INFORMATION TECHNOLOGY

By Charles S. Morgan

INFORMATION TECHNOLOGY

Export Control of Technology

In Canada, the control of exports in technology falls within the mandate of the federal government. These controls apply not just to physical shipments, but also to transfers by intangible means, including through the provision of services or training, downloads or other electronic file transfers, e-mails, faxes, telephone conversations and face-to-face meetings. Export of certain computers, technology and other products may be controlled by means of the *Export and Import Permits Act* (EIPA), the *United Nations Act* (UNA), or the *Special Economic Measures Act* (SEMA). Under the UNA and the SEMA, Canada can restrict the export of goods, as well as the movement of people and money and the provision of services, to any country against which the United Nations or Canada has imposed economic sanctions.

The Export Control List (ECL) kept under the EIPA restricts certain high-tech goods, but is not product specific; instead, it provides a set of technical specifications that are technology-neutral for the most part and are functional in their description. The ECL also regulates the export of certain software (software generally available to the public is not usually restricted). Software and other items having cryptographic security features are generally covered by export controls, subject to certain limited mass market and public domain exceptions, unless the cryptography employs very low-key lengths. In addition, all U.S.-origin technology that is to be transferred to a destination other than the U.S. is subject to export controls.

Consumer Protection — Internet Agreements

Over the past decade, various legislative initiatives have provided more legal certainty to doing business online. In Ontario, for example, the *Consumer Protection Act, 2002* (CPA) overhauled various existing consumer protection legal regimes and brought them under one roof for consistency and ease of administration. Some important extensions of the law favour consumers. These extensions are particularly germane to online commerce, where a growing number of Canadian consumers buy and sell goods and services, though they apply generally outside e-commerce as well. See Manufacture and Sale of Goods — Consumer Protection.

The creation of a new implied warranty, for example, requires that services supplied under a consumer agreement be of "a reasonably acceptable quality." It also extends the implied warranties in the *Sale of Goods Act* to goods that are leased or traded. Another important change is a provision that prohibits contracting out of the class action proceedings regime. This is designed to counteract the practice of some merchants to provide arbitration as the contractually stipulated dispute resolution mechanism, precisely to avoid a class action scenario. Further, the CPA requires the merchant to provide the consumer with a fairly extensive list of disclosure information before concluding an Internet agreement. The CPA also requires that this information be disclosed to the prospective consumer in a manner that is "clear, comprehensible and prominent," as well as "accessible." In addition, a confirmation screen that summarizes the consumer's purchase details just before the conclusion of the online purchase is mandatory, along with the requirement that the merchant provide a copy of the Internet agreement to the consumer within 15 days after the consumer enters into that agreement. Finally, recent amendments to the CPA set out rules for pre-paid cards such as gift cards, which comprise a growing segment of the consumer economy, especially online. These rules cover a number of requirements and limitations on issuers, such as whether a gift card can have an expiration date or whether the issuer can charge the consumer any fees, among other things. Similar provisions that regulate Internet agreements and pre-paid cards have been adopted in the majority of Canadian provinces.

Evidence Laws

Most jurisdictions in Canada have adopted rules of evidence that specifically address electronic documents. The statutes now also provide for the best-evidence rule to be satisfied in respect of electronic records, by proof of the integrity of the electronic records system by which the data was recorded or preserved. These provisions allow the integrity of the record-keeping system to be implied from the operation of the underlying computer-related devices. In short, the amendments support the admissibility of electronic evidence, while still permitting a party to challenge the reliability of the computer system or network that produced the evidence.

In the current era of electronic word processing coupled with e-mail, strict and literal compliance with litigation discovery rules, such as Rule

30 of the *Rules of Civil Procedure* (Ontario), would prove very expensive and largely of limited value to participating litigants. Therefore, judges in Canada are increasingly receptive to having parties to litigation follow e-discovery guidelines. These require, for example, that parties contemplating or threatened with litigation must consider e-evidence issues and, among other things, circumscribe the scope of e-discovery in order to comply with Rule 30. See **Dispute Resolution — Electronic Discovery**.

E-Commerce Statutes

The Canadian provinces have adopted electronic commerce statutes that address a variety of issues that arise in doing business electronically, such as the validity of using electronic messages to meet the writing requirements for legal documents. Ontario's *Electronic Commerce Act*, for example, provides that the legal requirement for a document to be in writing is satisfied by a document that is in electronic form — such as e-mail — if it is accessible so as to be usable for subsequent reference. The provincial electronic commerce statutes also stipulate that one can satisfy any legal requirement that a document be signed by an electronic signature. The definition of "electronic signature" is very broad and encompasses any electronic information that a person creates or adopts in order to sign a document and that is in, attached to or associated with the document. The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) is somewhat narrower and focuses only on "secure electronic signatures," which is currently taken by the government to mean, essentially, an authentication process based on public key type encryption.

In addition to writing and signature rules, most provincial electronic commerce statutes provide that an offer, an acceptance or any other matter material to the formation or operation of a contract may be expressed by electronic information or by an act intended to result in electronic communication, such as touching or clicking an appropriate icon or other place on a computer screen or even by speaking. These rules are useful because they confirm that contracts made over the Internet will not be unenforceable simply because they were concluded electronically. There is jurisprudence in Canada supporting the enforceability of "express-click consent" agreements. Where a user is not required to click "I agree" expressly, but rather where the terms say,

for example, that using the website denotes consent to the terms, there is less certainty as to enforceability.

Anti-spam, Anti-spyware

The federal government enacted Canada's *Anti-Spam Act* (CASL) in December 2010. CASL came into force in 2014. It is widely considered to be one of the most stringent anti-spam laws in the world. The legislation implements a broad range of requirements intended to reduce spam, identity theft, phishing and spyware. Unlike the U.S. *CAN-SPAM Act*, which allows businesses to send commercial electronic messages to individuals without prior consent so long as the message contains a valid unsubscribe mechanism, CASL requires businesses to obtain valid consent prior to sending even the first commercial message to intended recipients. Violations of CASL may be subject to administrative monetary penalties of up to C$1 million for individuals and C$10 million for other offenders. Commencing in 2017, CASL provisions that implement a private right of action will come into force pursuant to which businesses and consumers will be granted a right to take civil action against violators of the law to recover damages.

Many industry groups consider parts of the legislation to be overreaching because: a) the law governs all forms of "commercial electronic messages" (not merely misleading or bulk e-mails used for direct marketing); and b) the law imposes an "opt-in" consent requirement and detailed disclosure requirements to both the delivery of "commercial electronic messages" and to the installation of computer programs on another person's computer system (whether or not the computer program might be considered "spyware" or "malware").

Since coming into effect, the Canadian Radio-television and Telecommunications Commission (CRTC), which is responsible for enforcing the law, has received over 750,000 complaints from Canadians; although it has rendered very few enforcement decisions thus far.

Cyber-Libel

Cyber-libel is posting a publication onto the Internet that is calculated to injure the reputation of another without lawful excuse. Recent Canadian court decisions have awarded significant damages to plaintiffs who were libelled by defendants sending defamatory e-mails and making other similar online postings about plaintiffs. The case law is developing

to minimize potential liability of responsible hosts of online discussion forums.

Jurisdiction

In the criminal, quasi-criminal and regulatory arenas, Canadian courts and regulators seem to have little hesitation assuming jurisdiction over foreign-originated Internet-related conduct they view as harmful to the public good, so long as there is a real and substantial connection to the court's or regulator's own jurisdiction.

Criminal Law

In general, the Canadian government has made useful strides in combating computer crime by continuously amending the *Criminal Code of Canada* over the past 20 years to keep pace with perpetrators of computer-related crime. However, the Internet and other computer-based technologies and business practices raise a number of novel questions under these amendments, as well as the older provisions of the *Criminal Code of Canada*, highlighting (among other challenges) the difficulty in enforcing a national criminal law in an increasingly global technology environment. As technology evolves, the applicability of the *Criminal Code of Canada* to certain harmful behaviour remains in question.

FOR MORE INFORMATION, PLEASE CONTACT:
Charles S. Morgan
514-397-4230
cmorgan@mccarthy.ca