INTERNATIONAL LAWYERS NETWORK

2024 ILN DATA PRIVACY GUIDE

An International Guide

www.iln.com

ILN Cybersecurity & Data Privacy Group and ILN Technology Media & Telecommunications Group

Disclaimer

This guide offers an overview of legal aspects of data protection in the requisite jurisdictions. It is meant as an introduction to these marketplaces and does not offer specific legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship, or its equivalent in the requisite jurisdiction.

Neither the International Lawyers Network or its employees, nor any of the contributing law firms or their partners or employees accepts any liability for anything contained in this guide or to any reader who relies on its content. Before concrete actions or decisions are taken, the reader should seek specific legal advice. The contributing member firms of the International Lawyers Network can advise in relation to questions regarding this guide in their respective jurisdictions and look forward to assisting. Please do not, however, share any confidential information with a member firm without first contacting that firm.

This guide describes the law in force in the requisite jurisdictions at the dates of preparation. This may have been some time ago and the reader should bear in mind that statutes, regulations, and rules are subject to change. No duty to update information is assumed by the ILN, its member firms, or the authors of this guide.

The information in this guide may be considered legal advertising.

About the ILN

The ILN is a non-exclusive network of high-quality mid-sized law firms, which operates to create a global platform for the provision of legal services, particularly for clients with international needs. With a presence in 67 countries, it is exceptionally well placed to offer seamless legal services, often of a cross-border nature from like-minded and quality legal practices. In 2021, the ILN was honored as Global Law Firm Network of the Year by The Lawyer European Awards, and in 2016, 2017, 2022, and 2023 they were shortlisted as Global Law Firm Network of the Year. Since 2011, the Network has been listed as a Chambers & Partners Leading Law Firm Network, increasing this ranking in 2021 to be included in the top two percent of law firm networks globally. Today, the ILN remains at the very forefront of legal networks in its reach, capability, and depth of expertise.

Authors of this guide:

1. Cybersecurity & Data Privacy Group

Co-chaired by Jim Giszczak of McDonald Hopkins and Stuart Gerson of Epstein Becker & Green, the Cybersecurity & Data Privacy Specialty Group provides an international platform for enhanced communication, enabling all of its members to easily service the needs of their clients requiring advice.

2. Technology, Media & Telecom (TMT)

Co-chaired by Alishan Naqvee of LexCounsel in New Delhi and Gaurav Bhalla of Ahlawat & Associates in New Delhi the TMT Group provides a platform for communication on current legal issues, best practices, and trends in technology, media & telecom.

www.iln.com

Canada

Introduction

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 (as of March 2023, there are 36 different privacy laws federally, provincially and territorially in Canada).

Canada's two federal privacy laws are:

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

Currently, three provinces have legislation that is deemed substantially similar to PIPEDA:

- the Personal Information Protection Act, SA 2003 c P-6.5 (Alberta);
- the Personal Information Protection Act, SBC 2003, c 63 (British Columbia); and
- an Act Respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1 (Quebec).

The Privacy Commissioner of Canada (the Commissioner) oversees PIPEDA and the Privacy Act. The Commissioner is an independent agent of Parliament and heads the Office of the Privacy Commissioner of Canada (the OPC).

While PIPEDA regulates the private sector and generally applies across Canada, the Privacy Act is a limited statute in that it applies only to federal government institutions and Crown corporations.

This chapter will highlight the key provisions of PIPEDA, as the principal legislation for private sector privacy law in Canada. The chapter will not address provincial privacy laws, public sector privacy laws, or personal health information laws at the federal or provincial levels.

Contact Us

(416) 864 9700
https://www.foglers.com/
bhearn@foglers.com
77 King Street West Suite 3000,
TD Centre North Tower
Toronto, Ontario M5K 1G8 Canada

Governing Data Protection Legislation

1.1. Overview of principal legislation

Enacted in 2001, PIPEDA regulates the collection, use and disclosure of personal information by organizations in the course of commercial activities in Canada. It aims to balance an individual's right to privacy with an organization's need to collect, use, and disclose personal information. PIPEDA applies regardless of the technology employed.

1.2. Upcoming or proposed legislation

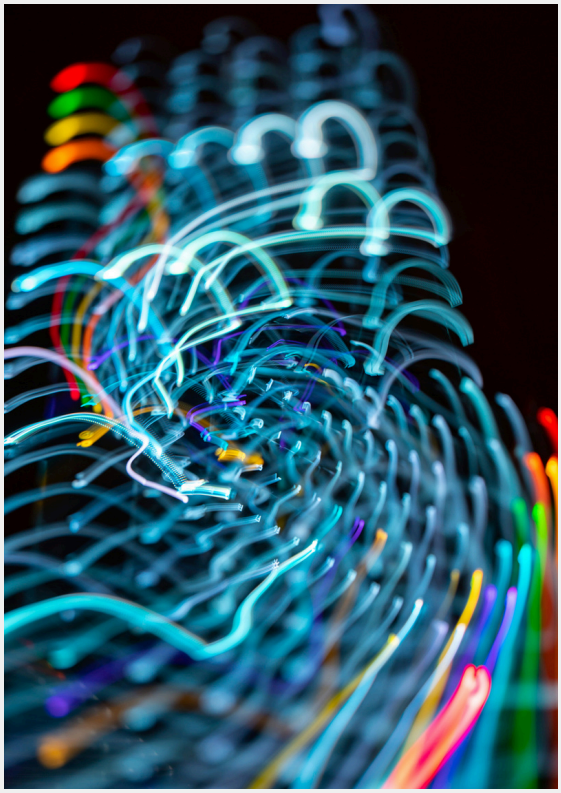
- The Federal Government has tabled Bill C-27, the Digital Charter Implementation Act, 2022. If passed, Bill C-27 would implement three new pieces of federal legislation:
    - the Consumer Privacy Protection Act (CPPA);
    - the Personal Information and Data Protection Tribunal Act (PIDPTA); and
    - the Artificial Intelligence and Data Act (AIDA).
- The Federal Government has also tabled Bill C-26, legislation aimed at preventing cybersecurity incidents.
- There are ongoing provincial privacy law reform initiatives in Ontario, British Columbia and Alberta.

Consumer Privacy Protection Act (CPPA)

If enacted, the CPPA would replace PIPEDA. It differs from PIPEDA in several key respects, some of which will be highlighted in this chapter.

Personal Information and Data Protection Tribunal Act (PIDPTA)

PIDPTA would establish the federal Personal Information and Data Protection Tribunal (the "Tribunal"). The Tribunal would hear appeals of certain findings, orders or decisions made by the Commissioner and impose administrative penalties of up to a maximum of C$10 million or 3% of the organization's gross global revenue, 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.

Artificial Intelligence and Data Act (AIDA)

If passed, AIDA would regulate artificial intelligence systems (AIS) in the private sector and create the role of an Artificial Intelligence and Data Commissioner. Its purpose is to establish common requirements for the design, development, and use of AIS and to prohibit AIS conduct that may result in serious harm to individuals.

Scope of Application

2.1. Legislative Scope

PIPEDA applies to organizations that collect, use, or disclose personal information in the course of commercial activities, unless that organization is exempted. PIPEDA defines commercial activity as any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering, or leasing of donor, membership, or other fundraising lists.

PIPEDA also applies to federal works, undertakings, or businesses (FWUBs), such as 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 (notably, such coverage does not extend to employees of organizations that are not FWUBs).

PIPEDA does not apply to charities and non-profit organizations, as long as they do not engage in commercial activities. Finally, PIPEDA lists organizations to which it specifically applies to in Schedule 4; only the World Anti-Doping Agency is listed.

2.1.1. Definition of personal information

Personal information is defined as information about an identifiable individual. PIPEDA does not define "individual" but the OPC has indicated that "individual" means a natural person.

Personal information includes any factual or subjective information, recorded or not about an identifiable individual. This includes information collected in any form (e.g., in electronic or other formats).

2.1.2. Different categories and types of personal data

Sensitive information is not defined in PIPEDA. However, sensitivity is tied to consent and safeguarding principles, and is a factor in determining whether a data breach creates a real risk of significant harm.

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

Other examples of types of personal information are:

- photographs and video surveillance;
- facial recognition and facial detection;
- location data (e.g., GPS and RFID); and
- employee and employee work product information.

2.1.3. Treatment of data and its different categories

Organizations are expected to comply with PIPEDA when dealing with personal information and use a higher level of care when the information is sensitive in nature.

Information that does not identify an individual or is anonymous is generally not subject to PIPEDA. PIPEDA does not explicitly address personal information that has been de-identified, however, it also does not distinguish de-identified from anonymized information.

If enacted, the CPPA would define and regulate de-identified and anonymized information (which are to be defined as two distinct concepts).

2.2. Statutory exemptions

The following are exempt from PIPEDA:

- personal information that is handled by the federal organizations listed under the Privacy Act;
- provincial or territorial governments and their agents;
- business contact information that is collected, used, or disclosed solely for the purpose of communicating with that person in relation to their employment;
- an individual's collection, use or disclosure of personal information strictly for personal purposes; and
- an organization's collection, use or disclosure of personal information solely for journalistic, artistic, or literary purposes.

2.3. Territorial and extra-territorial application

PIPEDA applies across Canada unless an organization is operating in a province with legislation that has been deemed substantially similar to PIPEDA. PIPEDA may also apply to organizations outside Canada if there is a real and substantial connection to Canada.

Legislative Framework

3.1.Key stakeholders

Data Controller: PIPEDA does not use this term, however, organizations subject to PIPEDA that collect, use, or disclose personal information in the course of commercial activities are akin to "data controllers".

Data Processors: PIPEDA does not use this term. That said, while not explicitly defined, PIPEDA refers to "service providers" which are akin to "data processors".

If enacted, the CPPA will define "service provider" as an organization, including a parent corporation, subsidiary, affiliate, contractor, or subcontractor, that provides services for or on behalf of another organization to assist the organization in fulfilling its purposes.

Data Subject: PIPEDA does not use this term. PIPEDA protects the personal information of individuals who are akin to "data subjects".

Organization: PIPEDA defines this term as an association, a partnership, a person, and a trade union.

3.2. Role and responsibilities of key stakeholders

Schedule A to PIPEDA sets out the ten fair information principles that organizations must comply with:

1. Accountability

- Designate responsible persons for privacy law compliance.
- Ensure personal information transferred to third parties for processing has a comparable level of protection (e.g., via contractual or other measures).
- Implement privacy policies and procedures, which include procedures to protect personal information, training employees, and processes for responding to complaints or inquiries.

2. Identifying Purposes

- 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.

3. Consent

- Acquire consent for the collection, use and disclosure of personal information, unless an exemption applies.

4. Limiting Collection

- Limit the collection of personal information 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.

5. Limiting Use, Disclosure and Retention

- Develop guidelines and implement procedures with respect to the retention of personal information, including setting minimum and maximum retention periods.

6. Accuracy

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

7. Safeguards

- Implement physical, organizational, and technological safeguards.

8. Openness

- 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.

https://www.foglers.com/

- Ensure employees are made aware of the importance of maintaining the confidentiality of the personal information.

9. Individual Access

- Provide access to an individual to their personal information.

10. Challenging Compliance

- Put in place procedures to receive and respond to complaints or inquiries about organizations' personal information handling practices. All complaints must be investigated. If the complaint is justified, the organization must act appropriately to address the situation.

In addition to the ten fair information principles, there are compliance requirements mandated by PIPEDA:

- PIPEDA has mandatory breach reporting to both individuals and the OPC where there is a real risk of significant harm to individuals. It also has mandatory record keeping requirements for all breaches; and

- PIPEDA includes anti-spam provisions that target email address harvesting and the illicit access of another person's computer systems to collect personal information.

Requirements for Data Processing

4.1. Grounds for collection and processing

Consent (which may be express or implied, in writing or oral) is only valid if it is reasonable to expect that an individual to whom the organization'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. Failure to convey the purposes for collecting may render consent meaningless.

If enacted, the CPPA will change the consent regime; personal information may be processed with express consent, implied consent, or without consent if the collection or use is for a "business activity" or "legitimate interest", as set forth in the CPPA under certain circumstances.

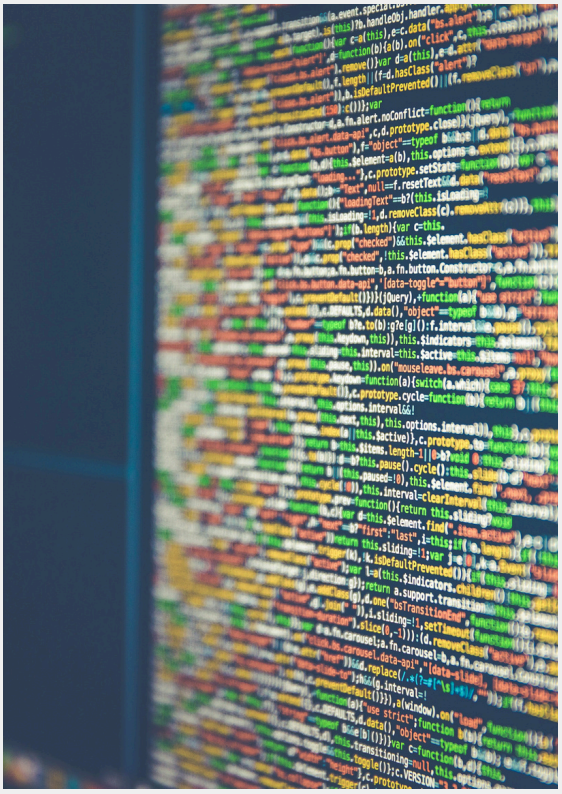
4.2. Data storage and retention timelines

PIPEDA mandates retaining personal information only as long as necessary to fulfil its purpose. Once the information no longer fulfils that purpose, it 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.

PIPEDA provides limited direction on the destruction of personal information. Organizations must develop their own guidelines that govern the disposal or destruction of personal information. The CPPA would specify that disposal of personal information means the permanent and irreversible deletion or anonymization of such personal information.

4.3. Data correction, completion, updating or erasure

Personal information about an individual must be accurate, complete and up to date. Organizations must respond to requests to amend personal information about individuals. An amendment may involve the correction, deletion or addition of information.



If requested, organizations 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 a minimal fee, within a reasonable time.

4.4. Data protection and security practices and procedures

PIPEDA requires organizations to implement appropriate safeguards against unauthorized access or modification of personal information. It mandates appointing privacy officer(s) to be accountable for ensuring compliance. The name, title and contact information of the privacy officer(s) must be readily available as they must act as the point of contact for individuals with compliance concerns.

If enacted, the CPPA will require that organizations implement and maintain a privacy management program. The Commissioner will be able to request access to an organization's privacy management program and recommend corrective measures be taken.

4.5. Disclosure, sharing and transfer of data

Organizations transferring data to service providers must ensure compliance by third parties. Contractual safeguards and monitoring can ensure that service providers are also compliant with

https://www.foglers.com/

PIPEDA. The CPPA will clarify the obligations of service providers, specifically stating that knowledge and consent are not required for transfers and making clear that certain obligations do not apply to service providers that are not collecting, using, or disclosing personal information for purposes other than the purpose for which the information was transferred.

The CPPA would also facilitate direct disclosure requests and allow data disclosure without consent for specific purposes, such as "socially beneficial purposes", statistics, study, or research, if certain conditions are met.

Individuals must receive notice about a potential transfer of information outside of Canada, but the individual's consent to the transfer is not required.

Rights of Data Subjects

5.1. Rights and remedies

PIPEDA provides individuals with the following rights regarding their personal information:

1. To be informed

- Organizations must inform the individual about the information collected, used, and disclosed and the purpose for such activities.

2. To withdraw consent

- May withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Organizations must inform the individual of the withdrawal's implications.

3. To access information

- Access their personal information.
- Upon request, access must be provided for free or at a minimal fee, within a reasonable time. PIPEDA provides for time limits, costs, and exceptions to access outside the principles concerning access.

4. To correction / rectification

- Request the correction, deletion, or addition of information. If appropriate, the amended information shall be transmitted to third parties that have access to the information in question.

5. To grievance redressal and appeal

- File a complaint about an organization's policies and practices relating to the handling of personal information. Organizations must investigate all complaints and must take appropriate corrective measures if justified.
- Individuals who pursue the internal complaint process may subsequently pursue an external process with the OPC. While not a precondition for OPC recourse, exhaustion of internal complaint processes may be required in certain cases.

Collecting and Processing the Personal Data of Children or Minors

PIPEDA does not have a section specific to minors, although Clause 4.3 of Schedule A to PIPEDA does say "seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated".

The OPC has interpreted and enforced PIPEDA in ways that establish privacy protections for minors. For example, the OPC has provided guidance stating that the information of minors will be considered particularly sensitive. It also has a general rule that meaningful consent cannot be obtained from minors under the age of 13.

The CPPA enumerates that the personal information of minors is sensitive.

Regulatory Authorities

7.1. Overview of relevant statutory authorities

The Commissioner is an independent agent of Parliament and heads the OPC.

7.2. Role, functions, and powers of authorities

The OPC has the authority to investigate complaints made under PIPEDA and can issue findings, express opinions regarding complaints, and make recommendations where it believes a violation has occurred. Complaints can be initiated by an individual or by the Commissioner if satisfied that there are reasonable grounds to investigate a matter.

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

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

The Commissioner has an array of investigative powers but no ability to impose administrative monetary penalties. At the end of an investigation, the 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 or in the United States under the Federal Trade Commission Act.

If enacted, the CPPA would grant the OPC order-making powers and the power to recommend to the Tribunal the imposition of administrative monetary penalties. The Tribunal may impose a recommended penalty or make its own determination of the appropriateness and amount of a penalty.

7.3. Role, functions, and powers of civil/criminal courts in the field of data protection

Individuals may commence litigation against organizations breaching privacy statutes. PIPEDA does not currently establish a private right of action, however, non-compliance may result in claims under contract law and/or tort law, such as negligence, breach of contract and privacy torts. In Ontario (and not necessarily in other provinces or territories in Canada), 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.

If enacted, the CPPA will introduce a private right of action. Individuals affected by organizations that contravene the CPPA will have a cause of action for damages for loss or injury suffered under certain circumstances.

The criminal courts do not play a role in enforcing or prosecuting under PIPEDA.

Consequences of non-compliance

8.1. Consequences and penalties for a data breach

Section 28 (1) of PIPEDA states that organizations that knowingly fail to report and maintain records of every security breach that could result in a real risk of significant harm to an individual could be found guilty of:

(a)An offence punishable on summary conviction and liable to a fine not exceeding $C10,000; or

(b)An indictable offence and liable to a fine not exceeding $C100,000.

8.2. Consequences and penalties for other violations and non-compliance

Section 28(1) of PIPEDA also applies to the following offences:

- obstructing the Commissioner or the Commissioner's delegate in the investigation of a complaint or in the conduct of an audit;
- failing to retain personal information that is the subject of an access request for so long as is necessary to enable the requester to exhaust any recourse available under PIPEDA; and
- disciplining or otherwise disadvantaging an employee who has acted in good faith and based on reasonable belief with a view to securing compliance with PIPEDA.

The CPPA provides for the same offences as PIPEDA but it would add one more offence: a breach of the prohibition on using de-identified information alone or in combination with other information to identify an individual. Offences under the CPPA are subject to higher penalties. Indictable offences could see fines of up to $C25 million or five percent of the organization's gross global revenue. For summary offences the fines will be up to $C20 million of four percent of the organization's gross global revenue.

Conclusion

Canada's privacy landscape, governed by federal and provincial/territorial laws, reflects a commitment to balancing individual privacy rights with organizational needs in the digital age. While PIPEDA has served as the cornerstone of private-sector privacy regulation for over twenty years, recent developments such as the proposed modernization of PIPEDA under Bill C-27 are long overdue.

The European Commission renewed Canada's adequacy status on January 15, 2024. An adequacy ruling allows data controllers or data processors to transfer personal data to a country outside the European Union ("EU"). The ruling signifies that the receiving country's privacy laws have an adequate level of protection for personal data. When a country is granted adequacy status, personal data can flow to and from the EU

without the need for additional safeguards. The EU report specifically highlights and recommends enshrining protections that have been developed at a sub-legislative level in Canada to enhance legal certainty. The report also mentions that recent legislative developments can further strengthen the Canadian privacy framework in a positive light.

Authors

Fogler, Rubinoff LLP (FR) is an agile, resourceful, and entrepreneurial mid-sized Canadian law firm based in Toronto, Ontario with over 130 lawyers spanning more than 20 practice areas (including Privacy, Data Governance and Cyber Security) across many industries.

The authors acknowledge, with thanks, the help of FR's articling student, **Diana Bonilla**, in preparing this chapter.

Bill Hearn has been a lawyer for over 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 FR's 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 modernized.

Ronald Davis is a litigation and privacy law partner at FR. 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.

Roberto De Pasquale is an associate in the firm's business law group. He is developing a corporate commercial practice focused on mergers, acquisitions and corporate finance. He regularly helps companies navigate complex regulatory issues, particularly in the privacy space. Roberto is a graduate of Western University's Ivey Business School and Western Law.

Valentina Galvis is an associate in the business law group at FR. Valentina graduated from Osgoode Hall Law School in 2022 and was called to the bar in Ontario in 2023. She is developing a broad corporate commercial practice, with an interest in Privacy and Cyber Security matters.

Contact Us

(416) 864 9700

https://www.foglers.com/

bhearn@foglers.com

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