Monthly Privacy Call

2025: The Privacy Law Year In Review

January 21, 2026

info@accessprivacy.com

accessprivacy.com

ACCESSPRIVACY BY OSLER

2025: The Privacy Law Year in Review

Adam Kardash

Co-Chair, Privacy and Data Management

National Lead, AccessPrivacy

Éloïse Gratton

Co-Chair, Privacy and Data Management

Joanna Fine

Partner, Privacy and Data Management

John Salloum

Partner, Privacy and Data Management

Rosario Cartagena

Special Counsel, Privacy and Data Management

François Joli-Coeur

Partner, Privacy and Data Management

Adam LaRoche

Partner, Privacy and Data Management; Employment and Labour

Outline

1. Federal Privacy and Data Legislative Reform
2. Data Sovereignty
3. AI and Privacy
4. Provincial Privacy Legislative Reform: Private, Public and Health Sectors
5. Key Regulatory Guidance:
    - Anonymization/De-Identification
    - Biometrics
    - Youth Privacy
6. Cybersecurity: Developments and Practice Trends
7. Access to Information Requests
8. CASL Update
9. Key Decisions and Litigation Practice Trends

Legislative Reform Update: Federal

Status of Federal Privacy and Data-Related Bills

- Bill C-27: part of the suite of bills that "died on order paper" when Parliament was prorogued in January 2025.
  - **Early 2026**: widely expected that a new federal private sector privacy statute to replace PIPEDA and a companion bill establishing a tribunal to administer a penalty-based enforcement regime will be introduced.
  - The proposed statute is expected to include potentially severe penalties, including the possibility of fines of up to the greater of C$25 million or 5% of gross global revenue, as well as other provisions reflected in the prior version of the CPPA contained in Bill C-27.
  - The new bill is also expected to incorporate measures addressing data sovereignty, children's privacy, and emerging AI technologies.
  - No re-introduction of the *Artificial Intelligence and Data Act* expected: the federal government has indicated that it will seek to regulate the design, development and deployment of AI technologies through privacy legislation, policy and investment, rather than with standalone AI-specific legislation.
- Bill C-8
  - **June 2025:** the federal government introduced a bill regarding critical infrastructure cyber systems – functionally identical to Bill C-26. Bill C-26 died on the order paper in January 2025 after a technical drafting error prevented its passing in December 2024.
  - **Status**: passed Second Reading in October 2025, under consideration by the Standing Committee on Public Safety and National Security.
  - Bill C-8 will establish a new federal framework governing the cybersecurity of Canada's critical infrastructure.

Legislative Reform Update: Federal

Open Banking and Data Portability in Canada

- The *Consumer-Driven Banking Act* (CDBA) passed in 2024: aims to create a data portability framework for securely sharing prescribed types of financial data among "participating entities."
- **November 2025**: In the *Budget Implementation Act* (Bill C-15), the federal government introduced amendments to the CDBA to complete the open banking framework.
    - **Status**: Bill C-15 passed Second Reading on December 10 and has been referred to the Finance Committee for consideration.
- Bill C-15 also introduced complementary amendments to PIPEDA to establish an interoperable data mobility regime, adding a data portability right to existing individual access rights.
    - PIPEDA data mobility amendments will give individuals the right to request that prescribed organizations provide specified personal information (in a structured, commonly used technological format), to an authorized person or organization.
    - Expected development of PIPEDA regulations to operationalize the data sharing framework (e.g. setting standards for security safeguard and interoperability measures).
- **January 15, 2026**: Competition Bureau released report on the significant benefits of data portability for Canadians and the economy generally (insurance industry case study).
    - Defines data portability, sets out opportunities and challenges, and outlines key factors for the creation of a successful Canadian data portability framework
    - In particular: importance of creating trusted guidance and frameworks, establishing clear standards for data types and formats, and prioritizing multi-level interoperability

Data Sovereignty

Background

- Definitions vary, but broadly speaking, concept refers to the **storage** and **processing** of data within Canada's borders and the ensuring that Canadian courts have exclusive authority
- Growing focus on "data sovereignty" at the national level, particularly about ensuring that Canadian data is insulated from search warrants or production orders issued in foreign jurisdictions
    - Particular concern re: US CLOUD Act
    - Legislative and policy options include legislated data localization requirements, legislated risk-based data transfer assessments, regulation or other policy instruments
    - These requirements or policies can be general, sector-specific, or targeted at certain classes of data
- Lessons from BC public sector: removed most restrictive data residency rules "so public bodies can use modern tools while continuing to protect personal information"
    - Strict data residency measures create significant economic and technological costs while often being disproportionate to the level of risk

Data Sovereignty

- **October 2025:** Government of Canada's "sprint" consultation for a new national AI strategy (expected early 2026) considered data sovereignty as a core issue.
- **October 2025:** Québec's legislature passed *An Act respecting the national digital identity* (Law 82).
    - Empowers the Minister of Cybersecurity and Digital Technology to take steps to "reinforce digital sovereignty in the governance and management of information resources, in particular as regards government digital data that contains sensitive personal information".
- **November 2025:** Federal government released its "Digital Sovereignty Framework" and re-published its "White Paper on Data Sovereignty and Public Cloud."
    - Framework outlines key procurement, supply and technical controls to strengthen institutional control over federal government data and information systems
    - White Paper acknowledges that complete digital sovereignty is not possible for public sector data given that business and operational needs require cloud computing technology
- **November 2025:** Federal budget committed significant investment over 5 years towards "sovereign AI infrastructure", building on its Sovereign AI Compute Strategy.
- **2026:** Expected that some degree of data sovereignty measures will be present in federal private sector privacy law reform and in provincial health privacy law reform.

AI and Privacy Trends

2025 saw broader enterprise adoption of AI, with notable privacy implications

- **Growing calls for legislation and governance**
  - In its submission to the consultation on a renewed AI strategy, the OPC called for modernized federal privacy laws and requirements for privacy by design, privacy impact assessments and robust data protection to encourage responsible AI.
  - The Alberta OIPC has recommended standalone AI legislation and a comprehensive governance framework, including mandatory algorithmic impact assessments and transparency requirements for AI decisions.
- **AI-powered resume screening tools have become widespread**
  - Transparency: according to CAI guidance, organizations should disclose the use of these tools in applicant privacy statements and on the user interface. Ontario passed legislation requiring organizations to disclose in their public job postings if AI is used to "screen, assess, or select applicants."
  - Automated decision-making: s. 12.1 of the Quebec Privacy Act governs decisions made exclusively based on automated processing. Is having a "human in the loop" sufficient even if AI does the heavy lifting?
- **Is Agentic AI taking over?**
  - AI systems that can plan, reason and take action towards a defined objective amplify existing privacy risks as they autonomously gather, transmit and analyze data across systems.
  - Amplifies existing privacy and data protection risks associated with AI technologies and raises organizational risks such as prompt injection.

AI and Privacy Trends

AI scribes have joined the meeting

- Raises various privacy issues such as reasonability, consent/right to opt-out, accuracy/reliability, retention of transcription/recording, secondary use for training by vendor.
- Context will impact assessment and requirements.
    - May be inappropriate in certain high-risk context (e.g., HR meetings) and raise additional issues in regulated professions (e.g., healthcare).
- Guidance related to AI scribes has mainly come from health profession colleges. Privacy regulatory authorities also issued guidance in 2025:
    - Saskatchewan OIPC: "Checklist for Healthcare Organizations Considering the Use of a Scribe"
    - Alberta OIPC: "Artificial Intelligence (AI) Scribe Privacy Impact Assessment Guidance as well as Comments Regarding Responsible AI Governance in Alberta"
- Pilot projects in various provinces and support for widespread adoption of AI scribes in the health sector.

Ontario IPC recommendations to hospital following AI scribe privacy breach (October 2025)

- Physician installed an AI scribe on his personal device which had access to his calendar. *The* tool also acted as an AI agent and was able to join and transcribe meetings. After the physician no longer worked for the hospital, the physician's AI scribe accessed a rounds meeting invite via the physician's personal calendar. The AI scribe transcribed the meeting without notice and emailed summaries containing PHI to everyone on the invitation.
- Hospital reported the breach to the IPC and impacted individuals and took immediate steps.
- Additional IPC recommendations to the hospital included: follow-up with the vendor and recipients to ensure that the data was deleted; updating breach protocols, off-boarding protocols, and internal policies (including AI governance and accountability framework); creating new technical barriers such as meeting "lobbies."

Legislative Reform Update: Provincial Private Sector

Alberta: PIPA Reform

- Alberta's legislative committee tasked with reviewing the *Personal Information Protection Act* (PIPA) completed its report in February 2025.
- Alberta's legislature is expected to announce material amendments to PIPA in 2026 based on the committee's 12 recommendations, including:
  - more clearly defining acceptable forms of consent for the processing of personal information,
  - introducing specific obligations regarding children's privacy,
  - creating a penalty-based enforcement regime,
  - defining the "significant harm" threshold for reporting security incidents,
  - introducing notification obligations when automated decision-making systems are used to make decisions about an individual,
  - defining obligations regarding de-identified and anonymized data,
  - bringing non-profit organizations under the scope of PIPA, and
  - ensuring PIPA's interoperability with federal and international privacy laws.

Legislative Reform Update: Provincial Public Sector

Alberta public sector privacy and access legislation:

- **Bill 33, the *Protection of Privacy Act,* and Bill 34, the *Access to Information Act*, came into force in June 2025.**
  - Superseded and "split" the existing Alberta *Freedom of Information and Protection of Privacy Act* into two new pieces of legislation.
  - Each introduced new, more robust obligations for public-sector information governance in Canada.
  - Changes impact public sector entities as well as third parties who provide services to public sector entities.
  - Concerns raised by the Alberta Privacy Commissioner were not addressed.

Legislative Reform Update: Provincial Public Sector

Alberta public sector privacy and access legislation:

- **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 [in force 2026], 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
- **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: Nova Scotia

Introduction of the *Freedom of Information and Protection of Privacy Act* to consolidate related legislation and introduce significant changes (in force 2027):

- The Information and Privacy Commissioner designated as an officer of the legislature
- Municipalities brought within the scope of the legislation
- Introduction of notification obligations following security breaches
- Enhanced penalty-based enforcement framework

***Social Insurance Number Protection Act* (passed October 2025, not yet in force):**

- Applies to private sector organizations
- Generally probits the collection of SINs unless specifically authorized by regulation

Legislative Reform Update: Provincial Public Sector

Ontario public sector privacy and access legislation:

- **Significant Bill 194 amendments to the *Freedom of Information and Protection of Privacy Act* (FIPPA) came into force in June 2025:**
  - Mandatory PIAs
  - Security incident reporting and notification obligations
  - Enhanced Commissioner powers
    - New information-sharing powers and whistleblower protections (effective January 2025)
    - Expanded review and order-making powers
  - Expansion of data processing activities subject to offence provisions

Legislative Reform Update: Provincial Public Sector

Ontario public sector privacy and access legislation:

- ***Enhancing Digital Security and Trust Act* came into force in January 2025:**
  - Background: increasing focus on cybersecurity resiliency and responsible AI in the public sector
    - AI framework
    - Governing "prescribed digital information" relating to minors
    - Draft cybersecurity regulation applicable to colleges, universities, public hospitals, children's aid societies and school boards: consultation period December 2025-February 2026
- **Draft Regulations open for comment until February 9, 2026**
  - Draft *Cyber Security Regulation*
    - Applies to educational institutions under FIPPA, public hospitals, children's aid societies, and school boards
    - Introduces obligations to develop and implement a cyber security program, complete bi-annual cyber security maturity assessments, and report "critical cyber security incidents"
  - Draft *Digital Technology Affecting Individuals Under 18 Regulation*
    - Introduces obligations for school boards to provide notice when students' personal information is disclosed to software companies through software applications in schools

Legislative Reform Update: Provincial Health Privacy Law

Legislative Reform: General Trends

- Following the overhaul of Québec's health privacy regime in 2024, we expect significant discussion over the coming years in other provinces about the modernization of health privacy statutes – focused on facilitating the respectful leveraging of data to improve the delivery of healthcare services.

Ontario Update: Targeted Legislative Amendments

- **Bill 11: *More Convenient Care Act, 2025***
    - Creates Digital Health IDs for all Ontarians
    - Royal Assent: June 2025; PHIPA amendments proclaimed into force January 1, 2026
    - Substantively identical to previous session's Bill 231
        - New schedule under PHIPA: creates service to enable individual patient access to PHI in the provincial Electronic Health Record (EHR)
    - Bill 11 did not address IPC's key concerns regarding either Bill 231 or Bill 11:
        - Narrowing existing access rights to health records;
        - Digital Health ID scheme relies on open-ended authority and lacks appropriate guardrails;
        - Future regulations could undo established rights and requirements under PHIPA;
        - Adding a new prescribed organization role for Ontario Health without clear boundaries; and
        - Creating an incomplete and inconsistent oversight and enforcement regime.

Legislative Reform Update: Provincial Health Privacy Law

First AMP issued by the Ontario IPC (September 2025)

- Under PHIPA, the IPC may impose administrative monetary penalties (AMPs) of up to $50,000 for individuals and $500,000 for organizations, with the power to increase the penalty by the amount of any economic benefit from non-compliance.
    - Severe contraventions may constitute offences, with potential fines of up to $200,000 and/or one year imprisonment for individuals, and up to $1,000,000 for organizations.
- IPC ordered a $5,000 fine against a physician for accessing and using hospital records for personal financial gain; additional $7,500 fine ordered against the physician's private clinic.
- The decision emphasized the importance of demonstrable accountability with regards to PHI obligations, i.e. ***"a repeatable and demonstrable system of data governance whereby organizations can show regulators more concretely, backed by evidence, how they meet their legal requirements in practice."***
- Demonstrable accountability "is intended for organizations to close the trust gap with regulators and with individuals."

Anonymization/De-identification

Ontario IPC Guidance: Timeline

- **2016:** *De-identification Guidelines for Structured Data* guidance published.
- **2024:** Draft de-identification fact sheets released for targeted consultation.
  - In conjunction with the Canadian Anonymization Network (CANON), AccessPrivacy hosted a workshop to discuss the IPC's Draft De-Identification Fact Sheets.
    - Chief Privacy Officers, senior counsel and privacy professionals across a breadth of industry sectors attended the workshop, including representatives from retail, health, banking, telecommunications, trade associations, and other public- and private-sector organizations.
- **October 2025:** "Expanded" De-Identification Guidelines published (96-page document)

Anonymization/De-identification

Key Features of IPC's 2025 Guidance

- **The spectrum of identifiability**
  - Zero risk of re-identification acknowledged as unrealistic in practice; goal of demonstrably reducing risk of re-identification to a very low level.
  - Contextual nature of risk assessments.
- **Updated terminology, definitions and scope of application**
  - Pseudonymization is the process of transforming direct identifiers in a data set. Privacy protective benefits, but generally still considered personal information.
  - De-identification is the process of performing pseudonymization plus transforming indirect identifiers that remain.
    - A properly de-identified dataset no longer contains information that identifies an individual, or information that could be used alone or with other information to identify an individual, based on what is reasonably foreseeable in the circumstances (analogous to "anonymization" in other jurisdictions).
    - The re-identification risk must be measured and demonstrated to be very low.
  - De-identification as a use of PI under privacy laws (does not require consent under PHIPA).
- **Enumerated use cases**
  - Open data; data sharing among related organizations; data sharing with an external third party; custodian-controlled access by a third party; and internal data re-use.
- **12-step process for de-identifying structured data**
  - Includes selecting acceptable re-identification risk threshold, calculating risk, managing risk, and documenting the process.
- **Appendices:** Practical tools and checklists
  - Explicit acknowledgement that checklist items "may need to be adapted or interpreted to the size of an organization".

Biometrics

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
  - Organizations must obtain **express consent**
  - 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).
  - 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

Biometrics in Quebec: Trends

- The CAI has signaled a cautious approach to biometric tools, emphasizing necessity and proportionality, and has exercised robust oversight through orders and prohibitions in recent matters.
- **Transcontinental (2024):** CAI decision addressing an employer's use of facial recognition for access control, highlighting the requirement to substantiate a "real and important" purpose with objective, well-documented evidence beyond convenience or generalized operational challenges.
- **Metro (2025):** CAI prohibition of a retailer's facial recognition pilot for shoplifting/fraud prevention, reflecting concerns with automatic, systematic collection and the inability to obtain express consent at store entry; the CAI's stance confirms that both authentication (one-to-one) and identification (one-to-many) fall within "identity verification or confirmation."
- **Lessons learned for organizations:**
  - **Demonstrate necessity with evidence:** Show a genuine, well-documented problem and that biometrics are necessary and proportionate to address it, not merely convenient.
  - **Offer meaningful alternatives and obtain express consent (cannot rely on consent exceptions for fraud):** Ensure non-biometric pathways exist and that consent is explicit and valid for identity-related biometric uses.
  - **Expect close CAI scrutiny:** Declarations often prompt regulatory review focused on proportionality and consent; prohibitions like Metro illustrate the CAI's willingness to restrict or ban deployments that fail these standards.

Biometrics

OPC Guidance: Updated Taxonomy and Definitions

August 2025: OPC publishes "Guidance for Processing Biometrics – For Businesses" (as well as Guidance for Federal Institutions under the Privacy Act)

- Following draft guidance in 2023, public consultation process (including AccessPrivacy workshop) in 2023-2024
- **"Biometrics":** defined as the "quantification of human characteristics into measurable terms".
- **"Biometric technologies"** include physical biometrics (e.g. fingerprints, facial geometry) and behavioural biometrics (e.g. keystroke patterns, gait, eye movement)
  - Used for various purposes, including recognition (1:1 verification or 1:n identification) and classification
- **"Biometric samples":** data containing unprocessed representations of biometric characteristics (e.g. photos, voice recording)
  - Contain personal information with the potential to be converted into biometric information if processed using a biometric system
- **"Biometric information":** "information about biometric characteristics that has been extracted from a biometric sample."
  - Photographs, video recordings, and behavioral observations are, on their own, not necessarily biometric information until processed using a biometric system.

Biometrics

OPC 2025 Guidance: Biometric Information May or May not be Sensitive

- Historically, the OPC has taken the position that "by its very nature, biometric information is sensitive information."
- The Guidance contemplates that biometric data may or may not be capable of uniquely identifying an individual, and may or may not be sensitive.
    - Biometric information that "can **uniquely identify** an individual is sensitive information, regardless of the context in which it is collected, used, or disclosed" because it is "stable over time, difficult to change, and innately linked with an individual's identity".
    - Biometric information that is not capable of uniquely identifying an individual "**may or may not**" be sensitive depending on the circumstances.
- Biometric information "can be sensitive even if it is only used or retained for a brief period of time" (e.g. facial detection system that creates and retains a numerical representation of facial features for milliseconds).
- The OPC's 2025 guidance states that organizations should generally treat biometric information as sensitive if:
    - It is, or could readily be, combined with other information that would allow it to uniquely identify an individual;
    - Its misuse could pose a high risk of harm to individuals; or
    - It could reveal other categories of information that are considered sensitive (e.g. medical info).

Biometrics

Biometrics: A Condition of Service?

- OPC 2025 Guidance contemplates that consent to biometrics could be required as a conditions of service where integral to fulfill specified and legitimate purposes.
- **Non-integral and non-essential** collections of biometric data must be **voluntary** (and an alternative must be provided)
    - Differs from Quebec approach

Youth Privacy

2025: Youth privacy is a compliance priority in Canada

- **March:** OPC publishes “Consultation on age assurance mechanisms - What we Heard”
- **May:** OPC launches an Exploratory consultation on the development of a children’s privacy code
- **June:** OPC announced the launch of a Youth Advisory Council to help inform efforts by the Office of the Privacy Commissioner of Canada (OPC) to better protect the privacy of young people in the digital age
- **September:** Report of findings of joint investigation into TikTok with a strong focus on children's data
- **October:** Class action introduced in Quebec against more than 20 video game developers alleging illegal collection and disclosure of children’s personal information
- **November:** OPC joins Global Privacy Enforcement Network sweep focused on the protection of children’s privacy

Cybersecurity: Trends and Developments

Key practice themes

- Increasing volume of incidents
- Expanding breadth of incidents
- Sophistication of threat actors
- Supply chain focus
- Critical infrastructure focus
- Steadily growing incident preparedness/crisis response mandates
- Increasing volume of inquiries in privacy regulatory authority investigations

Key emerging developments:

- Ransomware and multifaceted data extortion attacks
- Increasingly sophisticated AI facilitated cyber attacks

Cybersecurity: Trends and Developments

OPC Self-Assessment Tool (March 2025)

- **Purpose:** Web-based tool to assess whether a privacy breach poses a "real risk of significant harm" (RROSH) under PIPEDA, informing whether to report to the OPC and notify affected individuals.
- **How it works:** Structured questionnaire evaluates factors such as the type and sensitivity of information, number of individuals affected, and likelihood of misuse; outputs an indication of whether the RROSH threshold is likely met.
- **Scope and data handling:** Intended for private-sector organizations subject to PIPEDA and federal institutions; information entered is not transmitted to the OPC; results can be saved and included in breach reports to support the organization's assessment.

Key Considerations for Businesses

- **Voluntary and advisory nature:** Use is voluntary and supports internal analysis; it does not replace legal judgment or regulatory discretion and is not an official OPC determination.
- **Sensitivity of results:** Outputs may reveal internal risk assessments, controls, or vulnerabilities; store and share carefully given potential regulatory or litigation scrutiny.
- **Broader regulatory context:** Aligns with PIPEDA's breach reporting framework, but organizations must also account for other applicable federal and provincial privacy laws and evolving OPC guidance on breach management and incident reporting.

Cybersecurity: Trends and Developments

Bill C-8: Federal Cybersecurity Reforms (June 2025)

- **Overview and status:** Reintroduced as Bill C-8, largely identical to Bill C-26 (2022; last published June 2024), and expected to pass without substantial amendment.
- **Telecommunications Act amendments:** Empowers government to direct telecom providers to avoid, remove, or prohibit high-risk products/services, including from vendors controlled by foreign states, even if already deployed.
- **CCSPA creation:** Establishes the Critical Cyber Systems Protection Act, setting baseline cybersecurity obligations for designated federally regulated critical infrastructure (e.g., transportation, energy, banking, telecommunications, nuclear).
- **Key refinements vs. C-26:**
  - Removes the consequential amendment to the Canada Evidence Act.
  - Narrows triggering threats for government orders to "interference, manipulation, disruption, or degradation" (s. 15.1(2)).
  - Reforms judicial review to enhance transparency by limiting confidential national-security submissions.
  - Introduces a new right of appeal for decisions issued during review proceedings.
- **Obligations and oversight:** Designated operators must implement cybersecurity programs, manage supply-chain/third-party risks, and report qualifying incidents; regulators gain broad inspection, audit, and order-making powers (including corrective measures or halts).
- **Impact on organizations:** Raises the national cybersecurity baseline and expectations for governance, risk management, and operational controls; tightens vendor oversight; expands incident reporting and transparency; and heightens board and senior leadership accountability for readiness, assurance, and resourcing.

Access Requests : Emerging Challenges and Practical Implications

- **Rising volume:** Osler Privacy team receiving an increasing volume of mandates to assist organizations in responding to access requests, and investigation mandates arising from complaints related to access request responses.
- **Increasing strategic use:** Access rights-once a transparency tool-are increasingly leveraged in litigation contexts, employment disputes, and to pressure or disrupt operations; requests are often sweeping and extend well beyond simple copies of customer or HR records.
- **AI-amplified scope and complexity:** An increasing share of requests appear AI-generated, demanding "all data," including system logs, metadata, CCTV, algorithmic outputs, and internal correspondence-much of which can be difficult, costly, or impracticable to retrieve in a meaningful way.
- **Third-party implications:** Requests may implicate third parties (e.g., details on complaints, fraudulent accounts opened using another's identity, etc.), raising difficult questions about whose personal information is at issue and what must-or must not-be disclosed.
- **Operational burden and legal risk:** Employee or long-standing client requests drive extensive searches across multiple systems and archives, followed by complex exemption analysis (third-party data, internal investigations, privilege, confidential commercial or security-sensitive information), creating significant resource demands and risk.
- **Misunderstandings of legal limits:** Some requesters conflate access with deletion, overlooking retention policies, legal holds, or preservation obligations that can require keeping data.
- **Regulatory escalation and proof of reasonableness:** More matters are reaching regulators, who may require affidavits or attestations of a "reasonable search"-challenging amid turnover, evolving retention, or lawful deletion, and underscoring the need for robust governance, documentation, and defensible processes.
- **Forward look and adaptation:** With potential PIPEDA reform on the horizon, organizations should reassess whether current frameworks balance individual rights and operational realities (including AI-generated requests and misuse) and adapt processes to respond efficiently, lawfully, and demonstrably.

Canada's Anti-Spam Legislation

2025 CASL Enforcement Update

- CRTC continues to receive a high volume of complaints to the Spam Reporting Centre.
  - Over 152,603 complaints received between April 1 and September 30, 2025
  - 75% of investigations start from a complaint to the Spam Reporting Centre
  - 25% of investigations come from stakeholder referrals (e.g., banks, law enforcement, cybersecurity experts) and online leads
  - Email remains the highest volume of reported spam, followed by text message

- CRTC continues to actively enforce CASL
  - Trend towards use of Warning Letters as initial enforcement tool
    - Between April 1 and September 30, 2025: **123 Warning Letters**; 1 Notice of Violation; 153 Notices to Produce; 5 Preservation Demands
  - One published Notice of Violation on August 13, 2025 and AMP of $50,000:
    - Under Section 7(1)(a) of CASL – prohibition on altering transmission data in an electronic message so that the message is delivered to a destination other than specified by the sender, unless express consent is obtained.
    - From 2020-2023, an individual redirected 49,819 electronic messages.
    - The individual obtained usernames and passwords from darknet marketplaces and used the credentials to access email accounts of individuals. He then set up forwarding rules to redirect incoming emails to his own address and obtain sensitive personal information.

Litigation Snapshot: Privacy Jurisprudence Review 2025

Privacy class action: data breaches

- **Royer c. Capital One Bank (Canada Branch) et al., 2025 QCCA 217**
- **InvestorCOM Inc. v. L'Anton, 2025 BCCA 40**
- Hvitved v. Home Depot of Canada Inc., 2025 BCSC 18
- Shriqui v. Blackbaud Canada Inc., et al., 2024 ONSC 6957
- Donegani v. Facebook, Inc., 2024 ONSC 7153

Biometrics

- **Cleaver v. The Cadillac Fairview Corporation Limited, 2025 BCSC 910**
- Doan c. Clearview AI inc., 2024 QCCS 3968
- Imprimeries Transcontinental inc., Re, CAI1024350-S
- Granger v. Ontario, 2024 ONSC 6503
- **Clearview AI Inc. v. Alberta (OIPC), 2025 ABKB 287**

Privacy litigation: key importance of consent

- **Hogue c. Société canadienne des postes, 2025 QCCS 49**
- E.G. v. Scotiabank (Bank of Nova Scotia), 2024 QCCS 3979

Privacy interests and torts

- Clearview AI Inc. v. Information and Privacy Commissioner for British Columbia,
- 2024 BCSC 2311
- Moon v. International Alliance of Theatrical Stage Employees (Local 891), 2024 BCSC 1560
- **The Hospital for Sick Children v. Information and Privacy Commissioner of Ontario,**
- 2025 ONSC 385
- Lamarche v. British Columbia (Securities Commission), 2025 BCCA 146
- Insurance Corporation of British Columbia v. Ari, 2025 BCCA 131

Access to information

- Centre d'acquisitions gouvernementales c. Teva Canada limitée, 2025 QCCQ 892
- Office of the Information and Privacy Commissioner for British Columbia v. Airbnb Ireland UC, 2024 BCCA 333

Jurisdiction of privacy authorities

- Société québécoise d'information juridique c. Commission d'accès à l'information, 2025 QCCQ 859

AI and privacy

- Svoboda v. Modiface Inc., 2024 ONSC 6249

Litigation Snapshot

Quebec Privacy Class Action Trends: Beyond Data Breaches

- **Shift in claims: Increasing** focus on allegedly intrusive practices (over-collection; collection/use without sufficient transparency or valid consent), with multiple recent Québec filings in this category:
  - **Mobile game developers (children's data):** Oct. 2025 proposed class action in Québec Superior Court on behalf of children under 14; alleges unlawful collection/sharing without parental consent against major publishers/gaming companies, citing insufficient controls, vague/deceptive policies, and violations of the Québec Charter, Private Sector Act, and Civil Code; seeks compensation and industry reform.
  - **Business-contact aggregators:** 2025 actions target data brokers and services commercializing online business contact information; Law 25's exclusion of business contact information from the definition of personal information introduces complex legal questions.
  - **AI training practices:** Emerging cases challenge collection and use of personal information to train/improve AI products.
- **Outlook:** Expect increased filings and scrutiny; organizations should assess consent, transparency, data minimization, and children's data controls, and map uses implicating business contacts and AI training.

Litigation Snapshot

Clearview AI Inc. v. Alberta IPC, May 2025 [note: appealed to Court of Appeal of Alberta]

- Context: the Alberta IPC had found that Clearview AI's facial recognition tool (which involved "scraping" images of faces from social media photos, storing the information on its databases, and creating numerical representations of each image) did not comply with PIPA Alberta.
    - Clearview applied for judicial review, arguing that this result was unreasonable.
- **Jurisdictional question:** Alberta Court of King's Bench confirmed that the IPC had jurisdiction over Clearview, a foreign organization, as it "chose to do business in Alberta and collects, uses, and discloses personal information of Albertans, some of which is hosted on websites with servers in Alberta."
- **Constitution question:** the Court found that the "publicly available" exception to consent in Alberta unjustifiably limited search engines' freedom of expression in the course of their "regular functions". It struck the offending language in the PIPA regulation:

> *7 … personal information does not come within the meaning of … "the information is publicly available" except in the following circumstances:*
>
> *(e) the personal information is contained in a publication, ~~including, but not limited to, a magazine, book or newspaper,~~ whether in printed or electronic form, but only if*
>
> *(i) the publication is available to the public, and*
>
> *(ii) it is reasonable to assume that the individual that the information is about provided that information.*

    - As such, personal information an individual publishes on social media sites, without the use of privacy settings, was found to constitute "publicly available information" for the purposes of the exception of consent.
    - However, lawful data processing under an exception to consent still requires reasonable purposes.
    - The Court upheld the Commissioner's decision that Clearview's purposes were not reasonable and therefore that its collection and use of personal information was unlawful.

Web Indexing: Lessons from Recent Decisions

August 2025: OPC recognizes a "right to be forgotten"?

- Complainant alleged that Google contravened PIPEDA (obligations re: accuracy and reasonable purposes) by displaying certain media articles when their name is searched.
    - Context: articles (from many years prior) concerned the Complainant's arrest and charge resulting from an allegation that they did not disclose their HIV status to a person with whom they engaged in sexual activity. Criminal proceedings were stayed in accordance with updated Attorney General policy – i.e. that no charges should be laid where there is no realistic possibility of HIV transmission.
- The OPC concluded that Google complied with accuracy obligations under PIPEDA, i.e. its obligations to ensure that:
    - The personal information in search results accurately reflects the content of linked articles; and
    - Those articles actually contain the searched name
- However, the OPC found Google in contravention of subsection 5(3) of PIPEDA.
    - In limited circumstances, a reasonable person would consider it inappropriate for a search engine to return results containing personal information about an individual in response to a search for their name:
        - The results reveal extremely sensitive personal information (in this case: sexual orientation, sexual activities, HIV status, criminal charge) causing significant harm; and
        - There is little to no public interest in the articles being returned in response to a name search (in this case: complainant not a public figure, stayed criminal charge, articles not updated to reflect stay).
- The OPC recommended that Google de-list articles from results displayed in a search for the complainant's name.
- Google declined, holding that whether PIPEDA includes a right to de-listing is a matter for the courts to decide.

Web Indexing: Lessons from Recent Decisions

September 2025: Certification overturned for proposed RateMDs Class Action

- BC court had certified a class action from health professionals whose name and contact information had been posted on RateMDs.com
  - Cause of action requirement: assuming the facts pleaded are true, is it plain and obvious that the plaintiff's claim cannot succeed?
  - Chambers judge found that the proceeding disclosed a cause of action, i.e. two actionable breaches of the *BC Privacy Act*:
    - Statutory tort of violation of privacy, and
    - Unauthorized use of individuals' names for advertising/promoting commercial service ("misappropriation of personality tort")
- BC Court of Appeal overturned certification on the cause of action requirement:
  - Violation of privacy:
    - Court found that the mere act of posting (and hosting) reviews on RateMDs does not violate the privacy of health professionals in the class.
      - No facts pleaded established a reasonable expectation of privacy → therefore, no right to control the use of the information
    - Does not preclude a claim arising from the content of particular reviews.
  - Misappropriation of personality:
    - Plain and obvious on the facts pleaded that the health professionals are not being commercially exploited for the purpose of increasing RateMDs' "sales".

Thank you for attending!

Contact Us:

(416) 646-3660

info@accessprivacy.com