Year 2024 in review and trends for 2025: Major developments in cybersecurity and personal information protection

January 28, 2025

To mark International Privacy Day, BLG presents a review of the past year's significant developments in cybersecurity and privacy law in Canada.

We have compiled our most significant Insights of 2024 to offer you a summary of recent developments, including legislative changes, emerging trends, and best practices. In addition, this publication provides an overview of the strategic priorities and issues that organizations should bear in mind as 2025 continues.

Retrospective of 2024

Artificial intelligence (AI)

Use of artificial intelligence (AI) by Québec public bodies

The year 2024 marked a key milestone in the global regulation of AI, notably with the European Union's AI Act coming into force, setting an international benchmark in the field.

Although Québec does not yet have an AI-specific legal framework, it is part of this global shift through initiatives aligned with international standards. Among these, the Ministère de la Cybersécurité et du Numérique (MCN) recently published an Énoncé de principes pour encadrer l'utilisation responsable de l'IA par les organismes publics (available in French only), which identifies ten fundamental principles for the responsible use of AI, including respect for individual rights, transparency, reliability, and sustainability. In parallel, the MCN has introduced a Guide des bonnes pratiques pour l'utilisation de l'IA

generative (available in French only), offering practical recommendations on privacy, neutrality, efficiency, diligence and awareness.

These are essential tools for Québec public bodies, providing a clear, operational framework for responsibly and securely integrating AI in line with legal and ethical expectations.

For more information: Responsible use of AI by Québec public bodies | BLG

AI best practices in the financial sector

The legal framework governing AI while fragmented is rapidly evolving, reflecting the diversity of sectors it impacts. Faced with increasingly precise regulatory expectations, the Autorité des marchés financiers (AMF) and the Ontario Securities Commission (OSC) have published guidelines to direct capital markets participants towards best practices to mitigate the operational and ethical risks associated with AI.

These guidelines address the validation and monitoring of AI systems to ensure their reliability, robust data governance to minimize bias and ensure data integrity, and the implementation of auditing and accountability processes. By advocating transparency in automated decision-making and adhering to ethical standards, financial organizations can strengthen stakeholder trust and align with regulators' growing governance and compliance requirements.

In addition, staff of the Canadian Securities Administrators published in December 2024 a Staff Notice and Consultation 11-348 *Applicability of Canadian Securities Laws and the use of Artificial Intelligence Systems in Capital Markets* to provide clarity and guidance on how securities legislation applies to the use of AI systems in capital markets.

For more information: AI best practices for Canadian asset managers | BLG

Law 5 and the protection of health information

Québec's *Act respecting health and social services information* (Law 5), which came into force on July 1, 2024, establishes a new legal framework for the management of health information in the province. It applies to healthcare organizations, including private clinics, and outlines rules for the processing of health and social service information, including information that identifies a person in relation to their state of health or the social services received.

Law 5 imposes strict governance obligations on healthcare organizations, requiring the adoption of detailed policies covering security measures, access controls, and the management of confidentiality incidents. It also introduces a default privacy obligation for deployed technology products and services, and requires a privacy impact assessment (PIA) prior to any technology project involving health information. Although it does not provide for administrative monetary penalties, Law 5 introduces penal sanctions of up to $150,000.

For more information: Law 5 and the protection of health data in Québec | BLG

Administrative monetary penalties under PHIPA

Effective Jan. 1, 2024, the Information and Privacy Commissioner of Ontario (IPC) has discretion to issue administrative monetary penalties (AMPs) for certain breaches of the *Personal Health Information Protection Act, 2004* (PHIPA) or its regulations.

AMPs are a new tool in the broader regulatory toolkit for encouraging compliance with PHIPA. AMPs can reach $50,000 for a natural person and $500,000 for organizations, and may be appropriate for severe PHIPA violations such as egregious snooping on patient records, contraventions for economic gain, or persistent disregard for an individual's right to access their personal health information. Importantly, where there is an economic gain, the IPC may issue an AMP above the regulatory ceiling, or even refer the case to the provincial Attorney General for prosecution.

These new measures underline the need for organizations to review their privacy policies and practices to limit legal and financial risks. To further promote compliance and encourage ethical privacy practices, the IPC has published guidance outlining how these sanctions are to be applied, emphasizing not only their punitive, but their educational role as well.

For more information: PHIPA administrative monetary penalties | BLG

Regulation respecting the anonymization of personal information

On May 30, 2024, Québec became the first jurisdiction in Canada to adopt a specific regulation on the anonymization of personal information.

The *Regulation respecting the anonymization of personal information* establishes a clear normative framework that provides businesses and public bodies with a procedure for anonymizing personal information. It aims to ensure that anonymized personal information, irreversibly, no longer allows the person to be identified directly or indirectly.

The Regulation requires that anonymization be carried out under the supervision of a person qualified in the field and imposes an obligation to conduct in-depth analyses of the re-identification risks throughout the process, notably by considering individualization, correlation and inference. Organizations must also establish anonymization techniques in line with recognized best practices, such as randomization and generalization. Finally, as of Jan. 1, 2025, organizations must maintain a register detailing anonymization processes, techniques used, and risk analyses.

For more information: Regulation on the anonymization of personal information | BLG

Law 25 introduces the right to data portability

The final part of Law 25, the "right to data portability," came into force in Québec on Sept. 22, 2024. The concluding chapter of extensive legislative reform, this right enables individuals to obtain and communicate their computerized personal information in a structured, commonly used technological format.

Inspired by the European Union's *General Data Protection Regulation*, the right to portability aims to strengthen citizens' control over their data. Organizations must be prepared to identify the information concerned, guarantee its secure transmission, and ensure compliance with technical criteria, such as the use of interoperable formats like CSV, XML or JSON.

The right to data portability is considered an extension of the right of access. Accordingly, organizations should handle data portability requests in accordance with the current regime applicable to access requests. The Québec government has published an explanatory table (available in French only) to illustrate the differences between the right of access to personal information and the right to data portability.

For more information: Law 25 introduces the right to data portability in Québec | BLG

Adoption of Bill 194 in Ontario

Bill 194, Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024 (Bill 194), adopted Nov. 25, 2024, sets a new standard in cyber security, privacy protection, and artificial intelligence governance for Ontario's public bodies.

Bill 194 aims to modernize the province's legislative framework by aligning its requirements with Canadian and international standards. It sets out concrete measures to strengthen the protection of personal information, including the contemplation of enhanced PIA and breach reporting obligations, while providing the IPC with expanded powers, enabling proactive oversight, and the implementation of mechanisms to better oversee the use of emerging technologies.

For more information: Bill 194 - The new Enhancing Digital Security and Trust Act, 2024 | BLG

Privacy sweep clarifies OPCs online consent expectations

On July 9, 2024, the Office of the Privacy Commissioner of Canada (OPC) published the *Sweep Report 2024: Deceptive Design Patterns* highlighting the results of an in-depth investigation into the use of deceptive design patterns, or "dark patterns" by various websites and apps to influence users' decisions about their personal information.

In addition, the OPC issued new guidance for individuals on navigating, and for organizations on avoiding deceptive design patterns. Together, the Report and Guidance shed light on the OPC's expectations when it comes to obtaining meaningful consent in an online environment.

While the Report and Guidance set out best practices rather than binding rules, they serve to highlight the OPC's priorities for potential future enforcement actions and provide concrete, illustrative examples of what the OPC finds acceptable. Organizations hoping to stay ahead of the curve should consider taking proactive steps to implement the OPC's recommendations for avoiding deceptive design patterns now, rather than wait for a formal complaint or investigation.

For more information: Privacy sweep clarifies OPCs online consent expectations | BLG

Facebook's privacy policy and meaningful consent

In its Sept. 9, 2024, decision, *Canada Privacy Commissioner v Facebook Inc.*, the Federal Court of Appeal ruled that Facebook had breached the consent and security requirements of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

As part of its ruling, the Federal Court of Appeal outlined the scope of these obligations. The Court ruled that Facebook's privacy policies, which were too long and complex, did not meet the transparency requirements necessary to obtain meaningful consent. Moreover, the decision raises the question of whether organizations must take reasonable steps to ascertain that third parties collecting personal information on their behalf respect their privacy commitments. In the case of Facebook, the failure to properly monitor third-party applications was considered a breach of the safeguarding requirement.

Overall, the Facebook decision underscores the importance of a proactive and transparent approach to the protection of personal information, which places the privacy rights of individuals at the heart of organizational practices.

On Nov. 8, 2024, Facebook applied for leave to appeal to the Supreme Court of Canada on the ground that the proposed appeal raises two questions of public importance concerning PIPEDA, specifically on the length of the privacy policy and meaningful consent, and the duty to police compliance by third parties to maintain reasonable security safeguards. A decision on the application for leave to appeal can be expected in May 2025.

For more information: Facebook's privacy policy and breach of meaningful consent | BLG

LifeLabs LP v. Information and Privacy Commissioner (Ontario)

As cybersecurity breaches multiply, organizations are faced with crucial questions about how to manage their internal investigations.

The case of *LifeLabs v. Information and Privacy Commissioner (Ontario)* highlights the limits of litigation privilege following a cybersecurity breach. The Court confirmed that litigation and solicitor-client privilege do not extend to underlying facts that would otherwise be disclosed pursuant to a statutory duty, even if they are embedded in privileged documents. For example, the investigative report prepared by an external cybersecurity firm for LifeLabs, although initiated by the company's lawyers, was not deemed privileged as it had been produced primarily for commercial purposes and not for imminent litigation. Similarly, sensitive communications, including ransom negotiations between LifeLabs and the suspected cybercriminal, did not qualify for legal protection.

In short, this decision is a reminder that underlying facts are not privileged information when they exist independently. In addition, this case underlines the importance for organizations of properly engaging external counsel under a legal retainer and clearly documenting the objectives of their cybersecurity investigations to effectively protect their legal privilege while meeting regulatory obligations.

For more information: LifeLabs LP v. Information and Privacy Commr. (Ontario), 2024 ONSC 2194 | BLG

New Regulation respecting the management and reporting of information security incidents by certain financial institutions

Québec's new *Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents*, which comes into force on April 23, 2025, imposes strict requirements on financial institutions and credit assessment agents to ensure proactive and effective management of information security incidents.

The Regulation imposes a duty on organizations to develop a comprehensive incident management policy, to appoint a manager to oversee its implementation, to report any incident to the AMF within 24 hours of notification to management, and to keep a detailed register of incidents for five years. Monetary administrative penalties for non-compliance include fines of up to $500 for individuals and $2,500 for legal entities.

The Regulation aims to ensure sound incident management and reporting practices, enabling targeted organizations to better anticipate and manage incidents, thus minimizing the potential impact on their reputation, solvency and customer confidence.

For more information, stay tuned: BLG plans to publish its analysis of the Regulation about a month prior to its coming into force.

AI framework and Bill C-27

On Jan. 6, 2025, Parliament was prorogued until March 24, 2025, with a proclamation of the Governor General on the advice of the Prime Minister, putting an end to the parliamentary session. There were three bills on the Order Paper that were expected to significantly transform the digital regulatory environment in Canada upon their passage, but were instead terminated with the announcement of prorogation: Bill C-27, Bill C-26 and Bill C-63.

Bill C-27 would have replaced the nearly 25-year-old PIPEDA with the Consumer Privacy Protection Act (CPPA), and enacted the *Artificial Intelligence and Data Act* (AIDA), which would have introduced a framework for regulating AI systems used in the course of commercial activities in Canada.

Following prorogation, it is unlikely that Bill C-27 would be resurrected as is (given the controversy surrounding AIDA), even though there is a broad consensus that federal private-sector privacy reform is needed.

AI legislation in Québec?

On Feb. 5, 2024, the Conseil de l'innovation du Québec issued a report entitled Prêt pour l'IA: Répondre au défi du développement et du déploiement responsables de l'IA au Québec (available in French only). The report calls on Québec to adopt legislation to regulate AI development and implementation, drawing on the principles established in the Montréal Declaration.

The report recommends basing Québec's legislation on the severity of risks associated with AI systems, in keeping with the approach selected by the Canadian federal government and the European Union. It further urges that this legislation set standards for the use of AI systems in the private and public sectors, and create an independent oversight body, which would also be tasked with recommending and drawing up related implementing regulations.

For more information: Ready for AI: The Conseil de l'innovation du Québec is calling for the adoption of AI legislation | BLG

Guidance on biometrics

The CAI and the OPC both published guidelines on biometrics in 2023: the CAI's Guidance surrounding biometric time clocks (available in French only)

and the OPC's "Draft Guidance for processing biometrics – for organizations - Office of the Privacy Commissioner of Canada" (open for consultation until Feb. 16, 2024). The regulators recommended that organizations should not collect biometric data for convenience and stressed that such sensitive information should only be collected where there is an urgent, genuine, important, or legitimate need to do so.

On a related note, the CAI recently rendered a decision concerning the necessity requirement when using a facial recognition system. This decision underlines, once again, the CAI's very high expectations when it comes to implementing a biometric system in the workplace.

News from the CAI

The National Assembly of Québec has appointed Me Lise Girard as President of the CAI. Her appointment was effective Nov. 8, 2024. Prior to her appointment, Me Girard was Assistant Deputy Minister at the MCN, as well as Chief Security Officer.

On another note, after a year in which the CAI has devoted itself to publishing guidelines on Law 25, we can now expect Québec's regulator to be more proactive in enforcing the law and applying its AMPs power.

Privacy class actions

On July 4, 2024, the B.C. Court of Appeal issued a duo of class action appeal decisions considering the potential scope of statutory and common law privacy claims against data custodians that fall victim to cyberattacks in data breach cases.

In both *G.D. v. South Coast British Columbia Transportation Authority* (G.D.) and *Campbell v. Capital One Financial Corporation* (Campbell), the B.C. Court of Appeal affirmed that victims of data breaches may have numerous causes of action (including the statutory tort of violation of privacy pursuant to the B.C. *Privacy Act*) against data custodians, even data custodians that have not committed any intentional wrongdoing. The unsuccessful parties in G.D. sought leave to appeal to the Supreme Court of Canada and a decision regarding leave is still pending.

In addition, the B.C. Supreme Court allowed an application for certification relating to Home Depot's alleged breaches of provincial privacy statutes when collecting and sharing customers' personal information after emailing purchase receipts but struck claims for breach of other contractual duties and obligations.

Report of the OPC 's investigation into OpenAI

In 2023, the OPC and the provincial privacy authorities of British Columbia, Alberta and Québec launched an investigation into OpenAI in response to a

complaint alleging the collection, use and disclosure of personal information without consent. The OPC has yet to provide details of the investigation's findings, but it is likely that it will be made public in 2025.

By

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

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 725 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