




14.

---

Information and  
Communications  
Technology



Companies wishing to conduct business in the Canadian information technology and communications sectors will need to address a number of legislative and regulatory requirements. This chapter aims to cover key legislative and regulatory considerations relating to Canadian information technology and communications law.

## E-commerce Legislation

Each province and territory has its own version of 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 three objectives: first, to ensure that contracts to which the legislation applies (some contracts, such as wills or contracts involving the sale or financing of real estate, are excluded) are treated in largely the same manner as contracts formed in offline formats, provided certain criteria are met; second, to establish when electronic documents will meet a statutory requirement for a document to be in writing, to be provided in writing, to be provided in a specified non-electronic form, or to be retained; and third, to establish that a legal requirement that a document be signed can be satisfied by an electronic signature that meets certain criteria.

For the province of Québec, the *Act to Establish a Legal Framework for Information Technology* (AELFIT) was enacted in 2001 by Québec's National Assembly for the purpose of modernizing and standardizing the legal treatment of technology-based communications and documents. It establishes a legal foundation for the use of digital documents, electronic signatures, and other technology-driven practices in both the public and private sectors by ensuring that electronic documents have the same legal validity as paper documents, under specified conditions. Finally, the AELFIT establishes a legal framework for the use of specific technologies by setting requirements for systems such as biometrics, digitization, geolocation, identification, authentication, and electronic signatures.

## CASL – Canada's Anti-Spam Legislation

Canada's anti-spam legislation (formally titled "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*", but informally and better known as CASL) has now been in force for over a decade.

CASL has significant impact on the use of electronic messages to promote activities or contact past or prospective clients or business partners, and on the installation of software on third party computer systems.




## CASL:

- Aims to address the problem of unsolicited electronic communications (i.e., spam) in the form of commercial electronic messages (CEMs)
  - Introduces rules to address the problem of unsolicited installed software programs (UIPs), which include cookies (even if their designation as software programs is technically debatable), and rules to address the unauthorized alteration of transmission data
  - Provides a set of rules to follow to obtain valid consent to send CEMs and install software programs, including specific procedural and content requirements for consent, as well as various categories of implied consent and certain exceptions to the consent requirement
  - Imposes various requirements regarding certain content that must be included in a CEM, including the identification of the person or entity sending the message and an unsubscribe mechanism that meets certain criteria, and sets out a strict and sometimes complex regime for giving effect to unsubscribe requests
  - Does not distinguish between messages sent for legitimate versus malicious purposes, nor between messages sent to a small number of recipients versus those sent in bulk
  - Sets out a framework that is significantly broader in coverage than its US or European counterparts, and is considered as one of the most stringent anti-spam regimes in the world
- **Application outside of Canada:** CEMs – for the CASL anti-spam requirements to apply, a computer system located in Canada needs to have been used to send or access the CEM, meaning foreign senders of CEMs into Canada are subject to this legislation; UIPs – for the UIP provisions to apply, either the computer system or the person (or person directing a person) who installs the UIP must have been in Canada at the relevant time, meaning foreign installers of UIPs on computer systems in Canada are subject to this legislation.
  - **Low threshold for application:** A CEM that is subject to the CASL anti-spam requirements is defined as any electronic message that “would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity” – a broad definition that includes more than what would otherwise 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 requirements 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: (a) an email address, (b) an instant messaging account, (c) a telephone account, or (d) “any similar account”.

The following are examples of some of the complexities that businesses need to address in seeking to comply with CASL:



- **Opt-in regime:** Unlike other anti-spam laws, including the US CAN-SPAM Act, CASL is an opt-in regime. With limited exceptions, CASL prohibits the sending of a CEM unless prior express or implied consent exists. Express consent must be obtained in a prescribed form under CASL. Implied consent is limited to certain enumerated categories, such as “existing business relationships” as defined in the legislation. In some categories of implied consent, the consent is only valid for a specified period of time. Requests for permission to send CEMs are also deemed to be CEMs, so organizations must carefully consider CASL requirements before sending any message to request consent to send CEMs.
- **Importance of relationship with recipient:** Depending on the sender’s relationship with the recipient, the CEM may be: (a) exempt from both the consent and message content requirements, (b) exempt from the consent requirements, or (c) subject to implied, 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 requirements, 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.
- **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 or 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. Also, a request for express consent must meet certain criteria in order to be valid. Businesses need to ensure that their requests for consent are designed in such a way that they comply with CASL.

- 
- **CEM content requirements are nuanced:** In addition to the consent requirements set out above, the CRTC has provided detailed guidance on the form and nature of required CEM content for a CEM to be compliant with CASL. For example, the CRTC's guidance includes details on how a sender of a CEM should identify third parties on whose behalf a CEM is being sent, as well as guidance on how an unsubscribe mechanism can be "readily performed" by the recipient of a CEM.

The consequences of violating CASL are significant. 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, and (d) injunctive relief. Notably, provisions providing for a private right of action that were to come into force on July 1, 2017, have been suspended indefinitely.

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 ten years since CASL came into effect, enforcement efforts have resulted in administrative monetary penalties and negotiated undertakings ranging from \$15,000 to \$200,000.

In addition to the provisions of CASL, enforcement activity by the CRTC has provided guidance on the manner in which organizations should conduct activities in order to mitigate potential administrative monetary penalties in the event of a CASL violation.

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 and UIP policies – and make any necessary amendments to their existing privacy policies.

A Canadian Radio-television and Telecommunications Commission bulletin issued November 5, 2018 (CRTC Compliance and Enforcement Information Bulletin 2018-415), provided general compliance guidelines and best practices for stakeholders with respect to the prohibition, under Section 9, to aid, induce, procure, or cause to be procured the doing of any act contrary to CASL requirements in respect of unsolicited CEMs or UIPs. It appears that Section 9 may apply to individuals and organizations who are (a) intermediaries that provide enabling services that allow someone else to violate CASL, or (b) receiving a direct or indirect financial benefit from such violations. Advertising brokers, electronic marketers, software and application developers or 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 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 CASL
- Evidence of reasonable steps taken to prevent or stop violations from occurring



## E-evidence Legislation

Canadian evidence legislation sets out the admissibility requirements for electronic documents (data recorded or stored in or by a computer system or similar devices). Mainly, the legislation seeks to adapt and codify the common law rules of authentication and “best evidence” for electronic evidence.

Under the *Canadian Evidence Act* (CEA), any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be. The goal at this stage is not to guarantee an e-document is genuine, it is merely to evaluate whether an e-document on its face seems to be what it is stated to be.

The “best evidence” rule acts as an “adjunct to authenticity”, providing light validation of a document’s integrity. Integrity, in this instance, refers to whether a document’s information likely remained complete and unaltered from input to submission in court. For e-documents, integrity for purposes of the “best evidence” rule is satisfied on proof of the integrity of the electronic document system by or in which the e-document was recorded or stored. This in turn, in the absence of evidence to the contrary, is proven by evidence capable of supporting a finding 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.


The thresholds for authenticity and best evidence are low, allowing for direct, indirect, and sometimes lay testimony as proof of admissibility. Importantly, however, ease of admissibility does not equate to high probative value in the eyes of the court. Judges retain the authority to evaluate the reliability and credibility of the evidence when making their final decision. Consequently, poor-quality e-documents admitted for consideration can still be deemed unreliable or insufficient in the end.

Having a reliable electronic document system not only helps with admissibility, but the methods used for storing, copying, transmitting, or reproducing the electronic records will also influence the weight e-documents carry in court.

The evidence legislation in other common law provinces and territories provides for a similar regime.

## Consumer Protection Legislation

Each province and territory of Canada has its own consumer protection regime consisting of legislation, rules and regulations, and in some cases the regimes vary considerably. 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 and certain actions be taken at certain times during the electronic contracting process).



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 requirements of the civil code of Québec such as those applying to contracts of adhesion, which are contracts in which the essential stipulations are imposed or drawn up by one of the parties and are non negotiable (e.g. online terms and conditions or “click-wrap” agreements). Significantly, limitations of liability provisions are not permitted under Québec’s *Consumer Protection Act*.

These regimes generally require that:

- a) Certain disclosures be (i) made to the consumer during the contracting process, and (ii) included in the actual contract
- b) The contract be in writing
- c) The consumer be given an opportunity to validate the transaction information prior to finalizing the purchase
- d) A copy of the contract be provided to the consumer within a prescribed period of time

In addition to a right to terminate the contract and other remedies available to the consumer, failure to properly follow these requirements can result in suppliers being liable to pay fines or penalties for a violation. Contraventions of provincial consumer protection statutes can, upon conviction, give rise to fines of \$100,000 - \$250,000 for a corporation’s first offence. Some provincial consumer protection statutes also contain administrative monetary penalties provisions that could give rise to penalties in lesser amounts. Directors of corporations found to have violated certain requirements under provincial consumer protection statutes 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” that 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.

In recent years, many provinces have updated their laws and regulations to respond to the evolving landscape of digital commerce and heightened sensitivity to consumer rights. For instance, Ontario passed into law a new *Consumer Protection Act, 2023* that builds on its previous legislative regime by, among other things, prohibiting a new set of unconscionable acts by suppliers and providing additional remedies to consumers, including a right to recover three times the refund amount in a civil action.



## Domain Names

Parties wishing to obtain a “.ca” domain name will need to satisfy the Canadian Internet Registration Authority’s Canadian Presence Requirements. Canada’s top-level domain name is generally available to citizens, permanent residents, companies incorporated in a Canadian jurisdiction, and partnerships registered in Canada, among others. In addition, the owner of a trademark registered in Canada has the right to a “.ca” domain name that includes the trademark.

## Website Accessibility

Most provincial accessibility statutes require that organizations ensure their websites meet certain accessibility standards or objectives. In Ontario, for example, organizations with fifty (50) or more employees are required under the *Accessibility for Ontarians with Disabilities Act* to ensure that their website meets Web Content Accessibility Guidelines (WCAG) 2.0 (Level AA) or later.

## IT Agreements and Contracting

Although there are no laws of general application focused primarily on the provision of IT services to the private sector in Canada, other Canadian laws will invariably apply to the provision of such services. These include laws and regulation relating to the processing and protection of personal information (both in the public and private sectors) and industry-specific regulations and guidelines (for example, requirements governing the provision and use of IT services by federally regulated financial institutions, discussed later in this chapter).

Also, companies seeking to license and commercialize information technologies in Canada should familiarize themselves with the Canadian intellectual property regime (see [Chapter 13](#)).


“Browse-wrap” or “click-wrap” licences may be enforceable if purchasers are made aware of the terms at the time of sale such that the purchaser was impressed with the knowledge of, and was given proper notice of, terms before the parties entered an agreement.

## French Language Requirements

Québec’s sole official language is French. As such, the Charter of the French Language, recently amended by Bill 96, imposes strict language requirements to promote the use of French in all aspects of public life, including commerce and business communications. While software may be sold in other languages if no French version exists, contracts of adhesion and product inscriptions must adhere to strict French language requirements. Contracts of adhesion, which are non-negotiable and drafted exclusively by one party (e.g. online terms and conditions), must be provided in French before parties can agree to be bound by a version in another language. Failure to comply with this requirement could render the contract null or unenforceable against the adhering party.

Product inscriptions—including packaging, user instructions, and any accompanying documents—must be available in French on equal terms as any version in another language. The same rule applies to commercial documentation such as catalogues and brochures on websites. Public signs and commercial advertisements must feature markedly predominant French text.





The *Office québécois de la langue française* (OQLF) oversees enforcement, typically favoring a collaborative approach, but may defer a matter for prosecution, where fines ranging from \$3,000 to \$30,000 can be imposed on a first offense. This framework underscores Québec’s dedication to preserving its linguistic heritage while providing businesses with clear operational guidelines.

## Artificial Intelligence

The Parliament of Canada is currently considering Bill C-27, legislation that would, among other things, enact the *Artificial Intelligence and Data Act* (AIDA).

AIDA and related initiatives from the Federal Government (discussed below) revolve around six principles: (i) accountability, (ii) safety, (iii) fairness and equity, (iv) transparency, (v) human oversight and monitoring, and (vi) validity and robustness. If passed into law, it would regulate the design, development, and use of AI systems in the private sector with a focus on mitigating the risks of harm and bias in the use of “high-impact” AI systems. Among other things, AIDA, as currently drafted, would do the following:

- Establish the criteria for high-impact AI systems to which the legislation will apply
- Establish requirements relating to conducting assessments of high-impact systems, establishing and monitoring risk mitigation measures, the use of anonymized data, record keeping, the publication of information about the AI system, and certain reporting obligations.
- Require the use of accountability frameworks by organizations that develop high-risk AI systems.
- Establish an enforcement regime,


including to establish and empower an Artificial Intelligence and Data Commissioner, prescribe administrative monetary penalties for non-compliance, the amount of which will be determined by future regulations, and set fines for specific offences under AIDA that could range up to the greater of \$25 million or 5 percent of the organization’s gross global revenues in the preceding year.

Parliamentarians proposed amendments to AIDA in November 2023 that would, among other things:

- Establish classes of presumptively high-impact AI systems (i.e., systems that relate to: (i) employment; (ii) determinations regarding access to services; (iii) biometric information processing; (iv) content moderation on social media services, search engines, and other online communication platforms; (v) healthcare or emergency services; (vi) court or administrative decision-making; and (vii) law enforcement).
- Introduce the concept of “general-purpose AI systems,” as distinguished from “high-impact AI systems,” and bring the general-purpose AI systems under AIDA’s regulatory scope.
- Further clarify accountability frameworks for organizations based on their roles and functions within the AI system lifecycle.

A companion document to AIDA published in March 2023, outlines a two-year period for regulation development. AIDA would only come into force after that period.

AIDA has completed second reading in the House of Commons and it is currently being considered by the House Standing Committee



on Industry and Technology (Committee), where the Government has detailed its intent to table wide-ranging amendments to AIDA. At the time of writing, it is unclear when and in what form AIDA will receive Royal Assent.

In September 2023, Innovation, Science and Economic Development Canada (ISED) published a “Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems” (the Code). The Code: (a) sets out voluntary measures for organizations developing and managing general-purpose generative AI systems to mitigate the risks posed by those systems; and (b) targets specific actors in the AI ecosystem, developers, and managers, who in accepting the Code’s voluntary commitments must reflect the six aforementioned principles (i.e., accountability, safety, fairness and equity, transparency, human oversight and monitoring, validity and robustness) in their work. Although its primary focus is advanced generative AI systems, the Code applies more broadly to a range of high-impact AI systems. The measures in the Code are intended to guide organizations in anticipation of binding regulations promulgated under AIDA.


In early 2024, the public consultation period closed for the Government of Canada’s “Consultation on Copyright in the Age of Generative Artificial Intelligence”. The intent of this consultation was to provide direction for future amendments to Canada’s *Copyright Act* in light of the rapidly expanding use of AI systems, including to consider whether AI systems can be considered owners of a work.

## Internet and other Telecommunications

Subject to limited exceptions, the provision of telecommunications services, including retail internet services, to residential and business customers is forborne from regulation in Canada. Exceptions include: (a) a Wireless Code that prescribes disclosure requirements and limits on consumer and small business wireless service contract terms, (b) an Internet Code applicable to designated large Internet Service Providers (ISPs) that prescribes disclosure requirements and limits on individual consumer contract terms for fixed internet services, (c) ISP internet traffic management rules, (d) number porting requirements, (e) customer transfer requirements, (f) accessibility obligations, (g) emergency service obligations, and (h) wholesale service obligations applicable to designated carriers.

Use of telecommunications services for telemarketing purposes is subject to do-not-call-lists and other restrictions. Use of automatic dial-announcing devices, or robocallers, is also very restricted. SMS or text-based marketing is governed by the CASL restrictions discussed earlier in this chapter.

Resellers of telecommunications services are not subject to foreign ownership restrictions. In limited circumstances, telecommunications carriers must be incorporated under the laws of Canada and may be subject to foreign ownership requirements (as described in Chapter 3).



## Requirements for Regulated Industries

The Office of the Superintendent of Financial Institutions (OSFI) is the Canadian federal regulator that supervises and regulates federally regulated banks and insurers, trust and loan companies, and private pension plans subject to federal oversight.

On May 1, 2024, OSFI's revised Guideline B-10 – Third Party Risk Management (the “Revised Guideline”) came into effect, replacing the previous long-standing Guideline B-10 – Outsourcing of Business Activities, Functions and Processes. The Revised Guideline sets out enhanced expectations for federally regulated financial institutions (FRFIs) in managing an expanded scope of third-party risks, and places greater emphasis on governance and risk management plans, and on specific outcomes and principles. The Revised Guideline expands the application of Guideline B-10 to “third-party arrangements”, which include any business or strategic arrangement with external entities. As such, the Revised Guideline will continue to apply to technology contracts, including (as expressly noted in the Revised Guideline): (i) relationships involving the provision of services for the storage, use or exchange of data; and (ii) generally, any outsourced activities, functions and services.

The Revised Guideline replaces the “materiality” threshold in the previous guideline, and introduces a new “risk-based approach”, which requires a more comprehensive risk-management framework that accounts for the level of risk and the “criticality” associated with individual third-party arrangements. It also includes more specific requirements for FRFIs to develop cloud-specific requirements and consider cloud portability in their contracting arrangements.

Guideline B-10 states that OSFI expects, as required under the *Bank Act*, the *Trust and Loan Companies Act* and the *Insurance Companies Act*, that certain records of FRFIs be maintained in Canada. In addition, a FRFI is expected to ensure that OSFI can access, in Canada, any records necessary to enable OSFI to fulfil its mandate.

While Guideline B-10 is directed at federal entities, it has also been voluntarily adopted by many provincially regulated entities in the financial sector. It is also of importance to entities providing products and services to FRFIs as they can expect FRFIs to negotiate contractual provisions to address Guideline B-10.

In addition to Guideline B-10, OSFI also released an advisory on Technology and Cybersecurity Incident Reporting, setting out OSFI's expectations in relation to the immediate and ongoing reporting of cybersecurity incidents, and which FRFIs should account for in their agreements with cloud providers. These expectations are in addition to the mandatory breach notification requirements under Canadian privacy laws.

In July 2022, OSFI released a final Guideline B-13 (titled “Technology and Cyber Risk Management”), which is intended to serve as a complement to existing guidelines, including Guideline B-10. Guideline B-13 is expected to be read, and implemented, from a risk-based perspective to allow FRFIs to compete effectively and take full advantage of digital innovation, while maintaining sound technology risk management. Guideline B-13 provides FRFIs with technologically neutral guidance to produce key “outcomes” in three domains:

- Technology, cyber governance and risk management
- Technology operations
- Cybersecurity.

Guideline B-13 came into effect on January 1, 2024.

## Research and Development

Technology companies looking to establish a presence in Canada should take note that Canada encourages research and development (R&D) activity through the Scientific Research and Experimental Development (SR&ED) program – an initiative of the federal tax authorities. It is the largest source of R&D support for taxpayers provided by the federal government. These tax credits often serve as an important benefit for technology companies, making Canada an attractive destination for companies seeking to conduct significant technology-related R&D activity. Under the SR&ED program, claimants can apply for investment tax credits for items like wages, materials, machinery, equipment, and contracts and even for a portion of company overhead.

To be eligible, a corporate claimant must be a Canadian-controlled private corporation (CCPC). Generally, a CCPC is a private corporation in which at least 50% of the registered shareholders with voting rights are held by Canadian residents. To put it another way, 50% of the corporation's shareholders can be non-residents, and there is no citizenship requirement.

CCPCs can earn a refundable investment tax credit of 35% on the first \$3 million of qualified expenditures. To qualify under the program, these expenditures have to have been made for SR&ED carried out in Canada. Beyond the initial amount, CCPCs can earn a non-refundable investment tax credit of 15%.

Other Canadian corporations that do not qualify as CCPCs are eligible for a 15% tax credit on qualified expenditures. These credits are non-refundable but can be used to reduce the tax burden payable to the tax authorities.

For more details on CCPCs, see [Chapter 7](#).

---

