Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers

Canada: Law & Practice

April Gougeon, Bill Hearn and Ronald Davis
Fogler Rubinoff LLP

practiceguides.chambers.com

CANADA

Law and Practice

Contributed by:
April Gougeon, Bill Hearn and Ronald Davis
Fogler Rubinoff LLP see p.24

Contents

1. Basic National Regime

1.1 Laws

As a federal state with law-making powers shared between federal and provincial/territorial governments, Canada has both federal and provincial/territorial privacy laws that govern the private and public sectors.

Federal Privacy Laws

Canada has two federal privacy laws:

- the Personal Information Protection and Electronic Documents Act, SC 2000, c 5 (PIPEDA); and
- the Privacy Act, R.S.C., 1985, c. P-21.

Both statutes are overseen by the Privacy Commissioner of Canada. The Commissioner is an independent agent of Parliament and heads the Office of the Privacy Commissioner of Canada (OPC).

PIPEDA applies across Canada, unless an organisation is operating in a province with substantially similar legislation. There are at present three such provinces (see below). PIPEDA also applies to organisations outside Canada, if there is a real and substantial connection to Canada.

PIPEDA regulates the private sector. It governs the collection, use, and disclosure of personal information in commercial activities. PIPEDA aims to balance an individual's right to privacy with an organisation's need to collect, use, and disclose personal information. PIPEDA is considered to be technology neutral; ie, it applies regardless of the technology employed.

PIPEDA also applies to federally regulated entities known as "FWUBs": federal works, undertakings or businesses. FWUBs include airports, airlines, banks, inter-provincial and international transportation companies, telecommunications companies, and radio and television broadcasters. PIPEDA's coverage here extends to personal information about FWUBs' employees and applicants for employment.

Finally, PIPEDA (Schedule 4) lists organisations to which it applies. At this writing, only the World Anti-Doping Agency is listed.

PIPEDA does not generally apply to charities and non-profit organisations. It may apply to them, however, if they engage in a commercial activity, for example, in selling, bartering, or leasing donor, membership or other fundraising lists.

The Privacy Act is a limited statute in that it applies only to government institutions and Crown corporations.

Provincial Private Sector Privacy Laws

Three provinces have private sector privacy laws considered substantially similar to PIPEDA:

- British Columbia – Personal Information Protection Act, SBC 2003, c 63 (BC PIPA);
- Alberta– Personal Information Protection Act, SA 2003, c P-6.5. (AB PIPA); and
- Québec – an Act to modernise legislative provisions as regards the protection of personal information, SQ 2021, c 25 (Québec's Private Sector Privacy Act, recently updated with the passing of Bill 64–also known as Law 25). See **1.7 Key Developments**.

Provincial Personal Health Information Laws

Some provinces have passed personal health information (PHI) laws. The provincial PHI statutes considered substantially similar to PIPEDA are:

- Ontario – Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A, overseen by the Office of the Information and Privacy Commissioner of Ontario (IPC ON);
- Newfoundland and Labrador – Personal Health Information Act, SNL 2008, c P-7.01., overseen by the Office of the Information and Privacy Commissioner for Newfoundland and Labrador (OIPC NFL);
- Nova Scotia – Personal Health Information Act, SNS 2010, c 41 administered by the Information and Privacy Commissioner of Nova Scotia (IPC Nova Scotia); and
- New Brunswick – Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05, overseen by New Brunswick Office of the Ombud (NB Ombud).

Alberta, Manitoba, Saskatchewan, Yukon, and the Northwest Territories have also passed PHI statutes but they have not been recognised as substantially similar to PIPEDA. Still, these statutes (which, with respect to personal health information (PHI) and to the extent they increase obligations on organisations handling PHI, effectively replace PIPEDA) must be complied with in those jurisdictions.

Provincial Public Sector Privacy Laws

All Canadian provinces and territories have privacy and/or access laws governing provincial-level government institutions or public bodies.

1.2 Regulators

Privacy Commissioner of Canada

The federal Privacy Commissioner of Canada is an agent of Parliament, appointed by the Governor in Council under the federal Privacy Act. The Privacy Commissioner is independent of Parliament, and reports to it directly, not through a federal minister.

Provincial Privacy Authorities

The provincial and territorial privacy authorities in Canada are:

- Office of the Information and Privacy Commissioner of Alberta (OIPC AB);
- Office of the Information and Privacy Commissioner of British Columbia (OIPC BC);
- Office of the Ombudsman Manitoba;
- NB Ombud;
- OIPC NFL;
- Information and Privacy Commissioner of the Northwest Territories;
- IPC Nova Scotia;
- Information and Privacy Commissioner of Nunavut;
- IPC Ontario;
- Information and Privacy Commissioner of Prince Edward Island;
- *Commission d'accès à l'information du Québec* (CAI);
- Information and Privacy Commissioner of Saskatchewan; and
- Ombudsman and Information and Privacy Commissioner of the Yukon.

1.3 Administration and Enforcement Process

PIPEDA

The OPC has the authority to investigate complaints made under PIPEDA in two circumstances:

- a complaint: where an individual has filed a complaint with the OPC alleging a contravention; or
- a Commissioner-initiated investigation: the Commissioner initiates an investigation if satisfied that there are reasonable grounds to investigate a matter.

Complaints can be declined or discontinued by the OPC for various reasons, including:

- the complaint could be more appropriately dealt with by another procedure under Canadian law;
- the organisation has provided a fair and reasonable response to the complaint; or
- the matter is already the object of an ongoing investigation.

Section 12 of PIPEDA lists further grounds for declining or discontinuing an investigation.

The Privacy Commissioner has an array of investigative powers, but no ability to impose administrative monetary penalties. At the end of an investigation, the Privacy Commissioner may make recommendations in a Report of Findings and make that report public.

Investigation respondents and complainants both have recourse to the Federal Court of Canada. In some cases, the Court has awarded damages for breaches of PIPEDA. However, these awards have been well below penalties issued in Europe under the General Data Protection Regulation (GDPR) or in the United States under the Federal Trade Commission Act.

PIPEDA also contains offense provisions for some violations, such as failing to report a breach to the Privacy Commissioner or obstructing an investigation or audit. Under PIPEDA (as well as the Alberta PIPA and BC PIPA), offending organisations may be subject to fines of up to CAD100,000.

Privacy Act

Under Section 29 of the Privacy Act, the OPC carries out impartial investigations of complaints against federal government institutions for matters within the OPC's mandate.

When received, a complaint is screened and assigned to an investigator. Investigators have the authority to receive evidence, enter premises where appropriate, and examine or obtain copies of records found on any premises during an investigation.

The OPC has flexibility in conducting investigations. Depending on the complaint, it can encourage an early resolution process, an expedited proceeding where no formal findings are issued.

For more complex cases, the OPC carries out a standard investigation, and issues a Report of Findings at the end.

The recommendations from an investigation are limited to achieving compliance with the Privacy Act. Since the OPC does not have order-making powers in its role as ombuds, it cannot force institutions to take specific actions to remedy the complaints.

Individuals unsatisfied with the outcome can apply to the Federal Court under the Privacy Act to review the findings where there has been a denial of access to personal information.

1.4 Multilateral and Subnational Issues

See **1.1 Laws** for how the national systems relates to subnational legislation.

Canada participates in several international organisations related to privacy:

- Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR);
- Global Privacy Assembly (GPA);

- Asia Pacific Privacy Authorities (APPA);
- *Association francophone des autorités de protection des données personelles* (AFAPDP);
- Global Privacy Enforcement Network (GPEN); and
- Organisation for Economic Co-Operation and Development (OECD)'s Working Party on Security and Privacy in the Digital Economy (SPDE).

1.5 Major NGOs and Self-Regulatory Organisations

NGOs

The major privacy or data protection non-governmental organisations are as follows.

- Canadian Civil Liberties Association (CCLA)–an independent, national, nongovernmental organisation, working in the courts, before legislative committees, in the classrooms, and in the streets, protecting the dignity and rights of people in Canada. Among other things, the CCLA advocates for privacy laws that recognise privacy as a fundamental human right.
- Public Interest Advocacy Centre (PIAC)–a national not-for-profit corporation and a federally registered charity that aims to protect consumers' interests in various industries, including privacy.
- Centre for Digital Rights (CDR)–a Canadian non-partisan, not-for-profit organisation that aims to promote awareness of digital issues related to the data-driven economy by (i) advancing the public's understanding of their rights, (ii) raising policymakers' understanding of advanced technology, and (iii) promoting best practices, laws and regulations that protect both the civic values and the rights of individuals in the 21st century economy, driven by the mass collection, use and disclosure of data.
- Digital Governance Council (formerly the CIO Strategy Council) – a not-for-profit organisation that works to provide Canadians with confidence in the responsible design, architecture and management of digital technologies through four streams of activity:
  (a) convening an executive forum for members to share best practices, identify digital governance gaps, and prioritise collective action;
  (b) partnering to prove out new technologies and deliver proofs of concept and common building blocks to manage risks and opportunities associated with the use of digital technologies;
  (c) establishing the Council's Digital Governance Standards Institute, independent of the Council, to develop technology governance standards; and
  (d) certifying organisations against digital governance standards.
- The Citizen Lab–an interdisciplinary laboratory created by the University of Toronto that focuses on research, development, and strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.
- Canadian Internet Policy and Public Interest Clinic (CIPPIC)–a public-interest technology law clinic based at the University of Ottawa which works to advance the public interest on privacy issues.

Self-Regulatory Organisations

The major industry self-regulatory organisations and trade associations are:

- Digital Advertising Alliance of Canada (DAAC) – an alliance of industry associations responsible for administering AdChoices, a programme to provide notice, transparency,

and accountability from the advertising sector online to consumers. The programme allows Canadians to opt-out of what the DAAC calls interest-based advertising, and requires that participants hold themselves to specific standards.
- Ad Standards – an independent, non-profit organisation that administers the Canadian Code of Advertising Standards, which is the principal instrument of responsible and effective advertising self-regulation nationwide. Ad Standards is responsible for monitoring the compliance of participants in the DAAC's AdChoices Program. Ad Standards reviews participating companies' online interest-based advertising practices, and helps ensure they meet the requirements set out in the DAAC's Canadian Self-Regulatory Principles for Interest-Based Advertising (revised October 2022). As an independent compliance partner, Ad Standards audits compliance and accepts complaints from the public about potential violations of the DAAC Principles under the AdChoices Accountability Program.
- Interactive Advertising Bureau of Canada (IAB Canada) – a trade association exclusively dedicated to the development and promotion of the digital marketing and advertising sector in Canada. As a not-for-profit association, IAB Canada represents over 250 of Canada's advertisers, ad agencies, media companies, service providers, educational institutions and government associations.
- Canadian Marketing Association (CMA) – an industry association that encourages its members to comply with the Canadian Marketing Code of Ethics and Standards and other best practices and guidance for marketers and, with respect to Canadian privacy law reform, engages with both federal and provincial governments through submissions developed by the CMA's Privacy and Data Committee.
- Canadian Anonymization Network (CANON) – an organisation whose objectives include advocating for legislative and policy standards for annonymisation that enable innovative and beneficial uses of data, while reasonably protecting against foreseeable privacy risks.

1.6 System Characteristics

Québec (under Bill 64) and Ontario (under PHIPA) are currently the only provinces with legislation that grants authority to the privacy commissioners themselves to impose administrative monetary penalties (AMPs).

While this sparse granting of AMP powers may change as privacy law modernises throughout Canada, it differentiates Canadian privacy offices from their G7 counterparts in terms of enforcement consequences. The lack of serious monetary consequences, however, is in keeping with the low damage awards that Canadian courts will grant for privacy torts, compared to other G7 jurisdictions.

Despite the perceived lack of enforcement consequences, Canadian privacy commissioners have undertaken several actions jointly based on an ombuds model, where commissioners make recommendations for privacy compliance, and companies may implement those recommendations. In many cases companies implement the Commissioner's recommendations, but some companies refuse and become subject to actions in Federal Court.

Canada is also unique due to its federal structure, where privacy is regulated on both provincial and federal levels. The application of one law does not always exclude the other, depending

on the circumstances. See **1.4 Multilateral and Subnational Issues**.

1.7 Key Developments

There have been several recent key developments in Canada, mostly concerning privacy law reform:

- the Federal Government has tabled Bill C-27, which introduces a new federal private sector privacy law, a privacy tribunal, and a framework for regulating artificial intelligence (AI);
- Québec has passed Bill 64, strengthening privacy protection and increasing compliance obligations within that province;
- the privacy tort of intrusion upon seclusion has been limited in "database defendant" class actions involving data breaches by third-party hackers;
- the Federal Government has tabled Bill C-26, legislation aimed at preventing cybersecurity incidents; and
- there are ongoing provincial privacy law reform initiatives in Ontario, British Columbia and Alberta – see **1.8 Significant Pending Changes, Hot Topics and Issues** (Provincial-Level Privacy Law Reform).

BILL C-27

The government introduced Bill C-27, the Digital Charter Implementation Act, 2022 in the House of Commons in June 2022. If passed, Bill C-27 would implement three new pieces of federal legislation:

- the Consumer Privacy Protection Act (CPPA);
- the Personal Information and Data Protection Tribunal Act (PIDPTA); and
- the Artificial Intelligence and Data Act (AIDA).

Consumer Privacy Protection Act (CPPA)

If enacted, the CPPA would replace PIPEDA. It differs from PIPEDA in several key respects. For example, the CPPA:

- introduces AMPs of up to CAD10 million or 3% of an organisation's gross global revenue for certain privacy contraventions;
- introduces fines of up to CAD25 million or 5% of an organisation's gross global revenue for offences;
- introduces the requirement that every organisation implement and maintain a privacy management programme, which includes policies, practices and procedures put in place to fulfil the obligations of the CPPA – the Privacy Commissioner can request access to an organisation's privacy management programme and recommend corrective measures be taken by the organisation;
- states that the personal information of minors is sensitive;
- brings de-identified personal information within the scope of the CPPA and prohibits re-identification;
- makes explicit that it does not apply to personal information that has been anonymised;
- changes the previous consent regime – organisations can process information with express consent, implied consent, or without consent if the collection or use is for a "business activity" or "legitimate interest", as prescribed by the CPPA under certain circumstances;
- defines "service provider" and clarifies service provider obligations, specifically stating that knowledge and consent are not required for transfers and making clear that certain obligations do not apply to service providers if they are not collecting, using, or disclosing personal information for purposes other than

the purpose for which the information was transferred;
- introduces the ability for organisations and entities to establish codes of practice and certification programmes;
- allows individuals to request that their personal information be disclosed directly to other organisations under Data Mobility Frameworks subject to regulations;
- introduces a private right of action (PRA) – individuals affected by a CPPA violation have a cause of action for damages for loss or injury suffered as a result of a contravention of the CPPA under certain circumstances;
- permits the disclosure of data, without consent, for public-interest purposes, such as "socially beneficial purposes", and statistics, study, or research, if certain conditions are met;
- requires personal information shared in prospective business transactions to be de-identified, unless de-identification would undermine the objectives for carrying out the transaction and the organisation has taken into account the risk of harm to the individual that could result from using or disclosing the information;
- provides the Privacy Commissioner with new order-making powers and the ability to conduct an inquiry; and
- increases openness and transparency requirements, such as requiring organisations to provide a general account of their use of any automated decision systems used to make predictions, recommendations or decisions about individuals that could have a significant impact on them.

Personal Information and Data Protection Tribunal Act (PIDPTA)

PIDPTA, if passed in its current form, would establish the federal Personal Information and Data Protection Tribunal (Tribunal).

The Tribunal is to have three to six members, at least three of whom must have experience in information and privacy law.

The Tribunal would:

- hear appeals of certain findings, orders or decisions made by the Privacy Commissioner; and
- impose administrative monetary penalties (AMPs) on organisations of up to a maximum of CAD10 million or 3% of the organisation's gross global revenue in the financial year before the one in which the penalty is imposed, whichever is higher.

Tribunal decisions are to be final and binding, except for judicial review under the Federal Courts Act, RSC 1985, c F-7, and are not subject to appeal or review by any court.

Artificial Intelligence and Data Act (AIDA)

If passed, AIDA would regulate artificial intelligence systems (ADS) in the private sector. Its purpose is to establish common requirements for the design, development, and use of ADS and to prohibit ADS conduct that may result in serious harm to individuals. AIDA seeks to establish measures to mitigate the risk of harm or biased output from the use of high-impact systems, and imposes ADS monitoring, communication, notification, and record-keeping requirements. AIDA in its current form relies heavily on details of the law being established by regulations.

AIDA would be administered by the Minister of Innovation, Science and Economic Development, who would have the power to audit and issue orders. Violations come with AMPs to be established by regulations and fines of up to CAD25 million or 5% of the organisation's gross global revenues in the preceding financial year for certain offences.

AIDA would also establish an "Artificial Intelligence and Data Commissioner", to assist the Minister in the administration and enforcement of the Act.

Bill 64/Law 25

In 2021, Québec passed Bill 64, which is generally recognised as the most stringent privacy law in Canada, strengthening privacy protection and increasing compliance obligations within that province.

Following its assent, Bill 64 became a chapter in the annual volume of the Statutes of Québec: 2021, chapter 25, titled: An Act to modernise legislative provisions as regards the protection of personal information, SQ 2021, c 25. While many people continue to refer to the passed legislation as "Bill 64", it is also referred to as "Law 25".

The passage of Bill 64 brought reforms and amendments to Québec's pre-existing privacy statutes, including Québec's Private Sector Privacy Act and the Act respecting the protection of personal information in the private sector, CQLR c P-39.1 (Québec's Public Sector Privacy Act).

Bill 64 introduces AMPs, increased use of privacy impact assessments (PIAs), new exceptions to consent, mandatory confidentiality incident reporting, and further requirements pertaining to accountability, cross-border data transfers, retention, anonymisation, data portability, de-indexing, automated decision making, and biometric data.

Québec's Private Sector Privacy Act has provisions that came into force in September 2022, as well as others that will come into force in September 2023 and 2024.

Bill 64 provisions that came into effect in 2022 include:

- there must be a "person in charge" of privacy compliance which, by default, is the highest authority in an organisation (for example, the CEO) – this person can delegate all or part of this function in writing to any person;
- new exceptions to consent, such as the ability to disclose personal information without consent in the context of a business transaction, or communicate personal information for statistical, study or research purposes if an assessment concludes certain privacy-related factors are met;
- a new reporting requirement for confidentiality incidents is defined to include:
  - (a) access not authorised by law to personal information;
  - (b) use or communication not authorised by law of personal information; or
  - (c) loss of personal information or any other breach in the protection of such information.

Confidentiality incidents must be reported to the CAI and the individual if there is a "risk of serious injury." In assessing the risk of injury, consideration must be given to the sensitivity of the information, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes. Organisations are required to keep a register of confidentiality

incidents, which must be sent to the CAI upon its request.

In June 2022, the Québec Gazette published draft regulations which set out specific requirements surrounding confidentiality incident reporting to the CAI. The CAI has also issued numerous guidance documents on their website, including a form for confidentiality incident reporting.

Restricted Scope of Intrusion Upon Seclusion ("Database Defendants")
The Court of Appeal of Ontario has recently decided a trilogy of cases that database holders who suffered a cyber-attack by external actors (ie, hackers) are not liable for the tort of intrusion upon seclusion. The court noted that database holders may still be liable for breach of contract, breach of confidence, and negligence, which requires proof of actual damage, as opposed to the symbolic/moral damages available for intrusion upon seclusion.

The tort of intrusion upon seclusion remains available where the unauthorised access was caused by internal actors (ie, a company's employees).

Bill C-26 – An Act Respecting Cyber Security
In 2022, the federal government also tabled Bill C-26, which would enact the Critical Cyber Systems Protection Act (CCSPA).

CCSPA aims to protect critical cybersystems in the federally regulated private sector (eg, banks, energy, nuclear safety, transportation, telecommunications). It requires designated classes of operators to establish cybersecurity programmes, mitigate supply-chain and third-party cybersecurity risks, and report certain cybersecurity incidents. The Governor in Council can also issue "Cyber Security Directions" to direct compliance with certain measures intended for the protection of cybersecurity.

Bill C-26 also makes changes regarding cybersecurity to the Telecommunications Act, which could prohibit a telecommunications service provider from using all products and services if it is necessary to secure the Canadian telecommunications system, in certain circumstances.

Bill C-26 also introduces AMPs for violations of CCSPA, with a maximum penalty of CAD1 million, in the case of an individual and up to CAD15 million in any other case.

1.8 Significant Pending Changes, Hot Topics and Issues

The most significant pending changes are described above, under **1.7 Key Developments**. There are two further significant pending changes.

Provincial-Level Privacy Law Reform
At the provincial level, British Columbia (BC), Alberta, and Ontario have signalled that private sector privacy law reform is on the horizon. In BC, a Special Committee appointed to review BC PIPA made recommendations to the BC Parliament to amend and strengthen BC PIPA, and harmonise it with federal privacy modernisation and international approaches. Furthermore, starting in 2023, BC public sector privacy legislation makes it mandatory for public bodies to report data breaches and implement privacy management programmes.

Ontario, which does not currently have its own private sector privacy legislation, held a public consultation on modernising privacy in the province, seeking to establish a comprehensive provincial privacy regime. It remains to be seen

whether Ontario will introduce new private sector privacy legislation.

Reform of the Privacy Act

Justice Canada has signalled that federal Privacy Act reform is coming. Consultations were held on modernising the Act in 2021, resulting in a comprehensive Report showing support for reform. The goals include using technology to modernise government processes, and granting the OPC a greater proactive and educational mandate for more effective support and oversight, while taking into account individuals' expectations of privacy and data protection laws from other jurisdictions.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

PIPEDA Requirements

PIPEDA requires compliance with the following fair information principles:

1. accountability;
2. identifying purposes;
3. consent;
4. limiting collection;
5. limiting use, disclosure, and retention;
6. accuracy;
7. safeguards;
8. openness;
9. access; and
10. challenging compliance.

Principle 1 – accountability

Organisations must:

- designate responsible persons for privacy law compliance;
- ensure personal information transferred to third parties for processing has a comparable level of protection (eg, via contractual or other measures); and
- implement privacy policies and procedures, which includes procedures to protect personal information, training employees, and processes for responding to complaints or inquiries.

Principle 2 – identifying purposes

Organisations must document the purposes for which personal information is collected. The purposes should be specified at or before the time of collection. New purposes require fresh consent.

Principle 3 – consent

Consent is only valid if it is reasonable to expect that an individual to whom the organisation's activities are directed would understand the nature, purpose and consequences of the collection, use, or disclosure of the personal information to which they are consenting.

The OPC, OIPC BC, and OIPC AB have issued joint guidance titled, Guidelines for Obtaining Meaningful Consent. These Guidelines describe the principles for meaningful consent, the appropriate form of consent, and consent in the context of children. They also provide a consent checklist.

The consent principle is central to the PIPEDA regime, since it is required for the collection, use, and disclosure of personal information, unless an exemption applies (and the exemptions are narrow and specific under PIPEDA).

Principle 4 – limiting collection

The collection of personal information should be limited to that which is necessary to fulfil the

identified purposes. Collecting personal information indiscriminately is prohibited. Personal information may only be collected by fair and lawful means.

Principle 5 – limiting use, disclosure, and retention

Organisations must develop guidelines and implement procedures with respect to the retention of personal information, including setting minimum and maximum retention periods. Personal information that is no longer required to fulfil an identified purpose should be destroyed, erased, or made anonymous.

Personal information used to make a decision about an individual must be retained long enough to allow the individual access to the information after the decision has been made.

Principle 6 – accuracy

Personal information must be sufficiently accurate, complete and up-to-date, to minimise the possibility that inappropriate information may be used to make a decision about the individual. However, routine updating is prohibited, unless this process is necessary to fulfil the purposes for which the information was collected.

Principle 7 – safeguards

Organisations must:

- safeguard personal information against loss or theft, unauthorised access, disclosure, copying, use, or modification;
- protect personal information with safeguards appropriate to the sensitivity of the information, thus more sensitive information should be safeguarded with a higher level of protection; and
- ensure employees are made aware of the importance of maintaining the confidentiality of personal information.

Organisations should implement physical, organisational and technological safeguards.

Principle 8 – openness

Organisations must be transparent about their privacy practices, policies and procedures, for example:

- by ensuring individuals can generally understand and easily acquire information about the organisation's privacy policies and practices;
- making available the name or title and address of the person who is accountable for the organisation's privacy policies and practices; and
- making known the process for access to personal information held by the organisation, as well who to contact with complaints or inquiries.

Principle 9 – access

Individuals have a right to be informed of and to access the personal information held by organisations about them.

Individuals must be able to challenge the accuracy and completeness of the personal information held, and be able to amend the information as appropriate within certain specific and limited exceptions. If requested, organisations must also be able to provide an account of the third parties to which the information has been disclosed. Access must be provided for free or at a minimal fee, within a reasonable time.

There are also provisions in PIPEDA (Sections 8 and 9) outside the principles concerning access

which speak to time limits, costs, and exceptions to access.

Principle 10 – challenging compliance
Organisations must put in place procedures to receive and respond to complaints or inquiries about their personal information handling practices. All complaints must be investigated. If the complaint is justified, the organisation must take appropriate measures to address the situation.

Other Requirements

In addition to the ten fair information principles, there are compliance requirements in the body of PIPEDA:

- Section 5(3) is an overarching requirement that the collection, use, or disclosure of personal information must be for an appropriate purpose, namely, one that a reasonable person would consider appropriate in the circumstances;
- PIPEDA has mandatory breach reporting to both individuals and the OPC where there is a real risk of significant harm to individuals (RROSH); it also contains the requirement to keep records of all breaches, not just RROSH breaches, which the Privacy Commissioner has the right to inspect. It is an offence under PIPEDA to knowingly contravene the requirements to:
  (a) report a breach to the Privacy Commissioner that creates a RROSH; or
  (b) keep and maintain a record of every breach of security safeguards involving personal information under an organisation's control.
- There are anti-spam provisions in PIPEDA targeting email address harvesting – eg, prohibiting the use of computer programs to collect email addresses ("electronic addresses") and the use of such email addresses collected by such programs. It is also prohibited to illicitly access another person's computer system to collect personal information – eg, via spyware.

De-identified Information

PIPEDA does not explicitly address personal information that has been de-identified. However, Bill C-27 defines and regulates de-identified information. (see **1.7 Key Developments**).

2.2 Sectoral and Special Issues

Sensitive Information

Sensitive information is not defined in PIPEDA. However, sensitivity is tied to the consent and safeguarding principles, and is a factor in determining whether a breach creates a RROSH.

While some personal information is generally considered sensitive (eg, health or financial information), sensitivity can also depend on the context (eg, personal information combined with other information can become sensitive). Sexual orientation, ethnic and racial origins, children's information, religious information, political affiliations, genetic and biometric data, drug and alcohol references, and/or information affecting a person's reputation have all been considered sensitive information.

Under Québec's Bill 64, examples of sensitive information include medical, biometric, or intimate information. Information can also be sensitive depending on the context of its use.

Children

PIPEDA does not have a section dedicated to youth and children, although 4.3 Principle 3 does say "seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated".

That said, the OPC has interpreted and enforced PIPEDA in ways that establish privacy protections for children. For example, the OPC has provided guidance stating that the information of children will be considered particularly sensitive. It also has a general rule that meaningful consent cannot be obtained from children under the age of 13. Bill C-27 (see **1.7 Key Developments**) states that the personal information of minors is sensitive.

Under Law 25, parental consent is required for processing the information of children, defined as under the age of 14, unless clearly for the child's benefit. In August 2022, the CAI issued a report on children's privacy, titled: Ensuring A Better Protection for Young People's Personal Information in The Digital Age, finding that children require additional measures, in addition to those afforded under Law 25, to better protect them.

Right To Be Forgotten

Under PIPEDA, individuals have a right to withdraw consent, access personal information, and ensure their information is accurate, complete and up to date. A 2021 Federal Court Reference decision found that PIPEDA applies to Google's search engine, and that it is not exempt from PIPEDA. Google has appealed the decision to the Federal Court of Appeal.

Financial Information

In 2022, the Office of the Superintendent of Financial Institutions (OSFI) issued Guidelines pertaining to technology and cyber-risk management by federally regulated financial institutions. The Guidelines set out obligations for cybergovernance and risk management, aim to enhance cybersecurity, and will be effective as of January 2024.

In addition to PIPEDA, federal banking legislation contains provisions for regulating personal financial data. There are also personal information obligations in various provincial consumer credit reporting laws.

2.3 Online Marketing

Canada's Anti-Spam Legislation (CASL)

Canada's Anti-Spam Legislation (CASL) prohibits the sending of commercial electronic messages (CEMs, such as emails) without consent unless an exception applies. CASL also requires CEMs to meet identification and unsubscribe requirements, again unless an exception applies. It also targets more egregious conduct, including botnets, malware, spyware, or viruses that result from the installation of a computer programm without consent or from altering transmission data.

Telemarketing

Telemarketers in Canada may also be subject to various telemarketing rules, administered and enforced by the Canadian Radio-television and Telecommunications Commission (CRTC), including:

- requirements for telemarketers to register with the national do-not-call list;
- specific requirements for calls made with automatic dialling-announcing devices;
- record-keeping obligations; and
- certain registration requirements for telephone calls made during an election period.

The CRTC has vast enforcement powers, including the power to conduct regulatory inspections, issue orders, compel information, and AMPs of up to CAD15,000 under the Telecommunications Act and up to CAD10 million under CASL.

Online Behavioural Advertising (OBA)

The OPC has issued guidance and a Policy Position on online behavioural advertising (OBA) (also known as interest-based advertising/personalised advertising) noting that reliance on opt-out consent for OBA requires that:

- the personal information not be sensitive;
- the purpose of consent be stated in a manner that is clear, understandable, and obvious;
- the opt-out be readily available, preferably at the time of collection, be persistent, and take effective immediately; and
- the tracking of children be avoided.

The DAAC has also developed self-regulatory principles for OBA, which include transparency, consumer control, data security, sensitive data, education, and accountability (see **1.5 Major NGOs and Self-Regulatory Organisations** for a description of the DAAC). In its October 2022 refresh of these principles, the DAAC officially adopts the term "interest-based advertising" as opposed to "online behavioural advertising".

2.4 Workplace Privacy

Ontario Employee Electronic Monitoring Policy

In 2022, the government of Ontario introduced a requirement for employers with over 25 employees to have a written policy on the electronic monitoring of their employees. The policy must contain:

- a description of the monitoring;
- the purposes for the monitoring; and
- how employees are electronically monitored.

A copy of the policy must be provided to all employees.

These changes were made under the Employment Standards Act, 2000, S.O. 2000, c. 41 (ESA) and not under privacy legislation. On its website, the Ontario government specifically states that these changes do not introduce any new privacy rights.

Notably, there is no enforcement mechanism for non-compliance with these ESA requirements.

Employee Privacy Rights Afforded Under Privacy Statutes

Workplace privacy rights differ throughout Canada.

Employee rights under PIPEDA only extend to federally regulated organisations and FWUBs (not the entire private sector). However, employee privacy rights are provided in BC PIPA, AB PIPA, and Québec's Private Sector Privacy law.

In an OPC Report of Findings issued in 2022, a transportation company was able to rely on an exception to consent to manage its employment relationships when installing a camera onto a truck cabin that recorded both video and audio of its employees.

Whistle-blowing

PIPEDA contains "whistle-blowing" provisions, allowing for the OPC to receive information from a whistle-blower, and to keep the identity of that person confidential.

Employee Privacy in the Courts

In the 2022 decision Elementary Teachers Federation of Ontario v. York Region District School Board, 2022 ONCA 476, the Court of Appeal for Ontario found that employees have a reasonable expectation of privacy in the workplace and are protected from unreasonable search and seizure under s. 8 of the Canadian Charter of Rights and

Freedoms. In this case, private password-protected teacher communications were afforded a reasonable expectation of privacy, although they were accessed via a web browser on a workplace computer, but not saved on any workplace network.

2.5 Enforcement and Litigation

Potential remedies and penalties for non-compliance with privacy legislation include administrative remedies, private litigation, and criminal penalties. See **1.3 Administration and Enforcement Process**.

Leading Regulatory Enforcement Cases

Investigation into Home Depot's use of Meta's offline conversions tool

The OPC found that Home Depot (the American multinational home improvement retail company) shared hashed email addresses and some purchase details of its customers who opted for an e-receipt with Meta via its offline conversions business tool without the express opt-in consent of those customers as required under PIPEDA. This tool allowed Meta to match the email address to a customer's Facebook account in order to evaluate the effectiveness of Facebook ads. Meta also used this information to construct "look-alike" audiences to deliver ads across the Facebook platform to people with similar profiles to existing customers. Home Depot committed to implement the OPC's recommendations and discontinued its use of Meta's tool.

Investigation into the TikTok App

In February 2023, four Canadian privacy offices announced a joint investigation into the application, TikTok. The investigation will examine the company's privacy compliance, including how TikTok's privacy practices relate to young users of the service.

Investigation into the Tim Hortons App

A joint investigation by four Canadian privacy offices (the OPC, OIPC BC, OIPC AB and CAI) found an app for customers deployed by Tim Hortons (the Canadian multinational coffeehouse and restaurant chain) had collected granular location data of its users (such as where they lived, worked, and travelled, and when they visited a competitor) for an inappropriate purpose and without valid consent.

The investigation also identified issues with vague contractual language used between TDL Group (Tim Hortons operator and franchisor; "TDL") and the third party providing the app tracking service, taking issue with an interpretation in the contract that the third party could have used the information for its own purposes.

Lastly, the investigation identified issues with TDL's privacy practices and recommended the establishment and implementation of a privacy management program. TDL agreed to implement all the privacy commissioner's recommendations.

Investigation into the Marriott data breach

Following the acquisition of a competitor, Marriott International (the American multinational hospitality company) discovered a data breach in a customer database that it had acquired and reported the breach to the OPC.

Despite due diligence conducted as part of the acquisition, such as receiving reports of compliance from two different independent security assessors, the investigation found that the breach went undetected for several years (both before and after the acquisition).

While the OPC's investigation noted the positive mitigation measures that Marriott offered

to its consumers, it found issues with Marriott's security safeguards in place, and recommended enhancements to Marriott's safeguards.

Private Litigation

Individuals may also commence litigation against organisations breaching privacy statutes. PIPEDA does not include a private right of action, however, non-compliance may result in claims under contract law and/or torts such as negligence, breach of contract and privacy torts. In Ontario, there are four privacy torts:

- intrusion upon seclusion;
- public disclosure of embarrassing private facts;
- appropriation of a person's name or likeness; and
- publicity placing a person in a false light.

Privacy class actions are common in Canada. Although the threshold for certification is not high, Canadian courts have been imposing limits to avoid opening the floodgates.

In 2022, the Court of Appeal for Ontario denied certification on a trilogy of "database defendant" class actions and determined that organisations are not liable for the tort of intrusion upon seclusion when a database is breached by external actors such as hackers.

Conversely, however, the Federal Court certified a class action against the government of Canada arising out of a cybersecurity attack by hackers into the government database in a negligence claim.

There are no decisions on the merits in privacy class actions yet. Most have ended in settlement with a low level of per person compensation.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

Law enforcement and national securities agencies can employ lawful access technologies to aid in the investigation of serious crimes. Such crimes include drug trafficking, money laundering, human trafficking, child pornography, murder and threats to national security.

Law enforcement can gain access to data for serious crimes through technologies that can intercept communications, and search and seize computer data. These investigative techniques require lawful authority by means of a warrant issued by a judge in specific circumstances, for example, under the Criminal Code, RSC 1985, c C-46.

Law enforcement access, as far as it concerns Canadian citizens, is subject to the Canadian Charter of Rights and Freedoms.

3.2 Laws and Standards for Access to Data for National Security Purposes

Several laws in Canada relate to government access to data for intelligence, anti-terrorism or other national security purposes, including: the Security of Canada Information Disclosure Act, S.C. 2015, c. 20, s. 2 (SCIDA), the Criminal Code, the Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23, (the "CSIS Act"), and other laws which entail a national security mandate or responsibility.

These laws are subject to the safeguards and framework under the Canadian Charter of Rights and Freedoms and the federal Privacy Act. They often require independent judicial approval for the execution of warrants, barring exigent cir-

cumstances. Furthermore, the SCIDA governs the sharing of information for national security purposes between federal departments. The National Security and Intelligence Review Agency (NSIRA), established in 2019, is mandated to review the sharing of information under the SCIDA as well as the government of Canada's national security and intelligence activities.

3.3 Invoking Foreign Government Obligations

Under PIPEDA, organisations are permitted to disclose personal information without the knowledge or consent of the individual, if the disclosure is to a government institution or part of a government institution that has made a lawful request for the information, identifying the lawful authority to obtain the information, and has indicated that the information relates to national security, the defence of Canada, or the conduct of international affairs. A request by law enforcement to disclose information on a voluntary basis will likely not suffice. A lawful authority is required.

In 2022, the United States and Canada formally announced bilateral negotiations on the US Clarifying Lawful Overseas Use of Data (CLOUD) Act, aimed at access to electronic information for the investigating serious crimes.

3.4 Key Privacy Issues, Conflicts and Public Debates

In November 2022, the House of Commons Standing Committee on Information, Privacy and Ethics (ETHI) issued a report on their study of device investigation tools used by the Royal Canadian Mounted Police (RCMP). The study looked at spyware and other technology-based investigative tools used by the RCMP in the context of investigations.

The purpose of the Report was to examine the benefits and risks associated with the use of device investigative tools and the measures that the federal government could take to better regulate the use of such tools in Canada. The Report included nine recommendations. One recommendation was to amend the federal Privacy Act to include an explicit obligation for government institutions to conduct privacy impact assessments prior to using high-risk technological tools to collect personal information.

Canadian privacy commissioners have also issued joint guidance for police agencies on their use of facial recognition technology, noting deficiencies in the current legislative scheme to sufficiently address the concerns brought about by such use. See **5.1 Emerging Digital and Technology Issues** (Facial Recognition Technology) for further discussion.

4. International Considerations

4.1 Restrictions on International Data Issues

PIPEDA does not prohibit the transfer of personal information across borders. However, any transfers of personal information outside of Canada must provide a comparable level of protection to PIPEDA. OPC guidance also states that individuals must be provided with notice of cross-border data transfers, and that organisations should disclose that personal information could be subject to the laws of a foreign jurisdiction.

In Québec, Bill 64 requires organisations transferring personal information to other Canadian provinces or outside of Canada to ensure that the third party receiving such information gives an adequate level of protection reflecting gen-

erally accepted data protection principles. In addition, Bill 64 requires organisations communicating personal information outside Québec to conduct a transfer impact assessment (TIA) before the transfer, taking into account these factors:

- sensitivity of information;
- purpose for which the information is to be used;
- protective measures that would apply to the communication (including contractual safeguards); and
- privacy laws of the jurisdiction which receives the information.

British Columbia requires a privacy impact assessment from public bodies transferring personal information abroad. These assessments assess risk on a case-by-case basis, and consider the sensitivity of the information and where it is stored. A supplementary assessment is required for storing sensitive information outside of Canada.

In Nova Scotia, the Personal Information International Disclosure Protection Act, SNS 2006, c 3, describes the circumstances in which public bodies may transfer information across borders–absent such requirements, international transfers are not permitted.

In Alberta, before the transfer, the transferring organisation must provide the individual with notice of its policies and procedures and its representative's contact information.

4.2 Mechanisms or Derogations That Apply to International Data Transfers

APEC

Canada endorses the Asia-Pacific Economic Cooperation (APEC)'s Cross-Border Privacy Rules (CBPR), created to establish privacy protections and remove unnecessary barriers to information flows between participating countries. In 2022, Canada formed part of the Global CBPR Declaration, which established the Global CBPR Forum. The Global CBPR Forum aims to promote interoperability between different privacy and data protection regulatory approaches and seeks to establish an international certification system, based on APEC's CBPR and the Privacy Recognition for Processors Systems.

PIPEDA

PIPEDA permits the use of any mechanism that ensures a comparable level of protection. However, the OPC encourages transferring organisations to implement privacy protections through written contracts. Among other things, contractual provisions should require third parties to have policies in place to protect personal information (eg, training staff and having effective security measures), and allow transferring organisations to audit the third party's handling and storing of personal information.

Organisations must give individuals notice of any potential transfer of their personal information outside of Canada, but their consent to the transfer is not required.

Bill 64

Québec's Bill 64 also relies on contractual measures to ensure compliance with its protective safeguards. However, it differentiates between transfers to service providers and other third parties. Transfers to service providers require a written contract that takes into account the results of the TIA and contains the specific safeguard measures identified in the Act. Transfers to other third parties do not have specific contractual requirements – although a written contract incorporating the OECD principles (namely, lim-

ited collection, data quality, purpose specification, use limitation, protection safeguards, openness, individual participation, and accountability) is highly recommended.

Ontario

In Ontario, PHIPA requires consent before disclosure of personal information to persons outside of Ontario.

4.3 Government Notifications and Approvals

See **4.1 Restrictions on International Data Issues** and **4.2 Mechanisms or Derogations that Apply to International Data Transfers**. There are no requirements under PIPEDA.

4.4 Data Localisation Requirements

Tax Records

Canadian income tax law requires certain tax-related records be kept in Canada or another place designated by the Minister of National Revenue. Records kept outside Canada and accessed electronically from Canada are not considered to be records in Canada. Additionally, in accordance with federal financial institutions legislation and Guideline B-10 of the OSFI, banks, trust and loan companies, insurance companies, and co-operative credit associations are required to keep records in Canada (to ensure OSFI can access in Canada any records necessary to enable OSFI to fulfill its mandate).

USMCA

The United States-Mexico-Canada Agreement (USMCA) prohibits any Canadian law from requiring the use or location of computing facilities in Canada as a condition for conducting business with parties in Mexico or the United States.

4.5 Sharing Technical Details

Software codes, algorithms or similar technical details are not required to be shared with the government without lawful authority. Under AIDA, however, organisations may be required to notify the government of artificial intelligence systems that have a high impact and risk potential. See **1.7 Key Developments** for further discussion.

4.6 Limitations and Considerations

PIPEDA authorises the disclosure of personal information without the individual's knowledge or consent when required by law – eg, to comply with (i) a subpoena or warrant issued or an order made by court, (ii) court production of records, or (iii) mandatory reporting under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.

4.7 "Blocking" Statutes

Canada has the authority under the Foreign Extraterritorial Measures Act (FEMA) to respond to unacceptable extraterritorial assertions of foreign jurisdictions in Canadian territory. There are currently two orders under FEMA, both unrelated to privacy law.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

Artificial Intelligence (AI)

Canada has tabled new AI legislation proposing to regulate how the private sector creates and uses AI systems with financial consequences for non-compliance (see **1.7 Key Developments**).

Profiling

The OPC has issued guidance, stating the collection, use, and disclosure of personal informa-

tion for the purpose of profiling or categorisation that leads to discrimination is prohibited under PIPEDA.

Facial Recognition Technology

In 2022, following investigations into the use of facial recognition technology, Canadian federal and provincial privacy offices jointly issued guidance on the use of such technology by police agencies across Canada. The purpose of the guidance is to clarify police agencies' obligations relating to the use of facial recognition under existing laws to ensure compliance with the law, minimise privacy risks, and respect privacy rights. The key recommendations include:

- ensuring lawful authority exists for each collection, use, retention, and disclosure of personal information;
- integrating privacy protections into proposed initiatives before using facial recognition technology;
- conducting privacy impact assessments to ensure that the technology meets legal requirements;
- ensuring personal information is accurate and up to date;
- minimising the collection of personal information based on the objectives of the investigative initiative;
- ensuring that the collected information is only used for the purpose for which it was collected (or consistent with that purpose); and
- using appropriate measures to protect the information by implementing openness, transparency and accountability measures related to the collection of the information.

Biometric Data

Bill 64 also amends Québec's Act to Establish a Legal Framework for Information Technology, CQLR c C-1.1. The amendments require companies to notify the CAI if they create a database of biometric characteristics within 60 days before it is brought into service.

Bill 64 also lists biometric information as sensitive. Biometric data is generally considered as sensitive under PIPEDA.

5.2 "Digital Governance" or Fair Data Practice Review Boards

Fair Data Practice Review Boards have not yet been set up under privacy legislation in Canada. The Standards Council of Canada has published a "Canadian Data Governance Standardization Roadmap", which outlines an approach to the development and compatibility of domestic data governance standards.

See reference to Digital Governance Council and its work in **1.5 Major NGOs and Self-Regulatory Organisations**.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

See **2.5 Enforcement and Litigation**.

In December 2022, the OIPC BC released a report on its investigation into BC public health information system, finding the system was vulnerable to misuse and attack, and making several recommendations for addressing privacy and security risks.

5.4 Due Diligence

Under both PIPEDA and provincial private-sector privacy law acts, there are carve outs for the use of personal information in the context of business transactions. Personal information can be shared in the context of business transactions without consent if certain conditions are met, such as a binding agreement, security safe-

guards, use solely for the purpose of the transaction, and notification following completion of the transaction.

Due diligence should also be conducted in the acquisition of personal information in a transaction. In the 2022 OPC Marriott Finding, the hotel chain acquired a competitor database that was being actively hacked, and despite Marriott's due diligence, the hack remained undetected. See **2.5 Enforcement and Litigation** (Investigation into the Marriott data breach) for further discussion.

5.5 Public Disclosure

Under securities legislation, publicly traded companies are required to disclose material changes, which may include cybersecurity incidents, as well as cybersecurity risks. The Canadian Securities Administrators (CSA) has issued a Cyber Security Staff Notice (Staff Notice 11-332) on the disclosure of cybersecurity risks and incidents.

5.6 Digital Technology Regulation/ Convergence of Privacy, Competition and Consumer Protection Laws

Canada's competition law is currently under review as the government has initiated a consultation on proposed changes to the Competition Act, RSC 1985, c C-34. These changes consider digital markets, data, and how competition law intersects with privacy and data protection.

One area where competition and privacy law concerns intersect is deceptive marketing practices. Under competition law, false and misleading advertising can be either a civil or criminal violation. Under PIPEDA, individuals cannot obtain consent through deception. Companies have been penalised under the Competition Act for making misleading claims about the use of personal information.

5.7 Other Significant Issues

A ground-breaking March 2022 order of BC's OIPC has found that BC's provincial private sector privacy law applies to the personal information practices of Canada's federal political parties' (FPPs) when they are engaging BC residents or otherwise operating in BC. This order is important because the FPPs have long asserted that they are not covered by any Canadian private sector privacy law (be it federal or provincial). The FPPs have applied for judicial review of the OIPC's decision which is scheduled to be heard by the BC Supreme Court in May 2023.

Fogler Rubinoff LLP is an agile, resourceful and entrepreneurial mid-sized Canadian law firm based in Toronto, Ontario with over 20 practice areas (including Privacy, Data Governance and Cyber Security) across many industries. With the firm's membership in the International Lawyers Network (an association of over 5,000 lawyers in 67 countries), there is no market or jurisdiction beyond its reach.

The authors acknowledge, with thanks, Foglers' articling students Luciana Andrade and Valentina Galvis's help writing this chapter.

Authors

April Gougeon advises on implementing privacy policies and privacy management programmes, conducting privacy audits, and responding to privacy complaints and investigations. April has over a decade of compliance and regulatory experience working at various government institutions, including the Office of the Privacy Commissioner of Canada, the Canadian Radio-Television and Telecommunications Commission, and the Competition Bureau Canada.

Bill Hearn has been a lawyer for 35 years since first reading law at the University of Toronto and Cambridge University. He is ranked in Chambers as one of Canada's leading advertising and marketing lawyers. Bill advises on matters at the intersection of privacy law and competition law in today's data-driven digital economy. He leads Foglers' Privacy, Data Governance and Cyber Security practice group. He acts for a range of clients (including businesses, trade associations, civil society, and governments) with respect not only to what the law is but how it should be modernised.

Ronald Davis is a litigation and privacy law partner at Fogler Rubinoff. He has appeared at all levels of court, including the Supreme Court of Canada and the Court of Appeal for Ontario. Ron is a cum laude University of Ottawa Common Law en français graduate. He taught at the Law Society of Ontario's Bar Admission Course for a decade. He has edited and written over 50 articles and books on varied topics and holds a PhD in French linguistics from the University of Toronto, where he was an Assistant Professor for five years.

Fogler Rubinoff LLP

77 King Street West, Suite 3000
TD Centre North Tower
Toronto, ON, M5K 1G8
Canada

Tel: 416.941.8805
Fax: 416.864.9700
Email: bhearn@foglers.com
Web: www.foglers.com

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com