4. Information and Communications Technology

Companies wishing to conduct business in the Canadian information and communications technology sector will face a myriad of considerations. Although these are similar to those found in the United States, there are certain key distinctions that parties should be aware of.

Internet and E-commerce

In order to manage the dynamic commercial nature of the Internet, federal and provincial governments have responded by:

- Implementing e-commerce legislation to facilitate the flow of online transactions and ensure that adequate safeguards are in place to protect parties from fraudulent activity
- Introducing legislation regulating the sending of e-mails, text messages, and other forms of electronic messaging, as well as the use of certain applications for marketing purposes
- Introducing legislation regulating the installation of computer programs and the "pushing" of software updates on a person's computer
- Enacting electronic evidence legislation to ensure that electronic records can be tendered as evidence in legal proceedings
- Updating consumer protection legislation in order to reflect the new realities of e-commerce
- Regulating the use of web addresses ending in ".ca" (Canada's top-level domain name)

E-commerce Legislation

The central component of e-commerce legislation across Canada is the issue of functional equivalency. Essentially, this means that e-commerce legislation is intended to achieve two objectives: first, to ensure that contracts formed online should be treated in largely the same manner as contracts formed in the traditional tangible format, provided certain criteria are met (some contracts, such as wills or contracts involving the sale of real estate, cannot be formed online); and second, to ensure that electronic documents will meet any statutory requirements for a document to be provided in writing.

Anti-Spam Legislation

On July 1, 2014, key portions of Canada's anti-spam law *(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)*, informally and better known as "CASL", came into force.

CASL addresses the problem of unsolicited electronic communications (i.e. spam) by focusing on commercial electronic messages (CEMs). Additionally, CASL introduces rules to address the problem of unsolicited installed software programs (UIPs), such as cookies. CASL creates a set of rules to follow to obtain appropriate consent to send out CEMs and install software programs. It also sets out specific procedural and content requirements for consent as well as provisions and exceptions to certain requirements. CASL does not distinguish between messages sent for legitimate versus malicious purposes, nor between messages sent to an individual and those sent in bulk. All CEMs require the appropriate consent of the recipient. Moreover, CASL sets out a framework that is significantly broader in coverage than its American or European counterparts.

CASL came into force over a period of three years, with an intended staged rollout as follows: (i) the anti-spam provisions coming into force on July 1, 2014, and (ii) the provisions regarding UIPs coming into force on January 15, 2015. However, the provisions providing for a private right of action that were to come into force on July 1, 2017, have been suspended indefinitely, but are still under consideration by the Canadian government.

The CASL legislation has a significant impact on the business of all individuals using electronic messages to promote their activities or enter into contact with past or prospective clients.

Seeking to comply with CASL:

- **Application outside of Canada:** In order for the CASL anti-spam requirements to apply, a computer system located in Canada needs to have been used to send or access the electronic message; accordingly, foreign senders of CEMs are caught by this legislation. For the UIP provisions to apply, either the computer system, the person, or the person directing a person must have been in Canada at the relevant time.
- **Low threshold for application:** A CEM that is subject to the CASL anti-spam rules is defined as any electronic message that "it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity". This is a broad definition that includes more than what would be traditionally defined as electronic spam. Accordingly, to the extent that a CEM has the encouragement of participation in a "commercial activity" as at least one of its purposes – even if not as its sole purpose – the CASL anti-spam rules will apply.

- **More than just e-mail:** While CASL is colloquially referred to as an "anti-spam law", it applies to any transmission of an electronic message, including text, sound, voice, or image messages, to (i) an e-mail address, (ii) an instant messaging account, (iii) a telephone account, or (iv), somewhat ambiguously, "any similar account".
- **Importance of relationship with recipient:** Depending upon the sender's relationship with the recipient, the CEM may be (i) exempt from both the consent and message content requirements, (ii) exempt from the consent requirements, or (iii) subject to deemed, rather than express, consent. For example, there are exceptions for prescribed pre-existing business and pre-existing non-business relationships as well as for employees of an organization sending CEMs to one another internally and to employees of other organizations if they have a relationship and the message concerns the activities of the recipient organization. Understanding when such exceptions might apply, however, is challenging.
- **Deemed express consent for certain UIPs:** In addition to anti-spam rules, CASL sets out rules concerning the express consent that must be obtained when software is installed on a person's computer system. This requires that certain disclosures be made to the recipient and that an appropriate acceptance mechanism be put in place. However, deemed consent is said to have occurred in the installation of certain prescribed UIPs – such as where the program is a cookie, an operating system, or a network update or upgrade – where the person's conduct is such that it is reasonable to believe that they consent to the program's installation. Unfortunately, it is not clear what "conduct" will be sufficient to meet the threshold of evidencing a "reasonable belief" that the person consents to the installation of such a program.
- **Express consent must be opt-in and unbundled:** The base consent principle of CASL is that express consent is required from a recipient in order to send CEMs and install UIPs. For example, CASL requires that express consent must be opt-in (i.e. the recipient must give an explicit indication of consent) and that each request for consent must be separate and cannot be bundled together with other requests for consent for different purposes, such as consent requests for general terms and conditions. Businesses need to ensure that their requests for consent are designed in such a way that they comply with CASL.

The consequences of violating CASL rules are significant. There are various provisions that set out the enforcement framework for CASL. They include (a) the application of an administrative monetary penalty, where the maximum penalty is $1,000,000 in the case of an individual and $10,000,000 in the case of any other person, (b) the entry into an undertaking by the offending party, (c) the issuance of a notice of violation against the offending party, (d) injunctive relief, and (e) a private right of action (currently not yet in force) that, if successful, could result in a court order requiring the offending person(s) to pay the applicant (i) compensation in an amount equal to the actual loss or damage suffered or expenses incurred and (ii) in the case of a breach of (A) the anti-spam provisions a maximum of $200 for each breach, not to exceed $1,000,000 for each day on which a breach occurred, and of (B) the UIP provisions $1,000,000 for each day on which a breach occurred.

In addition, any officer, director, or agent of a corporation that commits a violation can be liable for the violation if they directed, authorized, assented to, acquiesced in, or participated in the commission of the violation, whether or not the corporation is proceeded against.

In the seven years since CASL came into effect, enforcement efforts have resulted in over $1,400,000 payable in penalties, including $805,000 from administrative monetary penalties and $668,000 from negotiated undertakings. As part of such enforcement efforts, monetary payments as part of negotiated undertakings entered into by businesses for non-compliance have ranged from $10,000 to $200,000; there has been one notice of violation with an accompanying administrative monetary penalty of $200,000; and other compliance and enforcement decisions have imposed administrative monetary penalties ranging from $15,000 to $200,000.

Given the potential for personal liability for CASL breaches, it is important that businesses ensure that they develop and implement CASL compliance programs, including the development of anti-spam, as well as UIP policies, and any necessary amendments to their existing privacy policies.

A Canadian Radio-television and Telecommunications Commission bulletin on November 5, 2018 (CRTC 2018-415) provided general compliance guidelines and best practices for stakeholders with respect to the prohibition, under section 9 of CASL, to aid, induce, procure, or cause to be procured the doing of any act contrary to any part of sections 6 to 8. While untested, it appears that section 9 may apply to individuals and organizations who are (i) intermediaries that provide enabling services that allow someone else to violate sections 6 to 8 or (ii) receiving a direct or indirect financial benefit from such violations. Advertising brokers, electronic marketers, software and application developers, software and application distributors, telecommunications and Internet service providers, and payment processing system operators may be at risk, depending on certain factors, which include the following:

- The level of control over the activity that violates sections 6 to 8 of CASL and the ability to prevent or stop that activity
- The degree of connection between the actions that violate section 9 and those that contravene sections 6 to 8 of CASL
- Evidence of reasonable steps taken to prevent or stop violations from occurring

E-evidence Legislation

Canadian electronic evidence legislation aims to set out the conditions under which electronic evidence will be accepted as the "best evidence" available in a legal proceeding. The federal law, and most of the provincial evidence laws, have now been amended to address this issue.

To summarize, an organization wanting to ensure that its electronic records will be accepted in court must ensure that there is reliable assurance as to the integrity of the information contained in an e-document since the time the document was first created in its final form (that the information has remained complete and not been altered) and must establish the integrity of the system used to produce the e-document, specifically when the e-document was initially recorded.

Such an organization must also establish that the system was operating properly at all material times or that, if it was not operating properly, the failure did not affect the integrity of the e-document and there are no other reasonable grounds to doubt the integrity of the system or the e-document (*R v Hirsch*, 2017 SKCA 14). The way in which the electronic record has been stored, and the manner in which it is copied, transmitted, or reproduced, may also affect the admissibility of the electronic record.

The Québec legislative initiative in this area is the *Act to Establish a Legal Framework for Information Technology*, which came into force on November 1, 2001. Until recently, it has received little attention from courts and legal practitioners due to its complexity.

Consumer Protection Legislation

Unlike the American system of federal consumer protection, the Canadian consumer protection regime varies in each province and territory, with different rules and regulations to consider for each of these jurisdictions. For that reason, where an electronic contract is intended to be executed by a "consumer" (as defined in each jurisdiction's regulations), the contract must meet both general consumer protection requirements (e.g. prohibiting unfair practices) and e-commerce-specific formality requirements (e.g. that certain disclosures be made at certain times during the electronic contracting process). Both sets of requirements can differ significantly among the provinces and territories.

The consumer protection regime in Canada can be complex for other reasons as well. Online contracts often fall into multiple categories of regulations with overlapping requirements. For example, in Ontario, an online contract could constitute an "Internet agreement," a "future performance agreement," and/or a "remote agreement." In British Columbia, an online contract could be a "distance sales contract" and/or a "future performance contract." In Québec, following the amendments made to the *Consumer Protection Act* in 2006 (sections 54.1 to 54.16), an online contract can be qualified as a "distance contract" and must also fulfill the requirements of the *Civil Code of Québec*. Further provisions in some provinces and territories aim to reconcile the different requirements.

Additionally, some of these requirements are not necessarily intuitive. They include requirements that: (i) certain disclosures be made to, and also included in, an online contract with the consumer; (ii) the contract be in writing; and (iii), particularly odd in the context of an online contract, a copy of the contract be provided to the consumer. The *Ontario Consumer Protection Act*, for example, requires each supplier to deliver a copy of the Internet agreement in writing to the consumer within fifteen days after the consumer enters into the agreement.

Failure to properly follow these requirements can be costly, forcing a merchant to accept returned goods, provide refunds, or pay fines for a violation. For example, Saskatchewan's *Consumer Protection and Business Practices Act* imposes a $100,000 fine for contravening any of its Internet sales contract provisions; this is followed by up to $500,000 in fines for subsequent violations. Directors of corporations found to have violated Saskatchewan's rules can also be held liable, whether or not the corporation has been prosecuted or convicted.

In addition, a company may find itself "named and shamed" by the applicable regulatory authority. For example, Ontario's Ministry of Government and Consumer Services maintains a searchable "Consumer Beware List", which lists the company and the nature of the offence, and can be readily accessed and consulted by consumers to determine the nature of the complaint.

Software Licensing and Commercialization

Companies seeking to license and commercialize information technologies in Canada should familiarize themselves with the Canadian intellectual property regime.

Following the introduction of the Canada-United States-Mexico Agreement (which replaced the North American Free Trade Agreement), significant changes were made to both the *Copyright Act* and the *Trademark Act* effective as of July 1, 2020.

Regarding shrink-wrap licences, purchasers need to be aware of the terms at the time of sale in order for such licences to be enforceable in Canadian courts. In addition, sale-of-goods legislation is generally inapplicable to prepackaged software sold to a customer under a licence as there is no transfer of property.

ISPs and Telecommunications

Foreign ownership restrictions apply to telecommunications common carriers who are owners of telecommunications transmission facilities. Parties seeking an alternative may wish to consider becoming simple telecommunications service providers by leasing their facilities and equipment from an authorized common carrier.

With this in mind, a company could become an Internet service provider (ISP) in Canada without being subject to the foreign ownership restrictions. ISPs will not be held liable for copyright infringement perpetrated by their subscribers, provided the ISPs are acting in a passive manner as a conduit for the exchange of information. Furthermore, ISPs will not incur liability for caching (the act of temporarily storing a copy of a website or content), since this is a protected process under the *Copyright Act*.