INFORMATION TECHNOLOGY

By Mike Scherman, Jamie Parker, Oksana Migitko, Connor Bildfell and Keith Rose

INFORMATION TECHNOLOGY

Export Control of Technology

In Canada, the control of exports in technology falls within the mandate of the federal government. Export of certain hardware, software, and technology may be controlled by means of the *Export and Import Permits Act* (EIPA). These controls apply not just to physical shipments, but also to transfers by intangible means, including through the provision of services or training, server upload, downloads or access from abroad, other electronic file transfers, emails, faxes, telephone conversations, teleconferencing, and face-to-face meetings. Further, restrictions on export or transfer of certain goods, software, and technology are imposed under the sanctions laws, including the *United Nations Act* and the *Special Economic Measures Act.* In some cases, economic sanctions may overlap with export controls, however, they generally apply more broadly, including in circumstances where there is no export or transfer of restricted goods, software, or technology from Canada.

Established under the EIPA, the Export Control List (ECL) identifies those goods, software, and technology, including high-tech items, that may not be exported or otherwise transferred from Canada by tangible or intangible means without first obtaining an export permit, subject to exemptions for certain destination countries. The ECL is not product specific and instead provides a set of technical specifications that are technology-neutral for the most part and are functional in their description. Currently, the ECL contains controls pertaining to items with cryptographic functionality, intrusion software, items for defeating, weakening or bypassing information security, and surveillance items for monitoring or analysis by law enforcement of content of communications or metadata. 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

Various legislative initiatives have provided more legal certainty to doing business online. In Ontario, for example, the *Consumer Protection*

Act, 2002 (CPA) includes provisions germane to online commerce, where a large number of Canadian consumers buy and sell goods and services, though they apply generally outside e-commerce as well. See **Manufacture and Sale of Consumer Goods — Consumer Protection**.

Suppliers are deemed to warrant, for example, that services supplied under a consumer agreement be of "a reasonably acceptable quality." The CPA also extends the implied warranties in the *Sale of Goods Act* to goods that are leased or traded. Another important provision invalidates any requirement in a consumer contract compelling disputes to be submitted to arbitration, which some merchants use to try 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 in a manner that is "clear, comprehensible and prominent," as well as "accessible." In addition, the merchant must provide the consumer with an express opportunity to accept or decline, and correct errors in, the internet agreement immediately before entering into it and must provide a copy of the internet agreement to the consumer within 15 days after the consumer enters into that agreement. Finally, the CPA sets out rules for prepaid 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 prepaid cards have been adopted in the majority of Canadian provinces.

Notably, consumer protection laws are currently in flux and businesses should be aware of the changing consumer protection landscape in Canada. For example, Ontario is looking at significantly changing the CPA with changes to contract disclosure and consent requirements and prohibiting certain contract terms,[1] while Québec proposed legislation on June 1, 2023 that amends its consumer protection rules to prohibit the sale of goods with planned obsolescence and to introduce a legal warranty of good working order for certain commonly used new goods.[2]

1 https://www.mccarthy.ca/en/insights/blogs/consumer-markets-perspectives/ontario-issues-consultation-paper-consumer-protection-legislation.
2 https://www.mccarthy.ca/en/insights/blogs/consumer-markets-perspectives/government-proposes-changes-consumer-protection-act-ban-planned-obsolescence.

Evidence Laws

Most jurisdictions in Canada have adopted rules of evidence that specifically address electronic documents. These statutes generally require the best-evidence rule to be satisfied in respect of electronic documents, by proof of the integrity of the electronic documents system by which the documents were recorded or preserved. These provisions also allow the integrity of the electronic documents system to be inferred from evidence that the underlying electronic device was operating properly. In short, these amendments support the admissibility of electronic documents, while still permitting a party to challenge the reliability of the computer system or network that produced the documents.

In the digital era, strict and literal compliance with litigation discovery rules, such as Rule 30 of the *Rules of Civil Procedure* (Ontario), would often prove expensive, overwhelming, and in large measure unhelpful to litigants. Therefore, judges in Canada are increasingly receptive to having litigants follow e-discovery guidelines. These guidelines may require, for example, that litigants consider e-discovery issues and, among other things, circumscribe the scope of e-discovery in order to comply with Rule 30. See **Dispute Resolution — Electronic Discovery**. In addition, the COVID-19 pandemic has accelerated the adoption and use of new technologies in courts across Canada. Many Canadian courts have continued to mandate or encourage that all litigation documents be filed electronically with hyperlinks to relevant authorities and evidence.

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 email — 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

Canada's *Anti-Spam Legislation* (CASL) 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 provided 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. Since coming into effect, the Canadian Radio-television and Telecommunications Commission (CRTC), which is responsible for enforcing CASL, has received numerous complaints from Canadians; although it has rendered few enforcement decisions thus far. Notably, in at least one instance, the CRTC has held an individual liable under CASL for violations committed by a corporation. In April 2019, the CRTC imposed an administrative monetary penalty (AMP) of $100,000 on a director of a corporation in relation to commercial electronic

messages sent to recipients in Canada. In coming to this decision, the CRTC assessed the director's ability to pay, his experience with email distribution platforms, and the importance of this method of marketing to his business. The CRTC emphasized that the purpose of a penalty is to promote compliance with CASL and imposed the $100,000 fine to ensure this specific director would comply with CASL in any of his future endeavours.

Anti-spyware/Cookies

Under s. 8 of CASL, businesses normally require consent if they utilize programs that install software or other programs on a user's computer system. CASL mandates that a request for express consent must state the purpose for why consent is sought and the function of the computer program, the name of the entity seeking consent, and the mailing address and telephone number or email address for the entity that is seeking consent. However, for certain types of programs such as cookies, you are considered to already have express consent to save information from users without a request as long the user's conduct made it reasonable to believe they consented to the program's installation. For example, you are not considered to have consent to install cookies on a user's computer system, if that user disables them in their browser.[3]

It should be noted that as of September 22, 2023 under Québec's amended privacy law, technologies that collect personal information and that allow an individual to be identified, located or profiled must be deactivated as the default option, and the individual must be notified of the use of such technology and the means available to activate the functions that allow them to be identified, located or profiled.

Cyber-libel

Cyber-libel is publishing information that harms another's reputation through a computer system without lawful excuse. Recent Canadian court decisions have awarded significant monetary awards to plaintiffs who were libelled by defendants sending defamatory emails and making other similar online postings about plaintiffs. Cyber-libel can come in a various forms. In February 2021, the Ontario Superior Court of Justice even awarded a novel remedy for the "tort of internet harassment," making it the first common law court outside of the U.S. to do so.[4]

3 Ibid.
4 https://www.mccarthy.ca/en/insights/blogs/techlex/tort-internet-harassment-new-tort-extraordinary-remedy.

The case involved the dissemination of spurious and damaging accusations posted online by the defendant about the plaintiff. Because the court concluded that previously recognized torts such as defamation, intrusion upon seclusion (invasion of privacy), and intentional infliction of mental suffering were inadequate for the facts of the case, it recognized the tort of internet harassment.[5]

Further cyber-libel case law is also developing to minimize potential liability of responsible hosts of online discussion forums. Generally, an internet host will be treated as a non-publisher (passive instrument) until a potential plaintiff provides notice that they were libelled on the host's site. If the host fails to remove the content after notice, the court may decide that the host is liable by omission.[6]

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.

Organizations must be transparent about their personal information handling practices. This includes advising customers that their personal information may be sent to another jurisdiction for processing, and that while the information is in another jurisdiction, it may be accessed by the courts, law enforcement, and national security authorities. Additionally, transfers of personal information outside Québec (including to another province) require additional obligations, such as assessments of privacy-related factors prior to transfer.

Criminal Law and Ransomware

In general, the Canadian government has made useful strides in combating computer crime by continuously amending the *Criminal Code* 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

5 https://www.canlii.org/en/on/onsc/doc/2021/2021onsc670/2021onsc670.html?resultIndex=1#document at para 171.

6 Emily B Laidlaw and Hilary Young, Internet Intermediary Liability in Defamation, 2019 56-1 Osgoode Hall Law Journal 112, 2019 CanLIIDocs 3965 at page 122, https://canlii.ca/t/sqlp.

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.

The Canadian Centre for Cyber Security leads the Government's response to cybersecurity and lists ransomware as one of the most common forms of cyber attacks in Canada.[7] Ransomware is a type of malicious software used by cyber criminals to infect a device and hold its files and data for ransom. Once a computer or network is infected with ransomware, the software is capable of restricting access to the system or encrypting data from it.

The idea that cyberattacks only target "businesses of data" with ransomware is incorrect. All companies have data in their systems and cyber criminals have begun to target non-data businesses as well.[8] Consequently, it is important to properly manage the risk of ransomware by ensuring the proper precautionary steps are taken before an incident occurs. Businesses can be proactive by establishing a strong cybersecurity framework composed of organizational resources that can assess and mitigate cybersecurity risks such as ransomware.[9] Proper risk management also includes formulating cybersecurity response plans to the occurrence of a ransomware attack. The plan should address specific concerns such as the decision to pay the ransom or not and delineating a point in time where it might be necessary to involve external counsel and consultants.[10]

Artificial Intelligence (AI)

AI is actively changing the way business is conducted in Canada and around the world. AI encompasses a wide range of technologies, from chatbots and decision-making tools to software that generates entire documents, pictures and other content. Although provincial and federal governments are considering and developing AI regulations, only Québec (as of September 22, 2023) has legislation in force that directly addresses AI, and in that case only to the limited extent of requiring

7 https://cyber.gc.ca/en/ransomware-dont-get-locked-out.
8 https://www.mccarthy.ca/en/insights/blogs/techlex/emerging-developments-ransomware.
9 https://www.mccarthy.ca/en/insights/blogs/techlex/ransomware-avoidance-and-response.
10 Ibid.

organizations to make certain disclosures in connection with decisions they make that are based exclusively on automated processing of an individual's personal information.

The Federal Government has proposed the *Artificial Intelligence and Data Act* (AIDA) to regulate the design, development and use of AI in the private sector,[11] which is expected to come into force no sooner than 2025.[12] AIDA leaves many details to be set out in future regulations, and consultations with stakeholders during that time may change AIDA significantly from its current state. As proposed, among other obligations, AIDA will impose significant compliance obligations on those responsible for "high-impact" artificial intelligence systems (which are yet to be defined) and gives the Minister of Innovation, Science and Economic Development broad powers to enforce violations of AIDA, including maximum fines of the greater of C$10 million or 3% of gross global revenue. While the ultimate form and effect of AIDA is difficult to predict, the AI space will continue be a significant target for regulation and will likely have a substantial impact on the way that many organizations conduct their business in the near future.

FOR MORE INFORMATION, PLEASE CONTACT:

Christine Ing
christineing@mccarthy.ca
416-601-7713

Michael Scherman
mscherman@mccarthy.ca
416-601-8861

11 https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading.
12 https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document.