

Defending Your Business Against Cybercrime and Cyberwarfare



March 13, 2024 Brent J. Arnold, Jasmine Samra & Alycia Riley

Agenda

Topic

A Whirlwind Tour of Canadian Federalism

Bill C-27—The *Consumer Privacy Protection Act*

Bill C-26: Cybersecurity for Critical Infrastructure

Canadian Privacy Data Breach Requirements

Data Breaches: Incident Planning and Response

Canadian Private Sector Privacy Laws*

British Columbia



Personal Information Protection Act
("PIPA BC")



Office of the Information & Privacy Commissioner for British Columbia

Alberta



Personal Information Protection Act
("PIPA AB")

Office of the Privacy Alberta

Federal



Personal Information Protection and Electronic Documents Act
("PIPEDA")



Office of the Privacy Commissioner of Canada

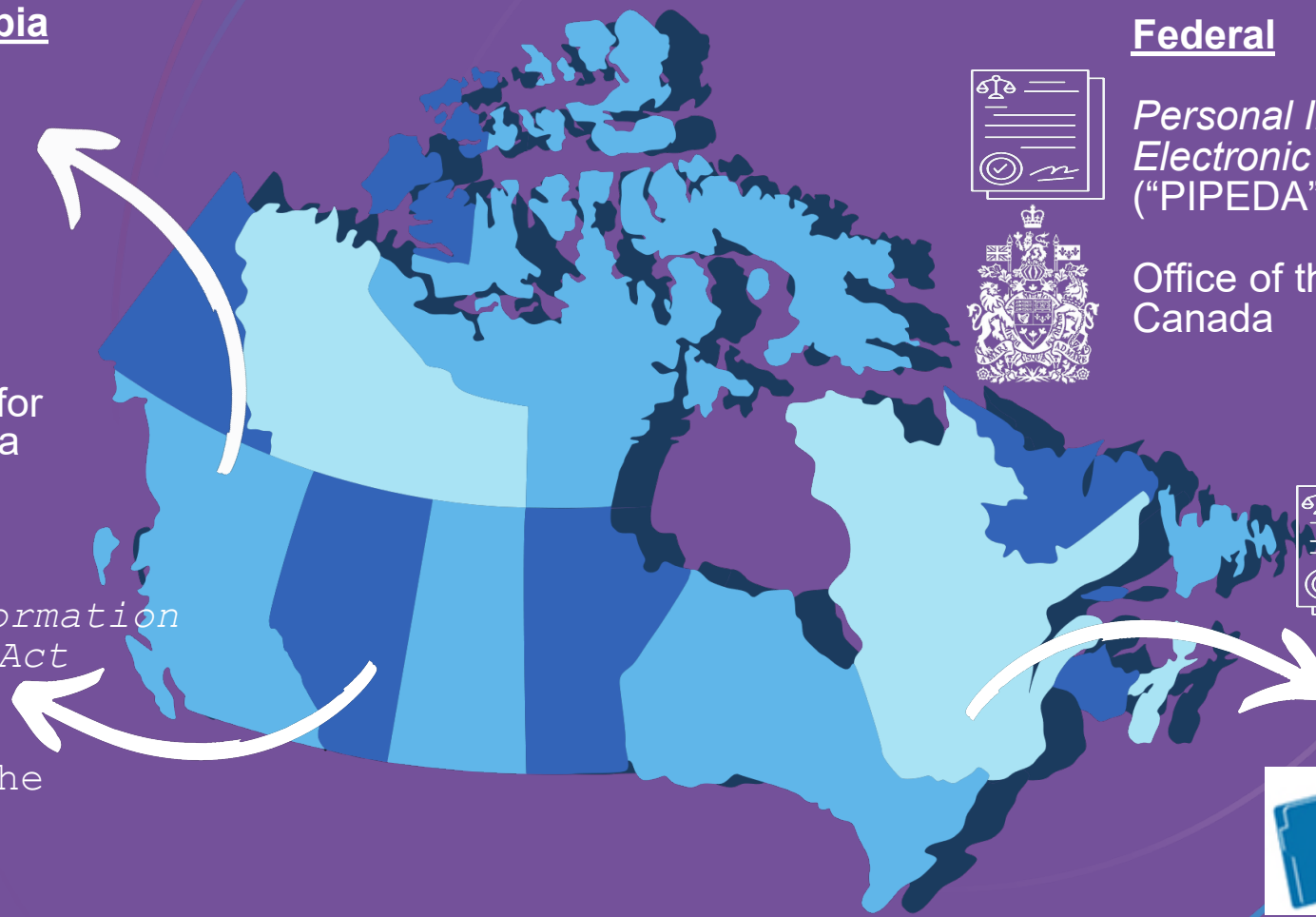
Québec



Act respecting the protection of personal information in the private sector
("Québec Act")



Commission d'Accès à l'Information



* Canada also has federal and provincial legislation governing the public sector, and sector-specific legislation governing personal health information held by "health information custodians".

Canada: Bill C-27

- In November 2020, the federal government tabled Bill C-11, which proposed to overhaul Canada's privacy regime by repealing the personal information-related provisions of *PIPEDA* and replacing them with a new Canadian privacy and data legal framework.
- In 2021, Bill C-11 died on the order of paper due to Canada's federal election.
- On June 16, 2022, the federal government resurrected Bill C-11 with the introduction of Bill C-27 in the House of Commons.
- Part of a global push to strengthen privacy regulations – a trend that commenced with the European Union's General Data Protection Regulation (“**GDPR**”) and Law 25 in Quebec.

Bill C-27: Background and Structure

Part 1: Consumer Privacy Protection Act (CPPA)

- Proposes to replace Part 1 of PIPEDA
- Would apply to **private sector** organizations in Canada that collect, use or disclose personal information in the course of **commercial activities**, and transfer information **across provincial and national borders**
- Would apply to **federally regulated works, undertakings and businesses**

Part 2: Personal Information and Data Protection Tribunal Act (PIDPTA)

- Would introduce a new administrative tribunal
- Tribunal would be responsible for hearing certain **appeals** of decisions by the Office of the Privacy Commissioner of Canada (OPC) under the CPPA
- Tribunal would impose **administrative monetary penalties** (AMPs) under the CPPA following representations by the OPC

Part 3: Artificial Intelligence and Data Act (AIDA)

- Regulate the development and deployment of AI systems in the private sector
- Applies to persons carrying out a "**regulated activity**"
- Proposes are to regulate **international and interprovincial trade and commerce** in AI systems
- **Prohibit certain conduct** in relation to AI systems that may result in serious harm to individuals or harm to their interests

The *Consumer Privacy Protection Act*

- The CPPA increases penalties for contravention of the law. Regulatory powers and penalties include:
 - AMPs of up to the **higher of 3% of gross global revenue or \$10 million**
 - Increased fines for certain serious contraventions of the law, up to a **maximum fine of the higher of 5% of gross global revenue or \$25 million**
 - Auditing and ordering-making powers for the Privacy Commissioner of Canada
 - A **private right of action** against an organization for damages due to a contravention of the CPPA



The *Consumer Privacy Protection Act*


- Bill C-27 proposes the following additional key changes.
 1. Minors' personal information constitutes sensitive personal information.
 2. The "business activity" exemption to consent includes "legitimate interest".
 3. "Anonymized" information is *not* subject to the CPPA.
 4. "De-identified" information is personal information, subject to a few exceptions.


The *Consumer Privacy Protection Act*

- Bill C-27 proposes the following additional key changes.
 5. Privacy management program requirements
 6. Security safeguards
 7. Codes of practice and certification programs
 8. New Individual Rights:
 - Right of disposal
 - Right to be informed of automated decision-making
 - Right to mobility

Status of Bill C-27

Summary

 **Current status**
At consideration in committee in the House of Commons



 **Latest activity**
Second reading and referral to committee on April 24, 2023 (House of Commons)



Progress


Details

About


House of Commons


  **First reading**
Completed on June 16, 2022


  **Second reading**
Completed on April 24, 2023

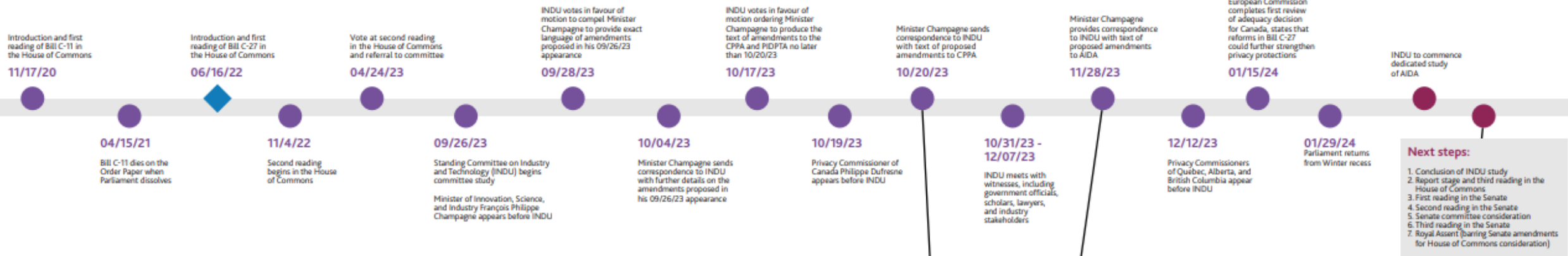
 **Consideration in committee**
In progress

Senate

 **First reading**
Not reached

 **Second reading**
Not reached

 **Third reading**
Not reached



INDU Committee Study to Date:

15 Meetings

69 Witnesses:

- 14 Government Officials
- 18 Scholars
- 20 Industry stakeholders
- 17 Lawyers

Issue	% of meetings addressing issue
Harms arising from AI, including collective harms	65%
The Personal Information and Data Protection Tribunal	60%
Children's privacy	53%
Exceptions to consent requirements (including legitimate interest)	47%
The fundamental right to privacy	33%
Anonymization and de-identification	33%

Amendments proposed by Minister Champagne to Date:

3 categories of amendments to Part 1 of Bill C-27, the Consumer Privacy Protection Act

1. Recognition of the fundamental right to privacy
2. Recognition and reinforcement of the protection afforded to children
3. Increased flexibility for the Privacy Commissioner to reach "compliance agreements"

5 categories of amendments to Part 3 of Bill C-27, the Artificial Intelligence and Data Act

1. High impact systems
2. International alignment
3. Clarifying obligations across the AI value chain
4. Obligations for general purpose systems
5. Clarifying and strengthening the role of the AI and Data Commissioner

Insights from Gowling WLG:

- [Bulletin: Committee study of Bill C-27 to start on September 26](#)
- [Bill C-27: Canada Reintroduces Sweeping Changes to Federal Privacy Law, Proposes New AI Legislation](#)
- [Bill C-27: A Deeper Dive into Canada's Proposed Artificial Intelligence and Data Act](#)
- [Canada's Proposed Privacy Law Moves to Second Reading in the House of Commons](#)
- [The Artificial Intelligence and Data Act \(AIDA\)](#)
- [Preparing for the Consumer Privacy Protection Act: Overview](#)
- [Much needed clarification: Canada sheds new light on proposed Artificial Intelligence and Data Act in companion document](#)
- [Bulletin: Minister Champagne Provides Details on Proposed Amendments to Canada's Bill C-27](#)
- [Opening remarks, as an individual, of Antoine Guilmain, Partner and Co-Leader of the Cyber Security and Data Protection Law Group](#)

Bill C-26: Cybersecurity

- Canada's first federal cyber security law i.e.: a law that focuses on cybersecurity, not *privacy*.
- Amends portions of the federal *Telecommunications Act*.
- Enacts the *Critical Cyber Systems Protection Act* to provide a framework for the protection of the critical cyber systems of services and systems that are vital to national security or public safety and that are delivered or operated as part of a work, undertaking or business within the legislative authority of Parliament.
- “Vital” = critical infrastructure.

Bill C-26: Cybersecurity

Amendments to *Telecommunications Act*:

- Empower the government to compel action by telecommunications service providers (TSP), including
 - Forcing TSPs to terminate service agreements, or
 - Forcing TSPs to cease using certain products and services.
- Unspoken goal is to avoid another Huawei 5G ban debacle by putting an at least partial technology strategy in place

Bill C-26: Cybersecurity

Under the new CCSPA, “vital” organizations must:

1. Create and file with the appropriate regulator cyber security programs
2. Disclose material changes in these to the regulator
3. Take “reasonable steps” to mitigate cyber risks
4. Keep records of steps taken
5. Report breaches

Bill C-26: Cybersecurity

CCSPA enforcement powers delegated to regulators for the 6 vital sectors:

1. Superintendent of Financial Institutions
2. Minister of Industry
3. Bank of Canada
4. Canadian Nuclear Safety Commission
5. Canadian Energy Regulator
6. Minister of Transport

Bill C-26: Cybersecurity

CCSPA Enforcement:

- Regulators may impose finds (\$1 million per individual, including officers and directors; \$15 million per organization) and to issue compliance orders and conduct audits.
- CCSPA imposes responsibility on the organizations to be named later for ensuring that their vendors and supply chains operate securely
- It does not impose liability directly on product and service vendors (e.g. cloud hosting or SaaS providers).

Bill C-26: Cybersecurity

- **Critical Reception:**

- Attacked by civil rights groups for lack of transparency and due process
- Attacked by business groups as too punitive and imposing unnecessary compliance costs on already mature organizations

House of Commons



First reading
Completed on June 14, 2022

Second reading
Completed on March 27, 2023

Consideration in committee
In progress

[Standing Committee on Public Safety and National Security](#) [Study details](#)

Committee meetings

Meeting date	Minutes
February 8, 2024	Meeting_93
February 12, 2024	Meeting_94

Report stage
Not reached

Third reading
Not reached




Senate

First reading
Not reached

Second reading
Not reached

Third reading
Not reached

CANADIAN PRIVACY BREACH NOTIFICATION REQUIREMENTS¹

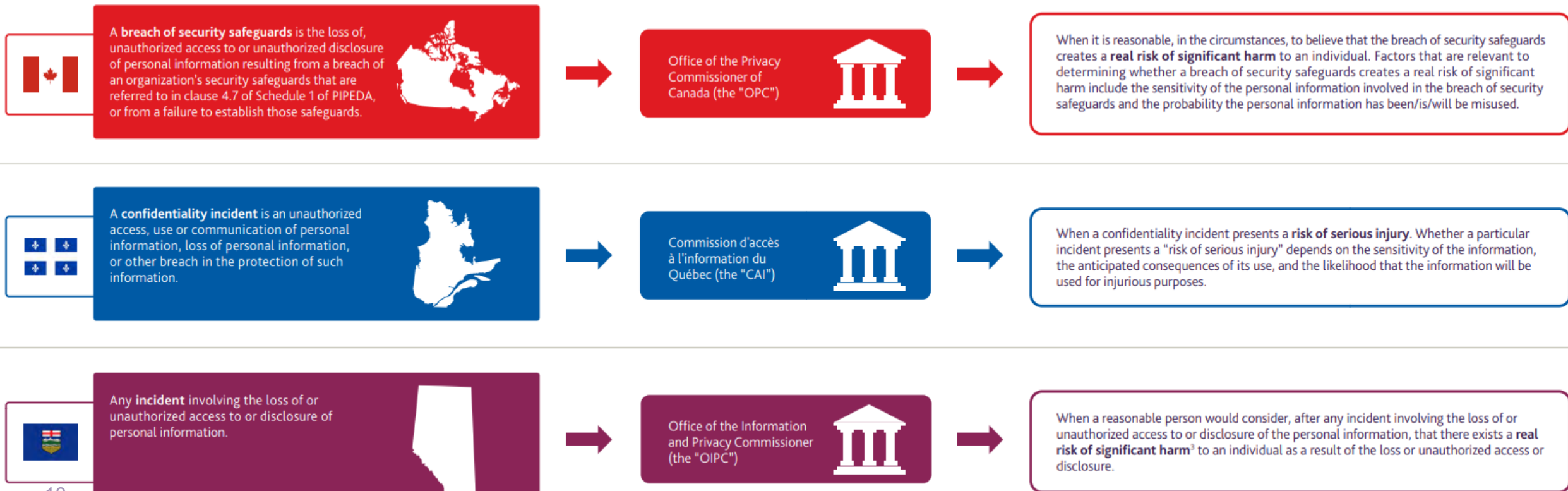
-  Federal privacy legislation is the Personal Information Protection and Electronic Documents Act ("PIPEDA")
-  Québec's privacy legislation is the Act to modernize legislative provisions respecting the protection of personal information ("Québec Act")
-  Alberta's privacy legislation is the Personal Information Protection Act ("PIPA AB")²

WHAT IS A PRIVACY BREACH?

WHO NEEDS TO NOTIFY WHOM?

WHEN IS NOTIFICATION MANDATORY?

The principal organization having control of the personal information must notify the affected individuals and the relevant privacy regulators



NOTIFICATION PROCESS



NOTIFICATION REQUIREMENTS TO PRIVACY REGULATORS: REQUIREMENTS BY JURISDICTION



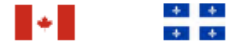
Information about the organization	Canada	Quebec	Alberta
Name of the organization	●	●	●
Contact information of a person within the organization who can answer questions about the breach	●	●	●
Breach description			
Description of the circumstances of the breach	●	●	●
Description of the cause of the breach, if known	●	●	●
Date or period during which the breach occurred (or approximate if unknown)	●	●	●
Date on which the organization became aware of the incident	●	●	●
Description of the personal information that is the subject of the breach if known. If unknown, the reasons why it is impossible to provide such description.	●	●	●
Number of individuals affected by the breach (or approximate if unknown)	●	●	●
Number of individuals affected by the breach in Québec (or approximate if unknown)		●	
Number of individuals affected by the breach in Alberta (or approximate if unknown)			●
Description of risk mitigation steps			
Assessment of the risk of harm to individuals			●
Description of the elements that led the organization to conclude that there is a risk of serious injury to affected individuals		●	
Steps the organization has taken to reduce/mitigate the risk of harm to affected individuals	●	●	●
Steps the organization has taken or intends to take to notify affected individuals of the breach	●	●	●
Steps taken or planned, including those to prevent new incidents of the same nature (with timeline)		●	●
Other			
Updates to be provided to the CAI as soon as possible when known by the organization		●	
Other organizations (e.g. regulators) informed about the incident (if applicable)	●	●	●

NOTIFYING AFFECTED INDIVIDUALS: REQUIREMENTS BY JURISDICTION



Direct Notice	Canada	Quebec	Alberta
Notice must be given directly to the affected individuals, unless prescribed circumstances for indirect notices are otherwise legislatively provided	●	●	●
Breach description			
Description of the circumstances of the breach	●	●	●
Date or period during which the breach occurred (or approximate if unknown)	●	●	●
Description of the personal information that is the subject of the breach if known. If unknown, the reasons why it is impossible to provide such description.	●	●	●
Description of risk mitigation steps			
Steps the organization has taken to reduce/mitigate the risk of harm to affected individuals	●	●	●
Steps affected individuals could take to reduce/mitigate the risk of harm	●	●	
Contact information of a person who can answer for the organization questions about the breach	●	●	●

RECORD-KEEPING OBLIGATIONS



Breach description	Canada	Quebec
Description of the circumstances of the breach	●	●
Date or period during which the breach occurred (or approximate if unknown)	●	●
Number of individuals impacted by the breach and the number of individuals residing in Québec (or approximate, if unknown)		●
Description of the personal information that is the subject of the breach if known. If unknown, the reasons why it is impossible to provide such description.	●	●
Description of risk mitigation steps		
Description of the elements that led to conclude that there is a risk of serious injury to affected individuals		●
Assessment of the risk of harm to individuals	●	
If the incident presents a risk of serious injury/real risk of significant harm, the dates of transmission of the notices to the privacy regulator and to the persons concerned. If indirect notification, the rationale justifying it	●	●
Steps the organization has taken to reduce the risk of harm to affected individuals		●
Other		
Date on which the organization became aware of the incident		●
Minimum duration for which the breach record is kept		2 years
		5 years

Cybercrime and Canadian Business

- **Statistics Canada, *Impact of cybercrime on Canadian businesses (2021)*:**
 - Just under one-fifth of Canadian businesses were impacted by cyber security incidents in 2021
 - Canadian businesses reported spending over \$10 billion on cyber security in 2021
 - Impacted businesses spend more to prevent and detect cyber security incidents
 - Canadian businesses are implementing formal policies for cyber security

Incident Planning

- Verify technical and physical information security measures meet legal obligations
- Secure breach assistance (legal, forensics, other) in advance
- Incident response plan and related policies in place
- Conduct regular data breach exercises (i.e. table top exercises)
- Cyber insurance (if you can get it)
- Pass privacy obligations downstream to vendors via contract provisions

Anatomy of a Cyber Breach Response

1. Stop the bleeding

- Identify nature of breach and contain
- Contact:
 - Insurer (if you have cyber coverage), breach coach / legal
 - Data forensics
 - Public relations

2. Investigate

- Identify source / cause of breach
- Preserve evidence
- Who's affected?
- Determine potential exposure

3. Notifications & message management

- Is there a “real risk of significant harm”
- Notify affected parties & report to privacy commissioner(s)

4. Remediation

- Look after the people affected
- Plug holes in your cyber security

Anatomy of a Cyber Breach Response

- **Lessons learned and continuous improvement**
 - Remediate security deficiencies identified by forensic investigator
 - Document changes / improvements made
 - Update incident response plan and policies as required
 - Key is to be able to show courts and regulators recognition of deficiencies in breach preparedness, responsible attitude toward affected parties, and proactive improvement of security posture

Questions?

Who to contact

Brent J. Arnold is a partner practising in Gowling WLG's Advocacy department, specializing in cyber security and commercial litigation. He acts for plaintiffs and defendants in data breach-related litigation, and serves as breach coach / counsel for companies affected by cyber attacks. In 2019, he co-authored the Canada chapter of Chambers *Global Practice Guide: Data Protection & Cybersecurity*, 2nd ed. In 2022, he co-authored the Canada chapter of the Chambers *Fintech 2022: Trends and Developments* report.

Brent chairs the Steering Committee for the Cybersecurity and Data Privacy section of the U.S.-based Defence Research Institute (DRI), and is past chair of the Ontario Bar Association's Privacy and Access to Information Law Committee. He currently serves on the Ontario Bar Association Council.

He is a Director of the Canadian chapter of the Internet Society, a global organization devoted to improving the affordability, accessibility, fairness and security of the internet. He is also a member of The Advocates' Society's Artificial Intelligence & Automated Decision Making Task Force, and International Association of Privacy Professionals, and the International Association of Defense Counsel.



Brent J. Arnold

Partner & Data Breach Coach / Counsel,
Advocacy Department
Toronto

☎ +1 416-369-4662

📱 +1 416-347-2737

✉ Brent.Arnold@gowlingwlg.com

 www.linkedin.com/in/brent-arnold-cyberlawyeryyz

 cyberlawyeryyz

 @cyberlawyeryyz.bsky.social

Who to contact

Jasmine Samra is recognized as a certified information privacy professional by the International Association of Privacy Professionals. Jasmine advises clients on a broad range of privacy and cyber security issues across a variety of industries. She advises companies on privacy compliance and data protection issues, and helps organizations develop privacy compliance programs, privacy and social media policies. Jasmine provides privacy advice in connection with corporate transactions, outsourcing arrangements and transborder data flows.

Jasmine has extensive experience in requests under Canada's Access to Information Act and provincial freedom of information legislation, and assists clients in protecting confidential third-party business information under these laws. She also helps clients manage and respond to data breaches and other privacy-related incidents.

She regularly advises on compliance with Canada's Anti-Spam Legislation and has created anti-spam compliance policies and programs.

Prior to joining Gowling WLG, Jasmine served as senior counsel at one of Canada's largest financial institutions. In this role, she was responsible for providing legal advice with respect to a range of issues affecting the privacy, cyber security and social media for various lines of businesses.



Jasmine Samra

Counsel

Toronto

+1 416-369-6676

Jasmine.samra@gowlingwlg.com

www.linkedin.com/in/jasmine-samra-02aa2254

Who to contact

Alycia Riley is a lawyer practising in privacy and employment law, specializing in the technology industry. She manages diverse employment matters at all stages of the litigation process and maintains a robust solicitor practice.

On employment matters, Alycia's practice centres on helping her clients develop strong and collaborative teams. She provides practical advice on a broad spectrum of legal matters, including recruitment, employee and labour relations, health and safety, and human rights. Alycia regularly assists employers with developing comprehensive compensation programs and implementing their strategic and operational initiatives for managing their workforce.

Recognized as a Certified Information Privacy Professional by the International Association of Privacy Professionals, Alycia advises clients on a broad range of privacy and cyber security issues, including privacy compliance, data protection, and privacy program management.



Alycia Riley

Associate

Toronto

 +1 416-369-7249

 Alycia.Riley@gowlingwlg.com



GOWLING WLG