in which messages were being sent, and that Blackstone may have been receiving a financial benefit as a direct result of messages sent in violation of the Act, but which cannot be quantified with the available information;
- that Blackstone's ability to pay could not be assessed because the company did not provide financial information as required in the notice to produce; and
- that Blackstone demonstrated a lack of cooperation by refusing to respond to the notice to produce, and did not indicate any likelihood of self-correction."

[27] See: http://www.crtc.gc.ca/eng/archive/2016/2016-428.htm. For a more in-depth review of the decision, see: Keith Rose, Daniel G.C. Glover, Charles Morgan and Kirsten Thompson, Seven Practical Lessons from CRTC's First CASL Enforcement Decision at https://www.mccarthy.ca/en/insights/blogs/cyberlex/seven-practical-lessons-crtcs-first-casl-enforcement-decision

To date, only a small number of administrative monetary penalties have been issued under the messaging provisions of CASL. The highest damages amount sought was $1.1 million dollars by way of a notice of violation (which was reduced to $200,000 on appeal to the CRTC).[28] The lowest was $15,000 but it is notable for being issued against a single individual in respect of just 58 emails (Compliance and Enforcement Decision CRTC 2017-65 or "*Rapanos*").[29]

Alleged messaging violators have typically agreed to an undertaking, which has always included a monetary payment. With respect to organizations, those payments have ranged from $48,000[30] up to $200,000.[31] Only one individual has entered into an undertaking, which involved a payment of $10,000.[32] In all cases, the undertakings have also involved a requirement to implement in a compliance plan.

### *Administrative Procedures*

The CRTC's designated investigators have the power to require preservation of data and to require the disclosure of data. They can apply for warrants to enter property to assess compliance with CASL and to assist in investigations. The CRTC has relied on its power to apply for warrants in at least one situation.[33]

The CRTC also has the power to issue notices to produce. It has demonstrated a willingness to use this power liberally.[34] For example, *Rapanos* stated that notices of production were issued against the party being investigated (twice), his spouse, the owner of the house where he resided, the host of his website domain and both of the companies that provided him with cell phone services (and that is just the notices that were mentioned in the decision). Early notices to produce have set aggressive timelines, provided little to no disclosure with respect to the nature of the alleged offences, and have demanded comprehensive disclosures in formats specified by the CRTC. They are very onerous in nature.

The CRTC may issue a "notice of violation" to a person or business that they believe, upon reasonable grounds, to have committed a CASL violation. This must be done within three years of the discovery of the alleged violation.

A person who receives such a notice must either pay the penalty stipulated in the notice, or make representations to the CRTC. Either the representations can be about the acts or omissions complained of—for example, to contest a factual or legal error—or simply to contest the amount of the penalty. The Commission must then decide, on a balance of probabilities, whether a violation has occurred. If it rules that the person or business has committed an offence, it may impose the penalty that was set out in the notice, or a lesser penalty it considers appropriate. It may also waive the penalty altogether or suspend it on conditions it considers necessary to ensure compliance. The CRTC must then serve notice of its decision on the person, along with notice of the right of appeal.

---

28 See http://www.crtc.gc.ca/eng/archive/2015/vt150305.htm

29 See http://www.crtc.gc.ca/eng/archive/2017/2017-65.htm. For a more in-depth review of the decision, see: Jade Buchanan, In New CASL Case, CRTC Sends $15,000 Message at https://www.mccarthy.ca/en/insights/blogs/cyberlex/new-casl-case-crtc-sends-15000-message

30 See http://www.crtc.gc.ca/eng/archive/2015/ut150325.htm

31 See http://www.crtc.gc.ca/eng/archive/2015/ut151120.htm

32 See http://www.crtc.gc.ca/eng/archive/2017/ut170612.htm

33 For a discussion of that warrant, see Keith Rose, CRTC Executes CASL Warrant as Part of Botnet Take-down at https://www.mccarthy.ca/en/insights/blogs/snipits/crtc-executes-casl-warrant-part-botnet-take-down

34 For a discussion of the CRTC's notice to produce power, see Kirsten Thompson, CASL Enforcement: Much Ado About Nothing? at https://www.mccarthy.ca/en/insights/blogs/snipits/casl-enforcement-much-ado-about-nothing

### *Right of Appeal*

There is a right of appeal to the Federal Court from a decision or order of the CRTC issued under CASL. Appeals must be filed within 30 days. If the appeal is on a question of fact, leave of the Federal Court is required. This leave must be applied for within 30 days of the decision or order, and the appeal must be filed within a further 30 days of the Court's decision to grant leave.

### *Injunctions*

The CRTC's designated investigators may also apply to a court of competent jurisdiction for an injunction to prevent any contravention of the anti-spam provisions of CASL. In order to grant such an injunction, the court must be satisfied that a person or business "is about to do or is likely to do anything that constitutes or is directed toward [such a] contravention." The injunction may be positive or negative: the court may order the person to do something, or not to do something, provided the order is directed at preventing a contravention of the law. Normally at least 48 hours' notice must be provided to all parties named in the application. However, in urgent cases where notice is not in the public interest, the court may issue the injunction on an ex parte basis.

## ADMINISTRATIVE PENALTIES UNDER THE COMPETITION ACT

The Competition Bureau enforces the deceptive marketing practices provision of the *Competition Act*—provisions that will now be augmented by CASL to deal with false or misleading electronic messages. The Bureau has extensive investigative powers. It can bring offending conduct to the Competition Tribunal, a court that deals with certain violations of the *Competition Act*. If the contravention is proven, substantial penalties can be levied: up to $750,000 for individuals and $10,000,000 for corporations (higher for subsequent contraventions). In the case of false or misleading representations that are done "knowingly or recklessly", there is also the possibility of criminal prosecution under the *Competition Act*.

As noted above, the Competition Bureau has taken aggressive approaches to false or misleading advertising cases with a CASL messaging components, leading to settlements of $3 million and $1.25 million for car rental agencies. The no-materiality standard for subject headers makes email messages a very attractive target and a major area of compliance concerns for organizations going forward.

## PRIVATE RIGHT OF ACTION

Finally, as noted above, the government has indefinitely suspended the coming-into-force of a section of CASL that provide a private right of action for persons who are affected by a violation of CASL. As drafted, this private right of action applied to violations of CASL, as well as those provisions of CASL that were exported into the *Competition Act* and PIPEDA. The applicant may apply for a court order for monetary relief. The application must be brought within three years from when the applicant learns of the alleged violation. There is no prohibition against joining different applicants together into a class action.

Potentially actionable conduct under the private right of action could include:

- harvesting contact information, for commercial purposes, by means of a computer program designed for that purpose, without the consent of the person whose information was obtained;
- using, for commercial purposes, a mailing list that was compiled by a computer program without the consent of the persons listed on it;
- misrepresenting the sender of a commercial electronic message; or
- making a materially misleading or false claim in a commercial electronic message.

If the court is satisfied that a business has committed a violation of CASL, the court can order that person to pay damages of:

- actual losses suffered or expenses incurred; and
- a statutory amount ranging from $200 per occurrence up to a maximum of $1,000,000 per day in which the violation occurred.

This amount is intended to promote compliance, not to be punitive. In assessing the appropriate amount, the Court must consider a list of factors including:

- the purpose of the order;
- the nature and scope of the contravention or reviewable conduct;
- previous conduct, including both previous violations and previous undertakings;
- any financial benefit that the person or persons obtained from the commission of the contravention or from engaging in the reviewable conduct;
- the person's or persons' ability to pay;
- whether the applicant has received compensation in connection with the contravention or the reviewable conduct;
- the factors established by the regulations; and
- any other relevant factor.

**TIP:** If the private right of action is re-introduced, organizations may consider self-reporting violations of the anti-spam, no-alter-transmission-data and anti-spyware provisions of CASL to the CRTC. A private action cannot be brought where the CRTC has taken enforcement action against an offender or entered into an undertaking with the offender.

## OTHER LIABILITY ISSUES

Officers, directors, agents and mandataries of corporations are personally liable for CASL violations committed by those corporations, if they direct, authorize, assent to, acquiesce in or participate in the commission. Employers are vicariously liable for the acts of employees. This applies equally to all offenses under CASL, including administrative penalties, private right of action damages, or penalties under the *Competition Act*.

So far, at least one officer of a CRTC target has been exposed to personal liability.[35] In that case, the CEO of a company that sent CEMs without meeting the unsubscribe requirements agreed to pay $10,000.

## DUE DILIGENCE DEFENSE

CASL provides for a due diligence defense to alleged violations. In order to increase the likelihood that such a defence will be available when needed, organizations are advised to undertake compliance activities such as implementing appropriate policies and procedures with respect to unsolicited commercial electronic messages, educating employees on CASL's requirements and appointing an officer in charge of ensuring compliance with CASL and dealing with complaints from message recipients.

[35] See: http://www.crtc.gc.ca/eng/archive/2017/ut170612.htm

Note that the *Competition Act* also allows for a due diligence defence in the case of false or misleading representations.

The CRTC's Compliance Program Guideline includes details on what the CRTC views as a suitable corporate compliance program. Following the CRTC's guidance should be helpful in establishing a due diligence defence. Some of the key recommendations in the Compliance Program Guideline include:

- having a single individual ultimately responsible for compliance. In the case of large organizations, this should be a member of the senior management team;
- having a written corporate compliance policy;
- providing employee training with corresponding corrective action for contraventions;
- engaging in monitoring and regular auditing of compliance; and
- establishing a system for handling complaints from customers.

# More Information

For more information on Canada's Anti-Spam Legislation, please contact:

TORONTO:

**Barry Sookman**
416-601-7949
bsookman@mccarthy.ca

**Dan Glover**
416-601-8069
dglover@mccarthy.ca

**Keith D. Rose**
416-601-7913
krose@mccarthy.ca

MONTRÉAL:

**Charles Morgan**
514-397-4230
cmorgan@mccarthy.ca

CALGARY:

**Cathy Samuel**
403-206-5528
csamuel@mccarthy.ca

VANCOUVER:

**David Crane**
604-643-5891
dcrane@mccarthy.ca

**Jade Buchanan**
604-643-7947
jbuchanan@mccarthy.ca

# Appendix A: Information to Collect for Compliance Audit

CASL impacts many ways in which organizations communicate with customers, other businesses and third parties. Before beginning any compliance audit, the following information should be gathered about your organization:

1. Who is your organization's Anti-Spam Compliance Officer or other person ultimately responsible for compliance?
2. Does your organization have a CASL Compliance Policy and documented CASL Compliance Process?
3. What forms of electronic communication does your organization use to communicate with outside parties for commercial purposes?
   - (a) Email?
   - (b) Instant messaging?
   - (c) Text messaging/SMS?
   - (d) Social networks (Facebook, etc.)?
   - (e) Other online services (e.g. web forums, portals)?
   - (f) Other means of electronic communication?
4. For each of these communication media, what identifying information about your organization is included along with each message (e.g. email signatures)?
5. For each of these communication media, how does your organization request consents to send electronic messages to recipients?
6. For each of these communication media, how does your organization record consents to receive electronic messages?
7. What express consents does the organization have to continue to send CEMs? Is proper documentation recorded?
8. Can the organization rely on any implied consents to continue to send CEMs?
9. For each of these communication media, how are requests to opt-out or unsubscribe from future messages received?
10. For each of these communication media, how are these opt-out or unsubscribe requests recorded or processed?
11. How does your organization ensure that contacts who unsubscribe are no longer contacted?
12. How does your organization track the way in which message recipients' contact information is received (e.g. business card, event registration, inquiry, etc.)?

13. Does your organization have an established process for handling customer complaints regarding CASL?

14. How does your organization track the date on which contacts are added to the contacts database

15. How does your organization add contacts to your mailing list in cases where the contacts do not have a relationship with the organization (for instance, by collecting electronic addresses from online websites or directories)?

16. Does your organization use “address harvesting” programs to collect electronic addresses to add to its contact list?

17. Does your organization rely on any third party providers to electronically communicate with customers or prospective customers on your behalf?

18. Does your organization purchase electronic mailing lists of prospective customers from outside parties?

19. Does your organization perform electronic messaging for third parties, or make available electronic mailing lists to third parties?

20. Does your organization provide training for external-facing employees against making false and misleading statements in outside communications?

21. Does your organization routinely run anti-malware scans on its mail servers to ensure they are not inadvertently being used by outside parties to send spam emails?

22. What training does your organization provide to employees with respect to CASL?

23. What remedial action is taken against employees who violate your organization’s CASL Compliance Policy?

# Appendix B: CASL Compliance Audit Checklist

Once a company has examined its commercial electronic communication practices, it is in a position to consider the requirements of CASL to assess its policies, processes and systems for compliance. The following checklist can help in determining the state of compliance with CASL:

- ❑ The organization has appointed an "CASL Compliance Officer" in charge of ensuring compliance with CASL, the *Competition Act,* and PIPEDA and to address complaints from members of the public. The CASL Compliance Officer should be a member of the senior management team.
- ❑ The organization has educated employees in detail on CASL's requirements including how to avoid sending unsolicited commercial electronic messages.
- ❑ The organization's education program includes educating employees on a zero-tolerance policy for making false and misleading statements in commercial electronic messages, including by way of omitting any relevant facts. The program must highlight the strict standards applying to electronic messages under the *Competition Act.*
- ❑ The organization's education program explains the consequences of non-compliance, including consequences for the organization and corrective action that will be taken with respect to the employee.
- ❑ The organization has a system in place to obtain and record consents to send commercial electronic messages and employees are aware of how to obtain, collect and record consents. The organization has made all necessary changes to its business processes and Customer Relationship Management (CRM) databases to ensure customer preferences are adhered to.
- ❑ Email signatures (and signatures for other electronic communication media) for external communications include the required prescribed information.
- ❑ The organization has implemented an unsubscribe system that will prevent future commercial electronic messages from being sent to those who opt-out, which takes effect within 10 days.
- ❑ The organization has ensured that its email and other messaging systems do not "alter transmission data" of emails as defined in CASL.
- ❑ The organization has ensured that it is not engaged in "email harvesting" as defined in CASL.
- ❑ The organization has ensured that it is not engaged in "accessing computer systems to collect personal information" as defined in CASL.
- ❑ The organization has revised its standard form agreements to ensure that third parties involved in sending commercial electronic messages to customers or other outside parties on its behalf are in compliance with CASL.
- ❑ The organization has conducted a technical audit to ensure that mail servers are not inadvertently being used by a third party to send out spam.
- ❑ The organization has a CASL compliance policy and regularly updates it. The policy should be designed to satisfy the due diligence defense.

mccarthy tetrault


## VANCOUVER

Suite 2400, 745 Thurlow Street
Vancouver BC  V6E 0C5
Tel: 604-643-7100  Fax: 604-643-7900

## CALGARY

Suite 4000, 421 7th Avenue SW
Calgary AB  T2P 4K9
Tel: 403-260-3500  Fax: 403-260-3501

## TORONTO

Suite 5300, TD Bank Tower
Box 48, 66 Wellington Street West
Toronto ON  M5K 1E6
Tel: 416-362-1812  Fax: 416-868-0673

## MONTRÉAL

Suite 2500
1000 De La Gauchetière Street West
Montréal QC  H3B 0A2
Tel: 514-397-4100  Fax: 514-875-6246

## QUÉBEC CITY

500, Grande Allée Est, 9e étage
Québec QC  G1R 2J7
Tel: 418-521-3000  Fax: 418-521-3099

## LONDON, UK

125 Old Broad Street, 26th Floor
London  EC2N 1AR
UNITED KINGDOM
Tel: +44 (0)20 7786 5700  Fax: +44 (0)20 7786 5702