Canada's Anti-Spam Legislation and Its Impact on US Businesses

JILLIAN SWARTZ, ALLEN MCDONALD SWARTZ LLP AND MELISSA J. KRASNOW, DORSEY & WHITNEY LLP, WITH PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

An Article providing an overview of Canada's Anti-Spam Legislation (CASL) and key compliance obligations. This Article discusses CASL's prohibition on sending commercial electronic messages (CEMs), such as emails or text messages, without express opt-in consent of the recipient, form requirements, key CASL exemptions, and regulatory enforcement. In addition, this Article addresses CASL's application in the context of cross-border transactions and commercial agreements and provides a comparison to US law.

Canada's anti-spam legislation (CASL) came into effect on July 1, 2014. Considered one of the most stringent anti-spam regimes in the world given its scope and penalties, CASL significantly affects the electronic communication practices of US businesses that carry on business or have customers, contacts or donors in Canada. While CASL includes some helpful exemptions, there is no blanket exemption for business-to-business communications. CASL is catching the attention of regulators and businesses around the world, in part due to the significant financial risk businesses face for failing to comply. As a result, businesses are developing and implementing robust compliance strategies. In addition, cross-border acquisition agreements and supplier agreements may include provisions to address CASL. Recent enforcement actions demonstrate that the Canadian Radio-television and Telecommunications Commission (CRTC) is expecting businesses to comply with all aspects of the law, including the consent, form and content, and unsubscribe mechanism requirements.

CASL applies to all commercial electronic messages (CEMs) where a computer system located in Canada is used to send or access the CEM, subject to certain exceptions. CASL prohibits:

- Sending CEMs without consent (*S.C. 2010, c. 23, § 6(1)*).
- Altering transmission data without express consent (*S.C. 2010, c. 23, § 7(1)*).
- Installing computer programs without express consent (*S.C. 2010, c. 23, § 8(1)*).
- Making false or misleading representations in electronic messages, including in the sender and subject lines (*S.C. 2010, c. 23, § 75*).
- Collecting email addresses using computer programs without consent (*S.C. 2010, c. 23, § 82*).
- Collecting personal information through unauthorized access to a computer system (*S.C. 2010, c. 23, § 82*).

(See *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23)*.)

This Article focuses on CASL's spam prohibition, given its broad applicability and commercial effects. In particular, it discusses:

- The application of CASL to US businesses.
- CASL's consent, opt-out, anti-spam, form and content and penalty and enforcement provisions.
- Strategies for complying with CASL.
- CASL's impact on transactions and supplier agreements.
- Recent enforcement actions.
- US counterpart laws, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) and the Telephone Consumer Protection Act (TCPA), comparing their key provisions to CASL.

CASL'S BAN ON SPAM

Unless a statutory exception applies (see *Exceptions from Consent Requirement* and *CASL Exemptions*), CASL prohibits sending a CEM unless:

- The recipient consents, either expressly or impliedly (see *Implied Consent* and *Express Consent*).
- The CEM complies with certain form and content requirements.

(*S.C. 2010, c. 23, § 6(1)*.)

If challenged, the CEM's sender bears the burden of establishing consent or that an exception applies (*S.C. 2010, c. 23, § 13*).

A CEM is an electronic message intended to encourage participation in a commercial activity, for example:

- Emails.
- Text messages.
- Instant messages.
- Direct messages sent through social networking sites.

Commercial activity is any conduct of a commercial character, whether or not there is an expectation of profit. Accordingly, CASL's prohibitions on spam cover a wide range of electronic communications including electronic messages that offer, advertise or promote any good, service, investment opportunity or gaming opportunity. (*S.C. 2010, c. 23, § 1.*)

EXCEPTIONS FROM CONSENT REQUIREMENT

Messages are exempt from the requirement to obtain consent if they solely:

- Provide a requested quote or estimate.
- Facilitate or confirm a previously agreed-on commercial transaction.
- Provide warranty, recall, safety or security information.
- Provide factual information about an ongoing subscription, membership, account, loan or similar relationship.
- Provide information related to an employment relationship or related benefit plan.
- Deliver a product, good or service under a prior transaction.

(*S.C. 2010, c. 23, § 6(6).*)

In addition, there is a one-time exemption where there is a third-party referral. To rely on this exemption:

- There must be an existing business relationship, an existing non-business relationship, a personal relationship or a family relationship between the referring person and the sender and recipient of the CEM.
- The CEM must disclose the full name of the person who made the referral and state that the CEM was sent as a result of the referral.

(*Electronic Commerce Protection Regulations, SOR/81000-2-175, § 4(1).*)

When a business relies on the implied consent provisions, the CEM must comply with the form and content requirements (*S.C. 2010, c. 23, § 10(9)* and see *Form and Content Requirements for Commercial Electronic Messages*).

IMPLIED CONSENT

Consent may be implied in several situations relevant to US businesses, for instance:

- When there is an existing business relationship.
- Where recipients have "conspicuously published" their electronic contact information.
- Under the "business card" exemption.

When a business relies on these implied consent provisions, the CEM must comply with the form and content requirements (*S.C. 2010, c. 23, § 10(9)* and see *Form and Content Requirements for Commercial Electronic Messages*).

EXISTING BUSINESS RELATIONSHIP

Implied consent exists where the recipient and the sender have an existing business relationship (*S.C. 2010, c. 23, § 10(9)(a)*). CASL narrowly defines existing business relationship as where in the two years preceding the date on which the CEM is sent the recipient of a CEM has done one or more of the following:

- Purchased or leased a product, a service or an interest in land from the sender.
- Accepted a business, investment or gaming opportunity from or with the sender.
- Entered into a written contract (that is currently in force or has expired) with the sender.
- Had a bartering relationship with the sender.

(*S.C. 2010, c. 23, § 10(10).*)

In addition, the definition of existing business relationship includes a situation in which the recipient of the CEM made an inquiry or application to the sender within the six-month period before sending the message.

To ensure they respect the two-year and six-month time frames, businesses need to maintain a sophisticated contact database to keep track of the date on which:

- A product or service is purchased or leased.
- Each contract is entered into (and its end date).
- Each inquiry or application is made.

TRANSITIONAL PERIOD FOR PRE-EXISTING BUSINESS RELATIONSHIPS

CASL contains a three-year transitional period starting on July 1, 2014 that allows senders of CEMs to rely on implied consent where:

- There is an existing business relationship that existed before CASL's effective date.
- The communications between the parties have included electronic messages.
- The recipient has not provided notification that she no longer consents to receiving CEMs.

(*S.C. 2010, c. 23, § 66.*)

As a result, US businesses that can prove they have an existing business relationship with a recipient and have communicated electronically with that recipient before July 1, 2014 have some additional time to scrub their contact databases and obtain express consent.

CONSPICUOUS PUBLICATION

CASL also allows businesses to send CEMs to recipients who have "conspicuously published" their electronic addresses, subject to certain conditions. To rely on this form of implied consent, both of the following conditions must be met:

- The publication of the electronic address must not be accompanied by a statement that the recipient does not wish to receive unsolicited CEMs.
- The CEM must be relevant to the recipient's business, role, functions or duties in a business or official capacity.

(*S.C. 2010, c. 23, § 10(9)(b).*)

BUSINESS CARD EXEMPTION

Similarly, the "business card" exemption applies where both:

- A recipient has disclosed her electronic address to the sender without indicating that she does not wish to receive unsolicited CEMs.
- The CEM is relevant to the person's business, role, functions or duties in a business or official capacity.

In this case, the sender can send CEMs without obtaining express consent. (*S.C. 2010, c. 23, § 10(9)(c)*.)

EXPRESS CONSENT

A sender of a CEM must obtain express consent from the recipient if it cannot establish implied consent and no exception or exemption applies (see *Exceptions from Consent Requirement* and *CASL Exemptions*). Express consent may be oral or written.

To obtain CASL-compliant express consent:

- **The person granting the consent must make a positive or explicit indication of consent.** According to regulatory guidance, consent must be opt-in consent, meaning that the consumer must take action to give consent. As a result, the common business practice of using an opt-out (or negative option) method for obtaining consent, such as a pre-checked consent box that a consumer has to un-check to signify that she does not want to receive marketing messages, does not comply with CASL. Businesses cannot rely on consents obtained in this manner before CASL came into effect.
- **Express consent cannot be subsumed in or bundled with requests for consents for other purposes.** For example, a sender cannot wrap express consent into its general terms and conditions. Further, a sender cannot condition the ability to purchase a good or service on providing express consent to receive CEMs.
- **The request for consent must contain certain information.** This information includes the name of the business seeking consent and a statement that the person whose consent is being sought may withdraw consent at any time.

An electronic message sent to obtain express consent to send CEMs in the future is itself a CEM. As a result, subject to certain exceptions, CASL does not permit businesses to send electronic messages seeking express consent after July 1, 2014. (*S.C. 2010, c. 23, § 1(3)*.)

FORM AND CONTENT REQUIREMENTS FOR COMMERCIAL ELECTRONIC MESSAGES

Each CEM that is not completely exempt from CASL must include certain identifying information and an unsubscribe mechanism.

IDENTIFYING INFORMATION

The CEM must include all of the following:

- The name of the person sending the message.
- If the message is sent on behalf of another person:
  - the name of the person on whose behalf the message is being sent; and
  - a statement indicating the person who is sending the message and the person on whose behalf the message is being sent.
- The sender's mailing address and:
  - a telephone number providing access to an agent or voice message system;
  - an email address; or
  - a web address of the person sending the message or, if different, the person on whose behalf the message is sent.

(*Telecom Regulatory Policy, CRTC 2012-183, app. § 2*).

UNSUBSCRIBE REQUIREMENTS

The unsubscribe mechanism must:

- Allow the recipient to indicate at no cost that she no longer wishes to receive CEMs from the sender.
- Be readily performed.
- Be available for use for at least 60 days after the CEM is sent.

A business must give effect to the unsubscribe mechanism without delay and within ten business days after the recipient has indicated that she wishes to unsubscribe. (*S.C. 2010, c. 23, § 11* and *Telecom Regulatory Policy, CRTC 2012-183, app. § 3*.)

CASL EXEMPTIONS

Certain CEMs are entirely exempt from CASL and businesses may send them without obtaining consent or complying with CASL's form and content requirements. These CEMs include certain:

- Business-to-business communications if there is a relationship between the sending and receiving businesses (the B2B exemption) (see *B2B Exemption*).
- Intra-business communications relating to the business (see *Intra-business Communications*).
- CEMs picked up outside of Canada (see *CEMs Picked up outside of Canada*).
- Posts on messaging platforms, such as social media sites (see *Platform Exemption*).
- Responses to requests, inquiries and complaints (see *Responding to Requests, Inquiries and Complaints*).
- Communications that satisfy legal obligations (see *CEMs That Satisfy Legal Obligations or Enforce Legal Rights*).

(*Electronic Commerce Protection Regulations, SOR/81000-2-175, § 3*.)

B2B EXEMPTION

One of the most helpful exemptions for businesses is the B2B exemption. Under this exemption, CEMs sent by an employee or representative of one business to an employee or representative of another business are exempt as long as:

- The businesses have a relationship.
- The message concerns the activities of the business to which the message is sent.

(*Electronic Commerce Protection Regulations, SOR/81000-2-175, § 3(a)(ii)*.)

CASL does not provide any guidance on what is a relationship in this context or the meaning of the phrase "the message concerns the activities of the business." Despite this lack of guidance, the B2B exemption allows many business-to-business communications to continue without the need to comply with CASL.

INTRA-BUSINESS COMMUNICATIONS

The intra-business exemption applies when:

- An employee, representative, consultant or franchisee of a business sends a CEM to another employee, representative, consultant or franchisee of the same business.
- The CEM concerns the activities of the business.

(*Electronic Commerce Protection Regulations, SOR/81000-2-175, § 3(a)(i)*.)

While these intra-business communications are exempt from CASL, employers should implement policies that prohibit employees from sending CEMs to other employees that do not relate to the employer, for example, messages that promote an employee's home business. These CEMs could form the basis of a complaint to the regulator based on CASL's vicarious liability provisions (see *Vicarious and Director Liability*).

CEMS PICKED UP OUTSIDE OF CANADA

In response to concerns of non-Canadian businesses that have little or no connection to Canada, CASL includes an exemption for a CEM that both:

- Is sent by a person who reasonably believes that the message will be accessed in a foreign state that is listed in the schedule to CASL's regulations (including the US, the UK, the EU, Japan, Australia and New Zealand).
- Conforms to the law of the foreign state.

(*Electronic Commerce Protection Regulations, SOR/81000-2-175, § 3(f)*.)

Therefore, CASL obligations generally do not apply where a business sends a CEM to a US customer who unexpectedly picks up the message while visiting Canada.

PLATFORM EXEMPTION

A CEM sent or received on an electronic messaging service is exempt from CASL if:

- The information and the unsubscribe mechanism CASL requires are conspicuously published and readily available on the user interface through which the message is accessed.
- The person to whom the message is sent consents to receive it either expressly or by implication.

(*Electronic Commerce Protection Regulations, SOR/81000-2-175, § 3(d)*.)

This means that the alerts and notices (but not direct messages from other platform users) sent through social networking sites, including Facebook and LinkedIn, generally are exempt from CASL.

CASL also exempts CEMs sent to a limited-access secure and confidential account, such as a message center in an online banking account, to which messages can only be sent by the person who provides the account to the person who receives the message (*Electronic Commerce Protection Regulations, SOR/81000-2-175, § 3(e)*).

RESPONDING TO REQUESTS, INQUIRIES AND COMPLAINTS

A CEM sent in response to a request, inquiry or complaint, or that the recipient otherwise solicits is exempt from CASL. However, the sender must ensure that the CEM only responds to the request or inquiry and does not provide other commercial information about the business or its products and services.

CEMS THAT SATISFY LEGAL OBLIGATIONS OR ENFORCE LEGAL RIGHTS

A CEM sent to satisfy a legal obligation or to enforce, or provide notice of, an existing or pending legal right or action need not comply with CASL. Similarly, a CEM sent to enforce a right, legal obligation or court order is exempt from CASL. (See *Electronic Commerce Protection Regulations, SOR/81000-2-175, § 3(c)*.)

PENALTIES AND ENFORCEMENT

Failure to comply with CASL may result in:

- Regulatory enforcement.
- Private lawsuits.
- Vicarious liability for the actions of employees and agents.
- Liability for directors or officers.

REGULATORY ENFORCEMENT

The CRTC has the power to enforce CASL's anti-spam provisions. CASL has an extraterritorial effect. CASL permits the Government of Canada, the CRTC, the Canadian Commissioner of Competition and the Canadian Privacy Commissioner to enter into written agreements with the governments of foreign states or international organizations to share information between signatories that pertains to one or more of the prohibitions in CASL (*S.C. 2010, c. 23, § 60*). Canada has entered into several of these agreements, which would facilitate enforcement of CASL against businesses outside of Canada.

Since CASL came into effect on July 1, 2014, the CRTC has received numerous complaints. The CRTC is assessing complaints submitted to the Spam Reporting Centre and has undertaken a number of investigations. The CRTC has made clear that it expects businesses to be in full compliance with all aspects of the law, including the:

- Consent requirements.
- Obligation to include a functional unsubscribe mechanism with each CEM.
- Requirement that each CEM contain prescribed information about the sender.

In addition, recent enforcement actions indicate that the CRTC is focusing on appropriate record retention by requiring alleged violators to prove that they have complied with each of CASL's requirements. For example, the CRTC suggested in guidance that, where a business wanted to rely on conspicuous publication as a basis for implied consent, it could either:

- Record screenshots.
- Maintain a contemporaneous record of the publication where the address was listed, including information such as the date, email address and URL (see *Compliance Strategies*).

PENALTIES

Potential penalties under CASL are substantial and include administrative monetary penalties of up to:

- Can$1 million for individuals.
- Can$10 million for corporations.

(*S.C. 2010, c. 23, § 20*.)

Based on an analysis of recent enforcement actions, it appears that the CRTC is considering the following factors when determining penalties:

- The purpose of enforcement (which is to ensure compliance rather than to punish).
- The nature and scope of the violation.
- Whether the violator has previously entered into any undertakings with the regulators.
- The financial benefits accruing to the violator resulting from the breach of CASL.
- The violator's willingness to cooperate with the regulator.
- The actions the business has taken to improve training and compliance programs and practices.
- Ability to pay.

PRIVATE RIGHT OF ACTION

CASL also creates a private right of action for persons affected by the violation of certain CASL provisions, including the anti-spam provisions. The statutory penalties available under the private right of action are up to Can$200 per breach to a maximum of Can$1 million per day plus the actual damages suffered or expenses the CEM recipient incurred. The private right of action under CASL does not take effect until July 1, 2017. (*S.C. 2010, c. 23, §§ 47, 51.*)

These statutory penalties are likely to provide a significant incentive to plaintiffs' attorneys to bring class action lawsuits. Therefore, the three-year delay is welcome news for industry, which has been concerned about facing class actions while both industry and the regulators are navigating the CASL regime.

VICARIOUS AND DIRECTOR LIABILITY

An employer can be held liable where an employee violates CASL while acting within the scope of her employment, unless the employer can show it exercised due diligence to prevent the violation (*S.C. 2010, c. 23, §§ 53, 54*). In addition, it is an offense to aid, induce, procure or cause to be procured the sending of CEMs in violation of CASL (*S.C. 2010, c. 23, § 9*).

CASL also provides for vicarious liability for directors and officers resulting from a company's failure to comply with CASL where they directed, authorized, assented to, acquiesced or participated in the non-compliance, subject to a due diligence defense (*S.C. 2010, c. 23, §§ 52, 54*).

COMPLIANCE STRATEGIES

To benefit from CASL's due diligence defense (*S.C. 2010, c. 23, § 33*), US businesses that have customers, contacts or donors in Canada should develop their compliance programs taking account of the following:

- **Categorizing their electronic messages.** By categorizing the electronic messages that a business sends by type and recipient, a business can obtain a better understanding of how CASL affects its electronic messaging practices. It can then consider the categories of messages that are exempt from CASL entirely or for which consent is not required or may be implied.
- **Creating standard templates for electronic messages.** Creating standard templates helps to ensure that the required identifying information and unsubscribe mechanism are included in every electronic message.
- **Creating a central contact database.** A central contact database assists the business in tracking consents and demonstrating it has obtained the required consent to send CEMs to its contacts. In addition, a database can effectively keep track of unsubscribe requests. Systems should also be introduced to ensure that opt-out requests are effected within the prescribed time frames.
- **Adopting a CASL policy and training employees on CASL compliance.** Since the CASL policy is an internal document, it should be kept separate from the business's privacy policy, which is a customer-facing document. Proper policies and training helps develop a business's CASL-compliance culture and build a due diligence defense.
- **Developing an audit program.** CASL compliance is not a one-time event; rather, it requires ongoing efforts. Instituting an audit program not only ensures that systems are working appropriately, but also supports a due diligence defense if a business's compliance is challenged.
- **Record retention.** CRTC guidance suggests that businesses consider maintaining hard copy or electronic records of:
  - CEM policies and procedures;
  - all contemporaneous unsubscribe requests and resulting actions;
  - all evidence of express consent (for example, audio recordings or completed forms) from those who agree to receive CEMs;
  - CEM recipient consent logs;
  - CEM scripts;
  - CEM campaign records;
  - staff training documents;
  - other business procedures; and
  - official financial records.

CASL'S EFFECT ON TRANSACTIONS AND SUPPLIER AGREEMENTS

Businesses in a wide variety of sectors, including technology, financial services and retail or consumer products, must evaluate CASL's effect on their ability to carry on business using their customary marketing practices.

CASL CONSIDERATIONS IN M&A TRANSACTIONS

Prospective buyers are inquiring about the regulatory and class action risks inherent in their targets' pre-closing electronic communication practices. As a result, CASL compliance has become a significant issue in both:

- Transaction due diligence.
- Allocating CASL-compliance risk in acquisition agreements in Canadian domestic and cross-border transactions.

In performing due diligence, counsel should be prepared to advise clients to review whether the target:

- Maintains a comprehensive contact database.
- Uses a template email format that complies with CASL.
- Has a CASL policy.
- Trains its employees on CASL compliance.

Conversely, counsel should prepare their target clients for requests for this information. Additionally, depending on the specific facts and circumstances, buyer's counsel should consider including representations and warranties and indemnification obligations specific to CASL in acquisition agreements.

CASL CONSIDERATIONS IN REVIEWING SUPPLIER AGREEMENTS

Businesses may request, or should consider requesting, that their suppliers provide detailed information about their electronic communications practices. Some large Canadian businesses have created multi-disciplinary teams sponsored by a senior executive that include members from the technology, legal, risk, procurement and marketing departments to review contracts with suppliers to ensure that these contracts include adequate protections.

Businesses that outsource their electronic communication or marketing functions should seek specific assurances from their suppliers and review their agreements to ensure they include representations, warranties and covenants to address ongoing CASL compliance. Suppliers should expect to receive these requests from their customers.

COMPARING US LAW TO CASL

The US compliance regime differs significantly from CASL and therefore creates compliance challenges for US businesses because CASL applies to a CEM where a computer system located in Canada is used to send or access it. While CASL covers a broad variety of CEMs, including commercial email messages, text messages, instant messages and direct messages sent through social networking sites, the US counterparts exist in two separate statutes:

- The CAN-SPAM Act, which applies to commercial email messages.
- The TCPA, which applies to text messages.

For a side-by-side comparison of CASL to these laws, see *Box, Comparison of CASL, CAN-SPAM and the TCPA*.

CAN-SPAM ACT GENERAL REQUIREMENTS

The CAN-SPAM Act applies to emails where the primary purpose of the email is the commercial advertisement or promotion of a commercial product (*15 U.S.C. §§ 7702(2)(A), 7702(6), 7702(9), (12), (15) and (16)* and *16 C.F.R. § 316.2(m)*).

The CAN-SPAM Act does not require the recipient's consent but does provide recipients opt-out rights. In addition to prohibiting materially false or misleading header information and deceptive subject headings, a commercial email message must:

- Be clearly and conspicuously identified as an advertisement or solicitation (except if the recipient has given prior affirmative consent to receipt).
- Include the sender's valid physical postal address.
- Include a clear and conspicuous explanation of how the recipient can opt out of getting commercial email messages from the sender.

(*15 U.S.C. § 7704(a)(1), (a)(2) and (a)(5).*)

For opt-out rights, the CAN-SPAM Act provides:

- Commercial messages must include a functioning return email address or other internet-based way to allow the recipient to opt out of receiving future commercial email messages that remains operative for at least 30 days after transmission of the original message (*15 U.S.C. § 7704(a)(3)(A)*).
- A recipient's opt-out request must be honored within ten business days of receipt, except if the recipient provides affirmative consent after the opt-out request (*15 U.S.C. § 7704(a)(4)*).
- The sender cannot require the recipient to pay a fee, provide any information beyond an email address and opt-out preference, or take any step other than sending a reply email or visiting a single internet page as a condition for honoring an opt-out request (*16 C.F.R. § 316.5*).

The email address of a recipient that opts out cannot be sold, leased, exchanged or otherwise transferred or released (including through any transaction or other transfer involving mailing lists bearing the recipient's email address) (*15 U.S.C. § 7704(a)(4)(A)(iv)*).

The Federal Trade Commission (FTC) has authority to enforce violations of the CAN-SPAM Act as unfair or deceptive acts or practices under the Federal Trade Commission Act, and it may:

- Pursue injunctive relief.
- Impose civil penalties of up to US$16,000 per email that violates the Act.

(*15 U.S.C. §7706(a), (d)* and *(e).*)

Other agencies, state attorneys general and other state officials or agencies also have authority to enforce the CAN-SPAM Act (*15 U.S.C. § 7706(b) and (f)*).

For more information on compliance with the CAN-SPAM Act, see *Practice Note, CAN-SPAM Act Compliance*.

TELEPHONE CONSUMER PROTECTION ACT GENERAL REQUIREMENTS

The TCPA applies where an automatic telephone dialing system is used to initiate text messages that are both:

- Directed to any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service or other radio common carrier service or any service for which the called party is charged for the call.
- The telephone call includes or introduces an advertisement or constitutes telemarketing.

(*47 C.F.R. § 64.1200(a)(1)(iii), (a)(2)* and *(f)(2).*)

The TCPA applies to text messages to wireless numbers (see *No. 02-278, FCC 03-153, In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 (July 3, 2003)*).

A sender must obtain prior express written consent of the recipient where the text message includes or introduces an advertisement or constitutes telemarketing.

Prior express written consent means a signed agreement in writing that clearly authorizes the sender to deliver advertisements or telemarketing messages using an automatic telephone dialing system that includes the telephone number to which the signatory authorizes delivery. The signed written agreement must both:

- Include a clear and conspicuous disclosure informing the signatory that executing the agreement authorizes the sender to deliver text messages using an automatic telephone dialing system.
- Provide that the person is not required, either directly or indirectly, to sign the agreement or enter into the agreement as a condition of purchasing any property, goods or services.

(*47 C.F.R. § 64.1200(f)(8)*.)

Under the TCPA rules, prior express written consent may be obtained by:

- Complying with the Electronic Signatures in Global and National Commerce (E-SIGN) Act (see *Practice Note, Signature Requirements for an Enforceable Contract: The Federal Electronic Signatures in Global and National Commerce Act (http://us.practicallaw.com/6-518-3096#a975253)*).
- Email.
- Website form.
- Text message.
- Telephone keypress or voice recording.

According to a Declaratory Ruling and Order issued by the Federal Communications Commission (FCC) in July 2015, a recipient has a right to revoke consent at any time and by using any reasonable method, including orally or in writing. The totality of the facts and circumstances surrounding a specific situation are taken into account in determining reasonableness. A sender must maintain proper business records tracking consent. (*No. 02-278, FCC 15-72, In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Federal Communications Commission Declaratory Ruling and Order (rel. Jul. 10, 2015)*.)

For more information on the affect of the declaratory order, see *Article, Expert Q&A: Far-reaching Declaratory Order on the TCPA (http://us.practicallaw.com/w-000-5132)* .

The FCC has authority to enforce violations of the TCPA and may impose forfeiture penalties of up to US$16,000 per violation (*47 U.S.C. § 503(b)*).

State attorneys general or other state officials or agencies also have authority to enforce the TCPA (*47 U.S.C. § 227(g)*).

In addition, the TCPA provides a private right of action for:

- Injunctive relief.
- Actual monetary loss or US$500 in damages per violation, whichever is greater.
- For willful or knowing violations, up to three times the actual monetary loss or US$1,500 in damages per violation, whichever is greater.

(*47 U.S.C. § 227(b)(3)*.)

TCPA text messaging violations have provided fertile ground for class action plaintiffs because of the nature of the penalties and the common issues often involved.

For more information on the TCPA, see *TCPA Litigation: Key Issues and Considerations (http://us.practicallaw.com/4-613-7306)*

COMPARISON OF CASL, CAN-SPAM AND THE TCPA

This table summarizes key differences among CASL, the CAN-SPAM Act and the TCPA.

	CASL	CAN-SPAM Act	TCPA
Messages covered	Commercial electronic messages, including: ■ Emails. ■ Text messages. ■ Instant messages. ■ Direct messages sent through social-networking sites.	Commercial email messages.	Text messages.
Scope	Applies where one of the purposes of the message is commercial.	Applies where **primary** purpose of email is commercial.	Applies where message is an advertisement or constitutes telemarketing.
Consent	Express consent, written or oral, required in all but a limited number of cases.	No consent required.	Prior express written consent for advertisement or telemarketing with some exceptions.
Identification requirements	Must: ■ Identify sender. ■ Identify person on whose behalf message is sent, if different. ■ Include certain contact information, including mailing address.	Must include sender's postal address.	Must identify sender.
Unsubscribe and opt-out requirements	■ Must be able to be readily performed. ■ Must be valid for 60 days after message sent. ■ Sender must give effect to unsubscribe mechanism within ten business days of receiving request.	■ Must be valid for at least 30 days after message sent. ■ Sender must give effect to opt out within ten business days.	■ Right to revoke consent at any time and by any reasonable method. ■ Industry practice.
Penalties and enforcement	■ Administrative monetary penalties: up to Can$1 million for individuals and up to Can$10 million for corporations. ■ Private right of action (takes effect July 1, 2017): actual damages suffered or expenses incurred plus up to Can$200 per breach up to a maximum of Can$1 million per day. ■ Employer and vicarious liability for directors and officers.	■ Violation as unfair or deceptive act or practice under Federal Trade Commission Act: ■ injunctive relief; and ■ civil penalties up to US$16,000 per email in violation. ■ Other federal and state regulator enforcement.	■ FCC Enforcement action: ■ Forfeiture penalties, including up to US$16,000 per violation. ■ Private right of action for either or both: ■ injunctive relief; or ■ US$500 per violation or US$1,500 for willful or knowing violation. ■ State regulator enforcement.

10-15