Year 2025 in review and trends for 2026: Major developments in cybersecurity and personal information protection

January 28, 2026

Like every year for International Data Protection Day, BLG presents a strategic overview of the most significant developments of 2025 in cybersecurity and personal information protection in Canada.

We have compiled the year's most noteworthy Insights to provide a strategic summary of legislative evolution, emerging trends, and best practices. This publication also highlights the strategic priorities and key issues that organizations should keep in mind for 2026. See also our previous Year 2024 in review.

Developments relating specifically to artificial intelligence, given their rapid evolution, will be covered in a separate publication. Stay tuned!

Retrospective of 2025

Legislative reforms

Bill C-8: new requirements for operators of critical systems

On June 18, 2025, the federal government tabled Bill C-8, the Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, effectively relaunching federal cybersecurity reform amid a sustained rise in cyber incidents.

Bill C-8 imposes stringent compliance obligations on designated operators of federally regulated critical cyber systems, including in the banking, telecommunications, energy, and transportation sectors. Key obligations

include implementing cybersecurity programs, reporting incidents within 72 hours, reporting material changes affecting systems or third-party providers, and complying with binding government directives. Sector regulators are granted broad inspection and enforcement powers, including administrative monetary penalties of up to $15 million per day, per violation, and potential personal liability for directors and officers.

Although many already possess the necessary sophistication, organizations subject to the Act must act proactively by mapping critical systems, determining their regulatory status, and strengthening governance and incident-response capabilities—particularly regarding third-party risk. The Bill positions cybersecurity as a core operational-resilience and risk-management issues, not merely a compliance exercise.

For more information: Bill C-8 revives Canadian cyber security reform: What critical infrastructure sectors need to know and *Critical Cyber Systems Protection Act* is back – seven points for designated operators

Alberta reform: new privacy laws for public bodies and private sector organizations

Two new Alberta statutes, the *Access to Information Act* (AIA) and the *Protection of Privacy Act* (PPA), came into force on June 11, 2025. Adopted as part of a reform adopted in December 2024, these laws replace the *Freedom of Information and Protection of Privacy Act* and introduce significant changes to the obligations regarding access to information and the protection of personal information.

The new AIA tightens access rights by introducing more restrictive definitions, new exclusions and exemptions, and mechanisms that facilitate the dismissal of certain requests, all within a context of increasing pressure associated with processing large volumes of emails and electronic records.

The PPA modernizes Alberta's personal information protection regime by requiring breach notification and reporting based on the "real risk of significant harm" (RROSH) standard, thereby aligning Alberta with Canadian norms. The Act also introduces innovative provisions on de-identification, the creation of non-personal information, and decisions based on automated processing.

The regime includes penalties of up to $200,000 for an individual and $1 million for an organization, placing the province among the strictest jurisdictions in the country.

For more information: Alberta overhauls its public sector access and privacy regime

Nova Scotia reform: modernized requirements for public bodies

On Sept. 26, 2025, Nova Scotia introduced Bill 150, *An Act Respecting the Right of Access to Records of Public Bodies and the Right of Privacy with Respect to Personal Information Held by Public Bodies*, a reform that consolidates and modernizes the legal framework applicable to the public sector in matters of access to information and the protection of privacy. The statute, which will come into force on April 1, 2027, will replace both the *Freedom of Information and Protection of Privacy Act* and the *Personal Information International Disclosure Protection Act*.

The bill introduces, among other things, a new exemption that excludes from disclosure any information that could reveal security measures protecting electronic systems. It also imposes structural requirements, including the obligation to conduct a Privacy Impact Assessment (PIA) before any project or activity involving personal information, as well as a notification regime triggered when significant harm is reasonably anticipated. Finally, it sets out rules governing the hosting, access, and transfer of personal information outside Canada, and grants the Nova Scotia Supreme Court the authority to issue orders in cases of unauthorized collection, theft, or disclosure.

For more information: Notes on Nova Scotia's FOIPOP Reform Bill

Joint investigation of 23andMethe importance of preventive measures and confidentiality incident management

As part of a joint investigation conducted with its U.K. counterpart, the Office of the Privacy Commissioner of Canada (OPC) examined the breach that affected 23andMe in 2023. The incident, attributed to a credential stuffing attack, compromised nearly seven million genetic profiles worldwide, thereby exposing the sensitive information of thousands of Canadians.

The commissioners concluded that 23andMe had not implemented security measures proportionate to the sensitivity of the information, notably due to the absence of multi-factor authentication and robust password-management mechanisms. The investigation also revealed significant deficiencies in detection, response, and notification: the company failed to act upon credible early warning signs of the attack and did not promptly inform authorities or affected individuals.

While the U.K. regulator imposed a £2.31 million fine, no penalty was issued in Canada due to limitations in the current federal framework, which highlights the need for modernization. The incident nevertheless resulted in class actions, with a proposed Canadian settlement of approximately US$3.25 million (nearly C$4.5 million), subject to court approval in the context of the company's insolvency proceedings.

The investigation's findings underscore the importance for organizations to implement adequate measures not only to safeguard personal information,

but also to detect and respond swiftly to a privacy incident—particularly when sensitive data is involved. Increased vigilance is essential.

Hospital for Sick Children v. Ontario: clarification of the scope of notification requirements in Ontario

The decision *Hospital for Sick Children v. Ontario*, issued by the Ontario Divisional Court on Sept. 16, 2025, confirms that a ransomware attack triggers a notification obligation even in the absence of evidence of access, exfiltration, or theft of personal information.

The Court endorsed the position of the Information and Privacy Commissioner of Ontario, holding that encryption rendering information temporarily inaccessible constitutes an unauthorized "use" and "loss," sufficient to trigger the obligation to notify affected individuals under the *Personal Health Information Protection Act, 2004* and the *Child, Youth and Family Services Act, 2017*. The decision clarifies that these notification regimes are not based on a risk threshold, but instead pursue objectives of transparency, organizational accountability, and effective regulatory oversight following an incident.

For organizations, this decision means that incident response plans must treat encryption-only incidents without exfiltration as full privacy incidents. They must include notification mechanisms that comply with applicable requirements and incorporate an analysis reflecting the coexistence of different thresholds under the relevant provincial regimes.

For more information: No need for access, theft or disclosure: encryption of data is notifiable under PHIPA and CYFSA Biometrics

Clearview AI v. Alberta (Information and Privacy Commissioner): potential legitimization of public data scraping for artificial intelligence training

In *Clearview AI Inc v. Alberta (Information and Privacy Commissioner)*, the Alberta Court of King's Bench issued an important decision in May 2025 as part of Clearview AI's challenge to an order resulting from the 2021 joint investigation conducted by several Canadian privacy authorities. Clearview's project relied on the scraping of billions of publicly accessible facial images posted online to create a biometric database and offer a facial-recognition service.

Here are some key takeaways:

- The decision clarifies the interpretation of the exception allowing the collection of personal information without consent when such information is "publicly available", a central issue for model training.

- The Court upheld the Commissioner's restrictive interpretation, finding that information taken from websites or social media platforms is not automatically captured by this exception.
- However, the Court recognized that an excessively narrow interpretation raises constitutional concerns, particularly regarding freedom of expression. Indeed, this interpretation unduly hinders certain legitimate uses of publicly disclosed information (such as content indexing).
- The Court opted for a modernized reading focused on information "intentionally made public" and ordered the removal of the restriction that limited the exception to certain traditional media (magazines, books, and newspapers).

In practice, although the decision may support the use of online data for training artificial intelligence models, organizations should exercise caution if they decide to rely on the "publicly available" information exception before it is officially reviewed by the legislature. That said, Clearview AI has challenged the findings of the investigation and filed a notice of appeal. It will therefore be interesting to closely follow the developments in this case and see how Clearview AI will once again contribute to the evolution of Canadian privacy law.

For more information: Alberta judgment opens the door to the legitimization of data scraping and AI model training and The extraterritorial reach of B.C.'s privacy laws: Court upholds privacy commissioner's order against foreign AI company.

Commission d'accès à l'information order against Metro Inc. : what does the future hold for biometric system deployment in Québec?

On Feb. 18, 2025, the Commission d'accès à l'information (CAI) issued a landmark order prohibiting Metro from deploying a facial recognition system designed to identify individuals involved in shoplifting. This represents the first formal prohibition on putting a biometric database into operation under Québec's Act to establish a legal framework for information technology, confirming the CAI's particularly restrictive stance toward biometric technologies in the post Law 25 environment.

As part of its project, Metro was planning to deploy a facial recognition system to identify any individuals who have been involved in shoplifting or fraud in its establishments. Metro would use its existing video surveillance system to capture facial images of suspected offenders at the entrances and exits of participating stores. These images would then be compared to a biometric database containing data on individuals who had previously been involved in similar offenses and had been the subject of police intervention to generate a new biometric template. If a match was found, designated store personnel would receive an alert to take appropriate action in accordance with internal procedures.

Substantively, the CAI adopts a broad and liberal interpretation of the notion of identification, treating the project as a form of "identity verification" even in the absence of nominative identification. It considers that a system may fall under the biometric regime whenever it allows a person to be distinguished and associated with a pre-existing database. The CAI also rejects the argument that facial recognition could be justified as a secondary use of footage already captured through video surveillance; it distinguishes between video recording and the extraction of biometric measurements, the latter constituting a standalone collection requiring express consent.

In all, the CAI concluded that Metro's system constituted identity verification within the meaning of the Act, that the biometric characteristics it used were inseparable from individuals' identities, and that the lack of express consent justified prohibiting its implementation.

The consequences of the Metro order are significant for biometric project governance; organizations doing business in Quebec must exercise great caution when developing tools, practices, or projects involving biometric data. That said, Metro has appealed the decision so that the CAI can assess the necessity and legitimate purposes of the project, two concepts on which the CAI remained silent in its order. Stay tuned.

New guidance from the Office of the Privacy Commissioner of Canada: clarification of the definition and scope of biometrics

On Aug. 11, 2025, the Office of the Privacy Commissioner of Canada (OPC) released Guidance for processing biometrics for businesses (the Guidance), following the public consultation on the Draft Guidance for processing biometrics for organizations in 2023.

Intended for private sector organizations that deploy biometric initiatives, the Guidance sets out the main privacy protection considerations under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). It also highlights best practices for the governance and management of biometric information.

The Guidance addresses key considerations for organizations when planning and implementing initiatives involving biometric technology. It emphasizes the importance of ensuring that there is an appropriate purpose for collecting, using, and disclosing biometric information, and of carefully assessing the risks involved, including the proportionality of potential privacy impacts. The Guidance also clarifies what biometric information is (which is a big development as it is not defined in PIPEDA), as well as consent requirements for biometric initiatives, as well as considerations around transparency, safeguarding data, and accuracy, including testing for biometric systems.

The OPC's updated Guidance generally aligns with Québec's Commission d'accès à l'information (CAI)'s guide on biometrics (available in French only),

and follows recent decisions from the CAI considering organizations' processing of biometric information for the purposes of loss prevention and access control to business premises. Note that while the OPC's Guidance is advisory, Québec has established more prescriptive requirements. Organizations must therefore ensure that their practices are consistent with the provincial and federal requirements for the processing of biometric information.

To this end, and to mitigate legal risks associated with biometric-information processing, organizations should consider establishing internal guidelines governing the use of biometric systems. These guidelines should reflect the obligations set out in the Guidance as well as other applicable principles related to the protection of biometric data. Organizations should also consider reviewing their consent forms and privacy impact assessments (PIAs) to reflect these new guidelines and ensure that they comply with all applicable requirements.

For more information: Privacy Commissioner of Canada's new guidance on biometrics: What does it mean for your business?

Joint investigation by Canadian commissioners into TikTok: increased protection of children's personal information

The joint investigation conducted by the federal, Québec, British Columbia and Alberta privacy commissioners concluded that TikTok was not complying with Canadian privacy laws regarding the personal information of children.

Despite the platform's formal prohibition on users under 13 (14 in Québec), TikTok was collecting and using children's personal information on a large scale for content personalization and targeted advertising. Its only age verification mechanism at registration, self declared date of birth, was easily bypassed, and subsequent detection mechanisms proved ineffective, allowing the profiling of children and the delivery of targeted ads before their accounts were eventually removed.

The commissioners found that TikTok pursued no legitimate purpose that could justify the collection or use of children's personal information, which is deemed sensitive by default. They also concluded that the consents obtained were neither valid nor sufficient: essential information relating to tracking, profiling, deployed technologies and the potential use of sensitive information was not provided in a clear, accessible or age appropriate manner. The privacy policies were difficult to access, incomplete, available only in English and did not adequately explain the use of biometric information.

In Québec, the CAI identified a heightened lack of transparency: TikTok automatically activated identification, geolocation and profiling technologies without prior notice and did not offer the most protective settings by default as required by law. The authorities also adopted a broad interpretation of

“biometric information,” finding that even non identifying data used for age estimation triggers the applicable legal obligations.

Given the heightened emphasis on protecting children’s personal information, which is considered sensitive by default, organizations must exercise considerable caution in assessing the purposes for which such information is collected and in tailoring explanations to the intended audience. It is worth noting, however, that despite the seriousness of the findings, the CAI did not impose administrative monetary penalties, leaving open the question of the severity threshold required for such sanctions. The matter nevertheless resulted in the filing of a proposed class action before the Québec Superior Court seeking compensatory and punitive damages.

RateMDs v. Bleuler: no reasonable expectation of privacy for public information about health professionals

In *RateMDs Inc. v. Bleuler*, the British Columbia Court of Appeal overturned the certification of a class action against RateMDs, a website that displays profiles of health professionals created without their consent along with client reviews, on the basis that the claim did not have a viable cause of action.

Under the *Personal Information Protection Act* (PIPA), the Court held that the right to privacy applies only to information for which there is a reasonable expectation of privacy, which excludes publicly available information relating to the provision of health services. The creation of profiles without consent therefore did not constitute a privacy violation against the physicians. The Court also rejected the argument that the reviews amounted to an unauthorized commercial use of the professionals’ names. Despite RateMDs generating profit from the platform, the Court concluded that health professionals could not reasonably expect information about their services to remain private, nor could they control the websites that might publish such information. Public notices about professionals’ services are common and do not, in themselves, constitute a violation of privacy. The Court also concluded that RateMDs did not commercially exploit the names of professionals, who were simply the subject of comments.

The decision highlights that privacy claims require more than a simple lack of consent: there must be a reasonable expectation of privacy. As a result, businesses that publish profiles or reviews should carefully assess the purpose of their commercial activities to ensure that they are not using personal information for commercial purposes without consent.

For more information: Novel privacy claims and the limits of class action certification: *RateMDs Inc. v. Bleuler*, 2025 BCCA 329

New guidelines on de-identification

The Information and Privacy Commissioner of Ontario (IPC) has released updated guidelines on the de-identification of personal information, which revise and clarify the initial guidance published in 2016.

These guidelines strengthen the operational approach to de-identification by adding upstream planning steps, including determining whether the de-identification process should be conducted internally or outsourced to a third party, assembling a competent team, and assessing whether a Privacy Impact Assessment (PIA) is required. They also recommend adopting a transparent approach, which includes informing affected individuals and communicating the general objectives pursued. This direction aligns with PHIPA Decision 175, which requires certain custodians to publicly outline their current de-identification practices.

The IPC further emphasizes that the disclosure of de-identified data does not eliminate governance obligations. Organizations must implement ongoing controls, including monitoring the risks of re-identification and verifying compliance with data-sharing agreements, whether the disclosure occurs in a private or public context. The IPC also notes that data publicly released is, by nature, more difficult to remove or correct once disclosed.

In practice, organizations should establish a formal de-identification framework that clearly defines roles, responsibilities, and decision-making authority, as well as contractual requirements for data-sharing arrangements, risk assessment mechanisms, and transparency commitments required under applicable laws and guidelines.

For more information: De-identification of personal information and the new IPC Ontario guidelines

First imposition of administrative monetary penalties

In its Decision 298, the Information and Privacy Commissioner of Ontario (IPC) imposed administrative monetary penalties (AMPs) for the first time since this enforcement power came into effect in January 2024.

Relying on the *Personal Health Information Protection Act*, 2004 and its own guidance framework on AMPs, the IPC emphasized that such measures are intended primarily to (i) promote compliance and (ii) prevent a custodian from obtaining an economic benefit from a contravention. In this case, the IPC found that a professional had used their access to a medical records registry to identify and contact potential patients in order to offer them services—an unauthorized use serious enough to justify the imposition of AMPs.

By comparison, in Québec, the CAI has not yet exercised its authority to impose AMPs since the amendments introduced by Law 25 came into force. This should not, however, be interpreted as leniency; the case perfectly illustrates the rationale behind the creation of AMPs: encouraging compliance and preventing individuals or organizations from deriving direct or indirect economic benefits from violating the law. Businesses should therefore ensure

they adopt appropriate privacy-protection measures, particularly given the growing number of investigations and class actions, as well as the evolving landscape of cybersecurity threats.

For more information: PHIPA Decision 298: First imposition of administrative monetary penalties

PIPEDA reform?

The 2025 federal budget signalled the government's intention to amend the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and to introduce related legislation establishing a tribunal responsible for administering a sanctions-based enforcement regime. The previous bill proposed by the federal government for this purpose, Bill C-27, died on the order paper in January 2025.

Much like Québec's reform, the forthcoming federal bill is expected to include potentially significant penalties, as well as measures relating to data sovereignty and data mobility—particularly to support and implement Canada's open banking framework. It is also expected to address the protection of children's personal information and emerging technologies.

In anticipation of a potential PIPEDA reform, organizations would be well-advised to begin preparing now for stricter requirements, drawing on certain provisions from Bill C-27 and the Québec model.

Regulatory future of biometrics

In Québec, the Metro decision (available in French only) marks a significant turning point in the CAI's interpretation of the concept of "identity verification." By adopting an expanded conception of this notion, the CAI broadens the scope of Québec's biometric regime to include uses that were previously viewed as non identifying. As a result, a greater number of projects now fall under Québec's enhanced biometric obligations, positioning the province as the most stringent jurisdiction in Canada in this area.

At the federal level, regulatory developments likewise show a widening of the notion of biometrics, as illustrated by the OPC investigation in the TikTok matter. However, the OPC's recent guidance adopts a more nuanced approach regarding organizational obligations by recognizing, in certain circumstances, the possibility of using biometrics without express consent, notably when such use is imposed as a condition of service and is supported by reasonable justifications. Grounded primarily in non binding guidance, the federal framework therefore remains more flexible and pragmatic than that of Québec.

In a context of rapidly growing adoption of biometric technologies, organizations nonetheless remain obligated to conduct rigorous preliminary assessments of their projects and to closely monitor upcoming developments in 2026.

Data governance and data sovereignty

In 2025, Canada intensified its efforts to strengthen digital sovereignty in order to better protect data, support digital transformation, and enhance the security and resilience of critical infrastructure.

In its Digital Sovereignty Framework, the federal government examines the legal, security, privacy, workforce, and supply-chain factors that influence the government's ability to maintain digital sovereignty. It highlights challenges associated with jurisdictional complexity, dependence on global service providers, evolving cybersecurity risks, and internal capacity constraints, while emphasizing the need for interoperability across government and with international partners.

In parallel, the Canadian Sovereign AI Compute Strategy, announced in the 2025 federal budget, includes major investments in sovereign AI infrastructure to ensure that the data and computing power required for AI remain under Canadian control.

Together, these initiatives reflect Canada's intent to combine technological autonomy with economic competitiveness, placing data governance and digital sovereignty at the core of its national strategy. As a result, Canadian organizations can expect these initiatives to translate into legislative measures, regulations, or other policy instruments.

Increase in class actions in Québec

In Québec, 2025 was marked by a rise in privacy-related class actions. The Superior Court authorized three proposed class actions alleging the access, collection, use, and disclosure of personal information without consent, as well as failures relating to data confidentiality and security (see: *Déziel c. Santé Québec*, *Synotte c. TiktTok Technology Canada Inc.* and *S.C. c. Gameloft and al.*, available in French only).

These three class actions lawsuits illustrate a shift in how litigants are using class proceedings in Québec to protect their privacy. Whereas such actions previously focused primarily on isolated confidentiality incidents, challenges are increasingly targeting organizations' overall governance practices relating to personal information management.

Given the significant increase in privacy-related class actions and confidentiality incidents, businesses should strengthen their preventive practices by enhancing their physical, organizational, and administrative safeguards. Doing so will help reduce the risk of incidents both internally and externally, and prevent potential investigations into their privacy and security policies.

Protection of children's privacy

The protection of children's privacy is increasingly emerging as both a regulatory and political priority. The Office of the Privacy Commissioner of Canada (OPC) has conducted a consultation aimed at improving the privacy and online safety of children. The purpose of this consultation is to develop a code for the protection of children online, setting out clear requirements for online platforms and services, including limits on data collection, transparency obligations, security measures, and the need to consider the best interests of the child when designing digital services.

This consultation follows the earlier consultation on privacy and age verification launched in 2024. That initiative sought to determine appropriate methods for age verification, understand the expectations of parents and young people, and identify best practices for informing and protecting minors online. The feedback gathered during the consultation has been compiled into a report, and the OPC will soon publish draft guidance based on these findings.

Although the federal government has not announced a timeline for adopting these measures, businesses offering digital services to minors should anticipate forthcoming legislative changes and review their practices to ensure transparency and the safety of children online. This is especially important given the growing legal risks and the significant increase in regulatory investigations and class actions.

By

Hélène Deschamps Marquis, Frédéric Wilson, Daniel J. Michaluk, Eric S. Charleston, Cléa Jullien

Expertise

Cybersecurity, Privacy & Data Protection, Artificial Intelligence (AI)

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.