ACCESSPRIVACY BY OSLER

Osler, Hoskin & Harcourt LLP

2024: The Privacy Law Year In Review

AccessPrivacy: January Monthly Privacy Call

January 29, 2025

OSLER



Adam Kardash

Co-Chair, Privacy and Data Management

National Lead, AccessPrivacy



Éloïse Gratton, Ad. E.

Co-Chair, Privacy

and Data Management



Kristian Brabander

Partner, Disputes



Joanna Fine

Partner, Privacy and Data

Management



John Salloum

Partner, Privacy and Data

Management



Rosario G. Cartagena

Special Counsel, Privacy

and Data Management



François Joli-Coeur

Partner, Privacy and Data

Management

Session Overview

1. Privacy and Data Legislative reform

- Federal privacy and data legislation reform update/key themes
- Provincial privacy law reform
  - Private sector
  - Health
  - Public sector

2. Key Themes and Regulatory Guidance

- Anonymization/de-identification
- Data portability
- Deceptive design
- Biometrics
- Youth privacy

3. Artificial intelligence

- Automated decision-making
- Standards

4. Incident Response Key Themes and Guidance

- Key practice themes
- Regulatory developments

5. CASL Update

6. Litigation snapshot

Legislative Reform Update: Federal

Current Status of Federal Bills:

- Over the past few years, the Federal Government had introduced a suite of data related legislative proposals:
  - Bill C-27: Sought to enact the *Consumer Privacy Protection Act* (CPPA), the *Personal Information and Data Protection Tribunal Act* and the *Artificial Intelligence and Data Act* (AIDA).
    - Would replace existing federal privacy legislation (PIPEDA) and create the first AI law in Canada
  - Bill C-26:Sought to enact the *Critical Cyber Systems Protection Act* and amend the *Telecommunications Act*.
  - Bill C-63: Sought to enact the Online Harms Act
  - Bill S-8: Would have imposed age verification requirements on platforms.

All federal government bills "died on order paper" when Parliament was prorogued on January 6th.

- ***Note**: The *Consumer-Driven Banking Act*, establishing an open banking framework, received Royal Assent in June 2024. This statute is unaffected by prorogation, despite the fact that key sections are not yet in force.

Legislative Reform Update: Provincial Private Sector

Quebec: Law 25

- Final phase of Law 25 amendments are now in effect
  - Data portability obligations in force September 2024
- New anonymization regulation in force
  - Applicable to private sector organizations and public sector entities
  - Most obligations in force May 2024
  - Record-keeping obligations in force January 2025
- Bill 73: *An Act to counter non-consensual sharing of intimate images and to improve protection and support in civil matters for persons who are victims of violence*
  - Received assent December 2024

Alberta: PIPA Reform

- The statutorily-mandated review of the Alberta *Personal Information Protection Act* commenced on January 22, 2024
- Reviewing committee's report due by July 2025

Legislative Reform Update: Provincial Private Sector

Alberta: PIPA Reform (cont'd)

- OIPC Alberta made a series of recommendations during the May 2024 consultative period, including:
  - Recognizing privacy as a **fundamental human right**;
  - Expanding applicability to **political parties and non-profit organizations**;
  - Creating **additional data subject rights**, including a right of access, a right to be forgotten, a right to data portability, and rights relating to automated decision-making
  - Introducing protections for **children's privacy**
  - Requiring organizations to implement **privacy management programs and conduct PIAs** in prescribed circumstances
  - Enhancing **safeguarding, notice, and breach reporting** obligations
  - Creating new obligations related to **service providers**
  - Introducing **de-identification, anonymization and synthetic data** provisions, and defining sensitive data
  - Strengthening **enforcement** regime (e.g., fines, AMPs, greater discretion for order-making)
- Additional recommendations were made by the OPC and the OIPC BC

Legislative Reform Update: Provincial Private Sector

British Columbia

- OIPC BC's submission to Alberta's PIPA reform consultation (indicating top priorities for PIPA BC review in 2027):
  - Five key recommendations: (i) data portability rights, (ii) rules governing automated decision-making, (iii) requirements for organizations to ensure service provider compliance, (iv) stronger notice requirements, and (v) meaningful enforcement measures (including AMPs)
- *Intimate Images Protection Act*: in force January 2024
  - Provide new civil remedies for complainants whose intimate images have been published or shared without their consent
  - Includes remedies against "internet intermediaries" that host or index third party platform through an online platform

Ontario (Employment Law Updates)

- *Working for Workers Four Act*, 2024: Royal Assent March 2024
  - Amends the *Employment Standards Act*, 2000 to include new job posting requirements
    - Including obligation to disclose the use of AI in the hiring process to screen, select and assess applicants for publicly advertised job postings
  - ESA amendments not yet in force

Legislative Reform Update: Provincial Health Privacy Law

Quebec's New Health Privacy Legislation: "Law 5"

- Applies to the processing of "**health and social services information**" by "**health and social services bodies**" (may be private or public sector)
- Preempts the application of the Quebec Privacy Act
- Impact on private sector:
  - "**Health and social services bodies**": include private health clinics
  - **Service providers**: prescriptive requirements for outsourcing contracts + PIA requirement for transfers outside of Quebec
    - The Minister may determine cases and circumstances in which only a **certified technological product or service** may be acquired or used by a body
- Imposes stringent **governance** obligations, such as:
  - The person with the highest authority is the "person in charge of the protection of health information"
  - Establishing an information governance policy setting out prescribed information
  - Conducting privacy impact assessments
  - Providing training recognized by the Minister

Legislative Reform Update: Provincial Health Privacy Law

Updates to the *Personal Health Information Protection Act, 2004*

- 1. Administrative Monetary Penalties ("AMPs") came into effect (January 2024)
  - Penalties are up to a maximum of $50,000 for individuals and $500,000 for organizations
- 2. Bill 231 - the *More Convenient Care Act* (December 2024)
  - New schedule under PHIPA: creates service to enable individual patient access to PHI in the provincial Electronic Health Record (EHR)
  - Ontario IPC concerns include:
    - Narrowing of existing access rights to health records
    - Future rule-making could undo established rights and requirements under PHIPA;
    - Digital Health ID scheme relies on open-ended authority and allows for potentially unjustified use; and
    - Incomplete and inconsistent oversight regime

Policy Impact of Health Privacy Updates - Ontario Perspective

1. **Revised *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*** (Jan 2024)
2. **IPC PHIPA Decision 243** (May 2024)
    - Research ethics non-compliance
3. **IPC Guidance - Privacy and Access in Public Sector Contracting with Third Party Service Providers** (June 2024)
    - Focuses on access to information and privacy responsibilities related to outsourcing of services that involve the processing of records and/or personal information
4. **IPC Report - Exploring the Potential for a Privacy Regulatory Sandbox for Ontario** (Dec 2024)
    - Insights on how regulatory privacy sandboxes can be used to support the development, testing, and validation of new products or services

Legislative Reform Update: Provincial Public Sector

- **Alberta's Bill 33, the *Protection of Privacy Act* and Bill 34, the *Access to Information Act***
  - Both received Royal Assent on December 5, 2024
  - Bill 33 and Bill 34 will supersede and "split" the existing Alberta F*reedom of Information and Protection of Privacy Act* into two new pieces of legislation
  - Each introduce new more robust obligations for public-sector information governance in Canada
  - Changes will impact public sector entities as well as third parties who provide services to public sector entities
  - Concerned raised by the Alberta Privacy Commissioner were not addressed

Legislative Reform Update: Provincial Public Sector

Alberta's Bill 33, the *Protection of Privacy Act*

- Significant changes from the previous *Freedom of Information and Protection of Privacy Act* (FOIP), including:
  - New privacy management program, PIA, and breach notice obligations for public bodies
  - New concept of "Non-Personal Data", including anonymized and synthetic data
  - New definition of biometric data
  - New notice requirements surrounding automated decision-making
  - Enabling "data-matching" between public body databases for limited uses

Alberta's Bill 34, the *Access to Information Act*

- Significant changes from FOIP, including:
  - Expanded exceptions to the right of access
  - New authority to disregard requests
  - Heightened obligations for requestors to provide adequate detail
  - New qualifications on public bodies' obligations to provide access ("reasonable and practical" threshold)
  - Lengthening of response timelines

Legislative Reform Update: Provincial Public Sector

Ontario: Bill 194

- Background: increasing focus on cybersecurity resiliency and responsible AI in the public sector.

Schedule 1: The *Enhancing Digital Security and Trust Act*

- Cybersecurity regulations
- AI framework
- Governing "prescribed digital information" relating to minors

Schedule 2: Amendments to FIPPA

- Mandatory PIAs
- Personal information breach reporting and notification
- Enhanced oversight and enforcement power for the Ontario IPC (and whistleblower protection)

Anonymization/de-identification

Quebec Privacy Act, section 23

- Where the purposes for which personal information was collected or used are achieved, the person carrying on an enterprise must destroy the information, or anonymize it to use for person carrying on an enterprise must destroy the information, **or** anonymize it to use it for **serious and legitimate purposes**, subject to any preservation period provided for by an Act.
- For the purposes of this Act, information concerning a natural person is anonymized if it is, **at all times**, reasonably foreseeable in the circumstances **that it irreversibly no longer allows the person to be identified directly or indirectly**.
- Information anonymized under this Act must be anonymized according to generally accepted **best practices** and according to the criteria and terms determined by regulation

Anonymization/de-identification : ***Regulation respecting the anonymization of PI***

New obligations	Section
Supervision of anonymization process by a person qualified in the field	4
Removal of all personal information that allows the person concerned to be **directly identified**	5
Conducting of **preliminary analysis** of the re-identification risks	5
Establishing **anonymization techniques** and security and protection measures, **+** implementing the techniques and measures	6
Conducting an analysis of the **re-identification risks** following the anonymization process	7
Periodically reconducting an analysis of the **re-identification risks**	8
Maintaining a **register** **In force as of January 1, 2025.*	9

Anonymization/de-identification :

- Information and Privacy Commissioner of Ontario issued draft de-identification fact sheets for targeted consultation in late 2024.
  - Detailed 50 page guidance consisting of 11 fact sheets building on the IPC's June 2016 De-identification Guidelines for Structured Data.
  - Canadian Anonymization Network (CANON) and AccessPrivacy hosted a workshop in December 2024.
- Alberta's Bill 33 imposes requirements on a public body's use of "non-personal data" which is defined to include data that has does not identify any individual, and includes synthetic data, broadening the scope of the act, and increasing scrutiny on approaches.
- OPC signed on to G7 report "Reducing Identifiability in Cross-national Perspective" in October 2024:
- Concept of anonymization/de-identification will likely be a feature of future private sector and health privacy legislative reform, supplemented by domestic & foreign standards & technological developments.

Data portability

- **Scope of the right to data portability** (Quebec Privacy Act, s. 27 para 3)
  - Right to receive (and to have transferred to a person or body authorized by law) computerized personal information, collected from the individual, in a **structured, commonly used and technological format** (e.g. CSV, XML et JSON).
    - Excludes non-computerized information (i.e., paper documents);
    - Excludes information collected from third parties;
    - Excludes "created or derived" information.



- **Exemptions** (Quebec Privacy Act, s. 27 para 3 and ss. 37-41)
  - Where it raises "**serious practical difficulties**" (e.g. high costs, technical complexity…etc.)
  - Where information is exempt from the right of access (e.g., likely to reveal personal information about a third person)

Data portability

- Increasing focus on data portability as a consumer right will have implications to consumer data frameworks, including open banking.
  - Data portability is a central feature of many open banking initiatives that have been implemented or proposed around the world.
  - Partnerships with intermediaries will play a crucial role in consumer-driven banking in Canada, by facilitating permission-based secure data sharing, ensuring that sensitive information remains protected.
- The federal government enacted a legislative scheme for “open banking” in the form of the *Consumer-Driven Banking Act* (CDBA) in 2024.
  - Not yet in effect, but received Royal Assent, and so not impacted by prorogation.
  - The CDBA is an “open banking” initiative designed to enhance consumer access and control over their financial data and to facilitate innovative financial services.
  - In essence, a consent-based data portability regime.

Deceptive Design Patterns: OPC's 2024 Sweep

OPC conducted a compliance sweep of 145 websites and apps based on five criteria identified by the Organization for Economic Co-operation and Development (OECD):

1. Complex & Confusing Language
2. Interface Interference
3. Nagging
4. Obstruction
5. Forced Action

Deceptive Design Patterns: OPC's 2024 Sweep

- **99%** of websites and apps had **at least 1 indicator** of deceptive design
- **Complex and confusing language** in privacy policies: most common pattern found
- **Obstruction** was also commonly cited in connection with **account deletion** (only 25% made the option available in 2 clicks or less, and sweepers could not find an option on 43%)

Deceptive Design Patterns: OPC's 2024 Sweep

- **Retailer apps and websites** accounted for ~**50%** of the sweep's focus
- **News**, **media**, **gaming** and **entertainment** represented ~11%

Notable items:

- **Length of privacy policies** was a key criticism in the report
  - > 3000 words is deemed to be "complex and confusing language"
  - 96% of websites and apps swept contained this indicator (compared to 89% globally)

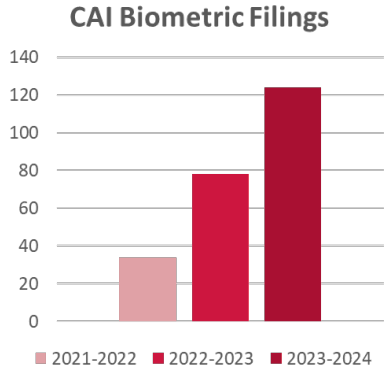
- **Public naming & process**
  - OPC did not contact all of the organizations named in the report prior to publication
  - Follow up correspondence also being sent to organizations not named in the report

Biometrics in Quebec – Legal Framework

- Regulated by Quebec Privacy Act **and** the *Act to establish a legal framework for information technology* (IT Act).
- Main categories of biometric information: behavioural, physical and biological
  - Sensitive information under the *Private Sector Act*
- Requirements for the processing of biometric information in Quebec under the law and CAI guidance
  - Collection of biometric information must be **necessary** for the purposes determined (legitimate, important and real objective), and must be **proportionate** to the intended purpose (rationally connected to the objective, minimal invasion, more using than harmful).
  - Organizations must obtain **express consent**, providing biometric information must be **optional**, and an **alternative solution** must be offered.
  - Organizations must **declare to the CAI:** (i) the use of biometric information for ID verification or confirmation purposes and (ii) the creation of a biometric database (at least 60 days before it is put into service).
- **Broad regulatory powers to issue orders** including any relevant order, and even a ban on the use of the biometric system entirely.

Biometrics in Quebec – Trends

- The number of **biometric declarations** to the CAI has consistently increased in the last three years
- The CAI has taken enforcement action against companies that use these technologies and expressed skepticism about the necessity and proportionality of such tools
  - **Guide on biometrics** (2022): CAI expressed concern about the growing reliance on biometric technologies and warned against trivializing their potentially significant privacy implications
  - **Report on biometric time clocks** (2023): CAI concluded that most workplace biometric time clock systems it reviewed failed to meet the strict legal thresholds of necessity and proportionality under the Québec Privacy Act
  - **Letters of non-compliance**: in our experience in the last few years, organizations that declare their use of a biometric system to the CAI often receive response letters regarding potential non-compliance
  - **Decisions and orders**: in a decision published in December 2024, the CAI concluded that the employer's collection of sensitive biometric data for access control purposes did not meet the requirements of the Quebec Privacy Act



OPC Draft Guidance for processing biometrics – for organizations

- Draft guidance published in 2023
  - Public consultation process ended February 2024
  - Submissions from consultation currently under review by OPC
  - Guidance contains “You Must” and “You Should” for various requirements:
    - Identifying an Appropriate Purpose
    - Consent
    - Limiting Collection
    - Limiting Use, Disclosure, and Retention
    - Safeguards
    - Accuracy
    - Accountability
    - Openness

Youth Privacy

- Canadian privacy regulators increasingly focused on youth privacy in 2024, including:
  - OPC's **Privacy & Age Assurance Consultation**
    - "Age assurance" refers to the process of determining a user's age within certain levels of confidence (e.g., through a declaration, verification, or estimation process)
    - Consultation document set out preliminary opinions related to the use of age-assurance systems (e.g., should be used in situations that are high risk to best interests of youth)
  - Public statements by the OPC in connection with ongoing investigations that they have findings forthcoming that will be relevant to privacy practices as they relate to younger users

Youth Privacy

- Canadian privacy regulators increasingly focused on youth privacy in 2024, including:
  - OPC issued a “Statement on AI and Children” with other G7 Data Protection Authorities
    - Statement called for close monitoring of the impact of AI’s use on children and young people given their vulnerabilities (e.g., limited life experience)
    - Statement identified several area of concern:
      - AI-based decision making
      - Manipulation and deception
      - Training of AI models

Youth Privacy

- Canadian privacy regulators increasingly focused on youth privacy in 2024, including:
  - OPC funded of research projects related to children's privacy, including projects to:
    - assess **mobile gaming application** terms and identify best practices; and
    - assess current law regarding the use of **emotional AI** with children
  - CAI submitted a brief to the Select Committee on the Impacts of Screens and Social Media on Young People's Health and Development that:
    - Called for extending Quebec's **prohibition on advertising to minors** to include 13-17 year olds;
    - Urged caution and restraint around the use of age assurance

Youth Privacy

- The Ontario Government also created the **Enhancing Digital Security and Trust Act** through Bill 194:
  - Applies to **children's aid societies and school boards** and enables the creation of regulations about "**digital information**" relating to individuals under 18
  - Governs how such entities collect, use and disclose digital information
  - Requires children's aid societies and school boards to file reports regarding their privacy practices
  - Prohibits certain prescribed digital information of minors from being collected

AI: Automated Decision-Making Requirements in Quebec

- Section 12.1 of the Quebec Privacy Act governs decisions made by AI systems
  - Organizations must inform individuals when a decision is made based exclusively on an automated processing of personal information (e.g., based on AI), not later than at the time it informs the person of the decision
  - Individuals also have the right to request: (i) details about the personal information used to render the decision, (ii) reasons and principal factors and parameters leading to the decision, (iii) their right to have their personal information corrected
  - Individuals have the right to submit observations to someone in a position to review the decision
- Practical issues
  - What is a decision? To which extent does it need to have an effect on the individual?
  - What is a decision based exclusively on automated processing? Does it exclude decision-making tools?
  - What are acceptable means to inform individuals of an automated decision? Is a privacy policy acceptable?
- Related obligations and best practices
  - Performing a PIA (may be required under s. 3.3), which may include an algorithmic impact assessment
  - Organizations must ensure the accuracy of personal information (s. 11), and automated decisions based on inaccurate information will lead to inaccurate decisions
  - Information used to make a decision must be retained for at least 1 year (s. 11 para. 2)

AI: Canadian Standards

- Despite the proposed *AIDA* dying on order paper, there has been considerable development of standards, codes of conduct, and other guidance across the Canadian data environment:
  - Osler survey of AI standards and guidance across Canada included more than 115 instruments, plus a flurry of foreign and transnational intruments
    - Example - International Standards Organization (ISO) has published 16 standards specifically relating to artificial intelligence

Government Oversight and Strategy

Federal

- The International Network of AI Safety Institutes: Mission Statement (ISED, November 2024)
- Canada launches Canadian Artificial Intelligence Safety Institute (ISED, November 2024)
- Joint ministerial statement between Canada and the UK on advancing artificial intelligence safety (ISED, May 2024)
- Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems (ISED, September 2023)
- Pan-Canadian Artificial Intelligence Strategy (ISED, July 2022)
- Advisory Council on AI: Annual Report (ISED, 2021)
- Advisory Council on AI: Annual Report (ISED, 2020)

Quebec

- Prêt pour l'IA : Répondre au défi du développement et du déploiement responsables de l'IA au Québec (Conseil de l'innovation du Québec, January 2024)

Office of the Privacy Commissioner of Ontario (IPC)

- Podcast episode: Artificial intelligence in Health Care - Balancing innovation with privacy **(June 2024)**
- Presentation to the National Institutes of Health Informatics (NIHI): Health Privacy Trends in Ontario **(December 2023)**
- Blog post: Keeping it real in 2023 **(December 2023)**

Office of the Information and Privacy Commissioner of Alberta

- Guidance for Small Custodians on the use of Artificial Intelligence **(November 2023)**

Office of the Information and Privacy Commissioner for Newfoundland and Labrador

- Submission of the Office of the Information and Privacy Commissioner to the Personal Health Information Act Review Committee **(May 2023)**

Self-Regulated Professional Bodies

College of Physicians and Surgeons of Ontario

- Privacy Principles to Guide Artificial Intelligence Use **(March 2024)**
- Can AI Boost Safety and Quality in Patient Care? **(September 2023)**

College of Physicians and Surgeons of British Columbia

- Ethical Principles for Artificial Intelligence in Medicine **(revised October 2024)**
- Position Statement: Introducing new technology and artificial intelligence in diagnostic facilities **(March 2024)**

Collège des médecins du Québec

- Pistes de réflexion sur l'intelligence artificielle **(June 2024)**

College of Physicians and Surgeons of Alberta

Health

Table of Contents

- Legislation and Regulations
  - Quebec
- Private Sector Industry
  - Government Oversight and Strategy
- Public Sector: Standards, Policies, and Directives
- Regulatory Authorities: Publications and Resources
  - Privacy Regulatory Authorities
    - Joint Publications by Privacy Regulatory Authorities
    - Office of the Privacy Commissioner of Ontario
    - Office of the Information and Privacy Commissioner of Alberta
    - Office of the Information and Privacy Commissioner for Newfoundland and Labrador
  - Self-Regulated Professional Bodies
    - College of Physicians and Surgeons of Ontario
    - College of Physicians and Surgeons of British Columbia
    - Collège des médecins du Québec
    - College of Physicians and Surgeons of Alberta
    - College of Physicians and Surgeons of Manitoba
    - College of Physicians and Surgeons of Saskatchewan
    - Royal College of Physicians and Surgeons of Canada
- Other Industry Stakeholders: Key Resources
  - Canadian Medical Protective Association
  - Healthcare Excellence Canada
- Resources from Academia, Think Tanks, and other Non-Governmental Bodies

Legislation and Regulations

Quebec

Health privacy law: *Act respecting health and social services information*

Incident Response: Key Themes and Guidance

- Key practice themes
  - Increasing volume of incidents
  - Expanding breadth of incident type
  - Sophistication of threat actors
  - Supply chain focus
  - Critical infrastructure focus
  - Steadily growing incident preparedness/crisis response mandates

- Key emerging developments:
  - Ransomware and multifaceted data extortion attacks
  - Increasingly sophisticated AI facilitated cyber attacks

Incident Response: Key Themes and Guidance

New information security incident reporting regime from Québec's financial sector regulator (AMF)

- Published in October 2024 and effective in April 2025.
- **Scope:** insurers, federations and credit unions, deposit institutions, trust companies and credit assessment agents (FI) operating in Québec and applies to "information security incidents," which are defined as "**an attack on the availability, integrity or confidentiality of information systems or the information they contain.**"
- **Reporting threshold:** when it has been (1) reported to the officers or managers of the FI and has "potentially adverse impacts" or (2) reported, in a notice or otherwise, to a regulatory body or to a person or body with either a legal mandate to prevent, detect or repress offences, or a contractual mandate to compensate for injuries resulting from the incident.
- **Key obligations :** Initial notification to regulator; Notification of developments; Form and contents of notification; Final incident report; Incident register; and Information security incident management policy

Incident Response: Key Themes and Guidance

Publication of privacy regulators' breach notification decisions

- **Alberta:**
  - Canada's first private sector privacy law requiring organizations privacy breach reporting (2010)
  - Decisions confirming a real risk of significant harm were made available on the OIPC website: Breach Notification Decisions – Office of the Information and Privacy Commissioner of Alberta
  - Over the last 14 years, the AB OIPC has published over 1000 breach notification decisions
  - On April 1, 2024, the AB OIPC announced that it will cease publishing breach notification decisions (prioritizing resources on failure to report breaches) + more reliance on breach PIPA Privacy Breach Notification Form
- **Quebec:**
  - Mandatory breach reporting and notification obligations since September 2022
  - Since April 2023, the CAI began publishing on its website each quarter the names of all organizations who submitted reports: Accès à l'information… | Commission d'accès à l'information du Québec

Canada's Anti-Spam Legislation

- 2024 CASL Enforcement Update
  - CRTC continues to receive a high volume of complaints to the Spam Reporting Centre
    - Over 205,000 complaints received between April 1 and September 30, 2024
  - Actively enforcing CASL but no published enforcement decisions in 2024
    - Trend towards use of Warning Letters as initial enforcement tool
      - 17 Warning Letters issued between April 1 and September 30, 2024
  - Anticipate emphasis on increased transparency about enforcement action by new CRTC Chairperson
- Abandoned Cart Guidance – FAQ May 2024
  - "*If a potential customer provides an email address or a phone number when putting items into an online shopping cart, but does not complete the purchase nor otherwise provide express consent to receive commercial electronic messages (CEMs), can the merchant still send CEMs to the address the potential customer provided*?"
    - Does not trigger a purchase EBR or 6 month implied consent based on an inquiry or application
    - CRTC recommends seeking express consent to send abandoned cart emails

Litigation Snapshot

- Canada as a mosaic: A variety of approaches to data breach and misuse of data class actions
- Certification / authorization of class actions is a “filtering exercise” - but the exercise is evolving and approached differently by different Courts
- A number of decisions in data breach / misuse of data class actions in 2024 – brief overview below

- **Ontario**:
  - Del Giudice v. Thompson, 2024 ONCA 70, leave to appeal to SCC dismissed 2024 CanLII 88330
  - Strict application of procedure and pleading rules lead to dismissal of proposed claim
  - Is Ontario no longer the preferred jurisdiction for plaintiffs among the common-law provinces?

Litigation Snapshot (Cont'd)

- **British Columbia:**
  - Ari v. Insurance Corporation of British Columbia, 2024 BCSC 964
  - G.D. v. South Coast British Columbia Transporation Authority, 2024 BCCA 252
  - Campbell v. Capital One Financial Corporation, 2024 BCCA 253
  - Lam v. Flo Health Inc., 2024 BCSC 391
  - Courts (esp. Court of Appeal) finding ways to allow claims to proceed?

- **Quebec**:
  - Option Consommateurs c. Home Depot of Canada Inc., 2024 QCCS 1305 (under appeal)
  - Homsy v. Google, 2024 QCCS 1324
  - Claims may be grounded in punitive damages, even where compensable harm is not found

Thank you for attending!

Contact Us:

(416) 646-3660

info@accessprivacy.com

This document is the sole property of Osler, Hoskin & Harcourt LLP (Osler). Its contents, including text, tables, diagrammatic or other visual representations may not be shared, distributed or reproduced in any form, electronically or otherwise, without the prior written consent of Osler.

We wish to confirm that our discussions will not constitute a solicitor/client relationship in respect of this matter unless and until we are formally retained and it is our expectation that we will not be receiving confidential information from you.