COUNTRY COMPARATIVE GUIDES 2020

The Legal 500 Country Comparative Guides

Canada
TECHNOLOGY

Contributing firm

Baker McKenzie

Theodore Ling

Partner (Toronto) | theodore.ling@bakermckenzie.com

Karina Kudinova

IP/Technology Associate (Toronto) | karina.kudinova@bakermckenzie.com

Jessie Sheehan

Associate (Toronto) | jessie.sheehan@bakermckenzie.com

Nadia Rauf

IT/Communications research lawyer (Toronto) | nadia.rauf@bakermckenzie.com

This country-specific Q&A provides an overview of technology laws and regulations applicable in Canada.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

CANADA
TECHNOLOGY

1. What is the regulatory regime for technology?

At the federal level, various government departments and agencies share responsibilities in overseeing and enforcing compliance with the laws applicable to technology in Canada. Core among these are (i) Innovation, Science and Economic Development Canada ("**ISED**"), and its agency, the Canadian Intellectual Property Office ("**CIPO**"), (ii) Global Affairs Canada, (iii) the Canada Border Services Agency ("**CBSA**"), (iv) the Canadian Radio-television and Telecommunications Commission ("**CRTC**"), (v) the Office of the Privacy Commissioner of Canada ("**OPC**"), and (vi) the Competition Bureau. At the provincial level, the Information and Privacy Commissioner of Alberta, the Information and Privacy Commissioner for British Columbia, and the Commission d'accès à l'information du Québec ("**provincial commissioners**") enforce private sector privacy laws in their respective provinces. Sector- and industry-specific laws applicable to technology exist at the federal and provincial levels in Canada.

2. Are communications networks or services regulated?

The term "telecommunications service" is defined by the federal *Telecommunications Act* ("**TA**") as a service provided by means of telecommunications facilities and includes the provision in whole or in part of telecommunications facilities and any related equipment, whether by sale, lease or otherwise. The CRTC administers telecommunication and broadcasting regimes in Canada and has broad powers to regulate the telecommunication industry pursuant to the TA. ISED is responsible for the technical aspects of satellite use, as well as policies on the use of satellites in Canada. To this end, it licenses satellites for Canadian orbital positions, issues spectrum licenses, and approves earth stations used to communicate with satellites.

3. If so, what activities are covered and what licences or authorisations are required?

Under the TA, the offering and provision of telecommunications services is subject to any conditions imposed by the CRTC. Before offering or providing users with telecommunications, an organization must register with the CRTC. The TA also requires the licensing of telecommunications service providers that carry telecommunications traffic between Canada and another country. The licence application process is generally streamlined; licences are granted barring any clear reason to the contrary. The CRTC determines the term of the BITS licence, which is not to exceed 10 years.

The *Radiocommunication Act* also requires that anyone wishing to manufacture, import, distribute, lease, sell, or use radio equipment in Canada, ensures that devices are tested and certified to meet applicable technical standards.

4. Is there any specific regulator for the provisions of communications-related services?

The primary regulator for communications-related services is the CRTC. ISED is responsible for regulating telecommunications equipment, the technical aspects of satellite use, and spectrum licensing.

5. Are they independent of the government control?

The CRTC is an independent public authority. It reports to Parliament through the Minister of Canadian Heritage. As a federal government department, ISED is not independent.

6. Are platform providers (social media,

content sharing, information search engines) regulated?

In Canada, platform providers may, depending on the nature of the service, fall subject to the regulatory regime noted in s. 1. The OPC and provincial commissioners often regulate their activities. At the federal level, the OPC has a mandate under the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") to protect and promote the privacy rights of residents of Canada whose personal information is collected, used, or disclosed by private-sector organizations in the course of a commercial activity. The provincial commissioners enforce laws that are substantially similar to PIPEDA in Alberta, British Columbia, and Quebec. The OPC sometimes works in concert with its provincial counterparts. Platform providers are also often subject to the oversight of the Competition Bureau, the independent law enforcement agency responsible for administering and enforcing the *Competition Act*. The OPC and Competition Bureau's activities overlap when platform providers collect personal information through deceptive means, and in such cases they work in collaboration.

7. If so, does the reach of the regulator extend outside your jurisdiction?

Canadian regulators focus on activities in or related to Canada. The OPC and the Competition Bureau have legal jurisdiction over extraterritorial conduct and foreign parties if there is a real and substantial connection between the alleged conduct and Canada. This analysis generally comes down to whether the conduct directly or indirectly affected residents of Canada. They also may seek extraterritorial remedies if and when they are appropriate.

8. Does a telecoms operator need to be domiciled in the country?

Telecommunications service providers may be domiciled outside of Canada unless they are terrestrial network facilities whose owners earned more than 10% of Canadian telecommunications service revenues in a year ("Canadian carriers").

9. Are there any restrictions on foreign ownership of telecoms operators?

A Canadian carrier must be a Canadian-owned and controlled corporation incorporated or continued under the laws of Canada or one of its provinces. Additionally, 80% of the members of the board of directors of these carriers must be Canadian and at least 80% of the voting shares of the carrier must be beneficially owned by Canadians. Finally, the corporation cannot be otherwise controlled by non-Canadians. Telecommunications service providers whose annual revenues from the provision of telecommunications services in Canada represent less than 10% of the total annual market-wide revenues in Canada are exempt from these requirements.

10. Are there any regulations covering interconnection between operators?

The CRTC provides regulatory oversight related to interconnection between operators. The TA requires Canadian carriers to gain prior approval from the CRTC for any written or oral interworking agreement or arrangement with other telecommunications common carriers. This includes the interchange of telecommunications by means of telecommunications facilities between carriers, the management or operation of either or both of their facilities or any other facilities with which either or both are connected, or the apportionment of rates or revenues between the carriers. The CRTC may order a Canadian carrier to connect any of the carrier's telecommunications facilities to any other telecommunications facilities.

11. If so are these different for operators with market power?

The CRTC is authorized under the TA to make decisions on issues related to interworking agreements or arrangements between telecommunications carriers, which may involve conducting an established market power test to ensure that fair competition practices are effected within the telecommunications sector. The CRTC, through its decisions, emphasizes the necessity to allow for the exchange of local traffic among carriers and encourages competition in the local exchange services market.

12. What are the principal consumer protection regulations that apply specifically to telecoms services?

The CRTC, as part of its mandate, promotes compliance and enforcement of consumer protection regulations for the telecommunications sector, which include:

1. Unsolicited Telecommunications Rules which covers Telemarketing Rules, National Do Not

Call List Rules, and Automatic Dialing and Announcing Device Rules;
2. Canada's anti-spam legislation ("**CASL**"); and
3. Wireless Code, which applies to wireless contracts and aims to protect consumers of mobile wireless voice and data services.

The *Competition Act* applies to all false or misleading advertising in the communications industry including telemarketing fraud. It contains criminal and civil provisions aimed at preventing anti-competitive practices in the marketplace. The *Competition Act* provides for a private right of action for losses or damage suffered by any person as a result of offences in relation to competition. In certain circumstances, the Competition Bureau holds authority, in conjunction with the CRTC, to regulate the telecommunications sector. Specifically, the Competition Bureau oversees any offences of the *Competition Act*, including those applicable to exclusive dealing, tied selling, and other trade restraints.

13. What legal protections are offered in relation to the creators of computer software?

Original computer software programs are copyright material. The copyright exists whether or not its creators seek a certificate of registration of copyright to evidence ownership. Creators may also protect their computer software innovations via patent. To secure a patent, creators must satisfy the requirements of the *Patent Act*, namely that the innovation is new, useful, and non-obvious, and that it falls within the scope of a patentable subject matter, which are either things with physical existence or things that manifest a discernible effect or change.

14. Do you recognise specific intellectual property rights in respect of data/databases?

The Federal Court of Appeal confirmed in *Canada (Commissioner of Competition) v Toronto Real Estate Board 2017 FCA 236* that there are no specific intellectual property rights in respect of data or databases. General areas of law, like contracts, intellectual property, and privacy and confidentiality, determine control and ownership rights in data and databases. Under intellectual property law, copyright may protect original data and databases, but establishing originality for aggregations or compilations of data in databases is a highly contextual and factual determination.

15. What key protections exist for personal data?

In Canada, various data privacy and security laws have been enacted at the federal and provincial/territorial levels, which apply to private-sector entities, public sector-entities and health information custodians. The *Privacy Act* covers the federal government's handling of personal information. Every province and territory also has laws applicable to their own provincial governments and agencies handling of personal information. The federal PIPEDA covers how businesses collect, use, and disclose personal information in the course of commercial activities across Canada, except in provinces that have adopted substantially similar privacy legislation (namely Quebec, British Columbia, and Alberta).

16. Are there restrictions on the transfer of personal data overseas?

Generally speaking, Canadian privacy laws do not prohibit organizations from transferring personal information to an organization in another jurisdiction for processing. The OPC has published guidance titled *Guidelines for processing personal data across borders,* which state that an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. Under the guidelines, organization must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. This means that the transferring organization must satisfy itself that the third party has policies and processes in place to ensure that the information in its care is properly safeguarded at all times. Organizations should also maintain the right to audit and inspect third parties' handling and storage of the transferred personal information, and exercise this right when warranted. Before transferring personal information overseas, organizations need to make it plain to individuals to whom the information relates that their personal information may be processed in a foreign country and that it may be accessible to law enforcement and national security authorities of that jurisdiction.

17. What is the maximum fine that can be applied for breach of data protection laws?

Fines for breach of data protection laws vary depending on the applicable law, and the nature of the specific circumstances resulting in the fine. Generally speaking, under the federal PIPEDA, Alberta *Personal Information*

Protection Act ("**Alberta PIPA**"), and British Columbia *Personal Information Protection Act* ("**BC PIPA**"), and Quebec's *Act Respecting the Protection of Personal Information in the Private Sector* ("**Quebec Act**"), organizations that commit certain offenses may be subject to fines of up to CAD 100,000.

18. What additional protections have been implemented, over and above the GDPR requirements?

Canadian privacy laws have been deemed by the European Commission to offer an adequate level of data protection.

19. Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?

While Canadian private sector privacy laws do not contain provisions that explicitly regulate cloud services they do establish rules governing the use of third parties in processing personal data—particularly with respect to obtaining consent for the collection, use and disclosure of personal information, securing the data, and ensuring accountability for the information, and transparency in terms of its practices. Transferring organizations should consider what information will be stored in the cloud and why, further taking into account the sensitivity of the personal information and carefully assessing all the risks and implications involved in outsourcing personal data to the cloud. Similarly, organizations should consider potential data security issues when evaluating a cloud provider and negotiating contracts or reviewing terms of service. In implementing cloud infrastructure, the organization is still accountable for the information at the hands of its service provider, and as such, should use contractual or other means to provide a comparable level of protection while the information is being processed and stored by the third party.

20. Are there specific requirements for the validity of an electronic signature?

In Canada, the validity of electronic signatures is governed by electronic contracts legislation including electronic transactions as well as, traditional common law principles and legislation applicable to contracts generally. All of the Canadian provinces and territories have enacted electronic transaction statutes. With the exception of Quebec, these statutes are significantly based on the model *Uniform Electronic Commerce Act* ("**UECA**"), adopted by the Uniform Law Conference of Canada in 1999, which establishes the principle that information shall not be denied legal effect or enforceability solely by reason that it is in electronic form. The requirements for the validity of an electronic signature are not uniform across the different provincial and territorial electronic transaction statutes.

21. In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?

Canada does not specifically regulate outsourcing transactions. Transfers of employees, assets or third party contracts are subject to contractual arrangements for the outsourcing transaction. Depending on the subject matter, the outsourcing transaction may be governed by specific federal/provincial laws or sector specific regulations. For example, private sector employee transfers are subject to provincial employment statutes. There are also sector specific regulations for the financial and health sectors such as, the Office of the Superintendent for Financial Institutions' ("**OSFI**") *Memorandum on New Technology-based Outsourcing Arrangements*. For the telecommunications sector, there are not any sector-specific regulations for outsourcing services.

22. If a software program which purports to be a form of A.I. malfunctions, who is liable?

The liability for AI malfunctions will be subject to terms of the software licensing agreement, which includes the provision of any AI. Typically, for these types of agreements, service providers aim to limit their liability. In the absence of adequate contractual protections or in the event of a dispute, the liability for damages from software malfunction may be attributed to any party involved in the product lifecycle of the software including development, manufacturing, and distribution. Canadian common law principles of contract and tort, product liability laws, and consumer protection laws may apply for actions for damages from software malfunctions. Product liability in all provinces is subject to common law principles of contract and tort with the exception of Quebec, where civil law principle of extra-contractual liability would be applicable.

23. What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of

hacking/DDOS attacks?

a) Generally speaking, Canadian privacy laws obligate organizations to protect personal information against loss, theft, or any unauthorized access, disclosure, copying, use, or modification. A basic principle of PIPEDA requires the protection of personal information by appropriate security relative to the sensitivity of the information.

Mandatory private-sector breach notification requirements for breaches of personal data other than personal health data exist under PIPEDA and Alberta PIPA. The British Columbia PIPA and the Quebec Act, do not require notification, but is a best practice. Similarly, the federal *Privacy Act* and various provincial public sector privacy laws require breach notification to impacted individuals and the applicable commissioner.

CASL also contains provisions governing software installation in the course of commercial activities, including prohibition aimed at viruses and spyware. Finally, there are sector specific laws and regulations that may include protection of personal information, such as provisions of the *Bank Act*, which regulate the use of personal information by federally regulated financial institutions.

b) The federal Criminal Code prohibits hacking and denial-of-service attacks under the crime of mischief in relation computer data. In this context, mischief involves either wilfully destroying or altering computer data, rendering it meaningless, useless, or ineffective, obstructing, interrupting or interfering with the lawful use of computer data or with a person in the lawful use of computer data, or denying access to computer data to a person who is entitled to access to it.

24. What technology development will create the most legal change in your jurisdiction?

Cloud migration, artificial intelligence ("**AI**"), financial technology, data monetization, and smart communities which leverage connected and shared data across platforms, will drive significant legal change in Canada. The increasing and innovative use, sharing, and transfer of personal data facilitated through technological developments will require constant focus on the adequacy of data protection measures offered through privacy legislation. The Government of Canada is actively engaged in consulting with appropriate stakeholders on establishing a legislative framework for the open banking space, modernizing the financial technology regulatory environment, and addressing privacy risks associated with the use of artificial intelligence related solutions. The concept of contractual liability and consumer protection with regards to these technological developments will also require further evaluation in areas such as, data sharing in the open banking sector.

25. Which current legal provision/regime creates the greatest impediment to economic development/ commerce?

Canada has had one of the world's most protected telecommunications sectors. Since 1993, Canada's TA has significantly restricted foreign ownership in the sector to protect Canadian identity and sovereignty. In 2012 and 2014, the federal government abolished these rules for telecommunications companies with a market share of less than 10 percent. In practice, the foreign ownership rules still impede new market entrants from challenging incumbents. The country's largest telecommunications companies remain protected, and so competitive intensity in the sector remains low. Barriers to universal service and service affordability continue to impede Canada's economic growth, and disproportionality impact lower income and rural residents of Canada.

26. Do you believe your legal system specifically encourages or hinders digital services?

The Canadian legal system is bijural, combining civil and common law, and bi-jurisdictional, dividing legislative powers between the federal and provincial governments. This complexity has created substantial barriers to interprovincial trade and labour mobility across the country, which continues to hinder economic growth and innovation. Recognizing the need improve prospects for Canada's long-term economic development in the digital age, Canada's federal, provincial and territorial governments negotiated the Canadian Free Trade Agreement ("**CFTA**"). Since the CFTA's entry into force on 1 July 2017, legislators and policymakers across the country have coordinated efforts at regulatory harmonization and modernization. These efforts at modernizing internal trade rules and reconciling regulatory differences across jurisdictions that act as barriers to trade were specifically designed to promote innovation and economic development. Under the CFTA, almost all areas of economic activity in Canada are covered unless explicitly excluded from the commitment to regulatory harmonization. Emerging digital services will benefit greatly since the development of new regulatory regimes for emerging digital services are

automatically covered by CFTA's rules and processes.

27. To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?

The regulation of artificial intelligence in Canada requires further development. The Government of Canada is engaged in advancing legislation related to the use of artificial intelligence across various industries such as, financial services and government services. The Department of Finance Canada released recommendations in January 2020 for the future of consumer-directed financial services including risk mitigation practices through the use of secure technology which meets requirements for cyber security, privacy and consumer protection. On 1 April 2019, the Government of Canada issued a *Directive on Automated Decision-Making* which applies to federal government departments that seek to utilize artificial intelligence to make, or assist in making, administrative decisions to improve service delivery. Companies providing the federal government with artificial intelligence technologies for automated decision making must consider the requirements under this Directive.

The OPC is developing legislative reform policy for federal privacy laws, which includes regulating artificial intelligence as it relates to PIPEDA. Currently, PIPEDA does not address the risks associated with the use of AI systems such as, the ability to rapidly process and analyse voluminous amounts of personal information. Since AI systems can be used for making predictions and decisions affecting individuals, there are associated privacy risks as well as risks of unlawful bias and discrimination.

Contributors

Theodore Ling
Partner (Toronto)
theodore.ling@bakermckenzie.com

Karina Kudinova
IP/Technology Associate (Toronto)
karina.kudinova@bakermckenzie.com

Jessie Sheehan
Associate (Toronto)
jessie.sheehan@bakermckenzie.com

Nadia Rauf
IT/Communications research lawyer (Toronto)
nadia.rauf@bakermckenzie.com