Data governance and privacy risks in Canada: A checklist for boards and c-suite

November 02, 2022

By Éloïse Gratton, Ad.E., LL.D., ICD.D, Board Member, Partner and National Co-leader, *Privacy and Data Protection, BLG*

Privacy compliance and cyber risks are hot issues for the c-suite and board of directors, and for good reason. Under Canadian law, corporate directors are responsible for their corporation's business, including risk identification and management activities, and are required to demonstrate a duty of care. And regulators aren't the only ones watching. Cybersecurity was the second-highest environmental, social and governance (ESG) concern cited by institutional investors and consultants in a 2021 RBC report, and proxy advisors routinely rate companies on their cyber and privacy practices under the governance category of ESG scoring.

If you are a senior leader, what are the new data privacy risks that should be on your radar? And how should you exercise your duty of care when it comes to these risks so you keep both regulators and investors happy? This article shares four privacy risks every director and officer should be aware of, then offers an 11-point checklist with key recommendations for data governance and privacy, with a special focus on Canada.

Privacy risks for Canadian organizations

Evolving legislation. In the U.S., the Security and Exchange Commission recently proposed new rules for publicly traded companies that would significantly increase the reporting requirements following cybersecurity breaches and the duty of directors and officers to mitigate such risks. In both Canada and the U.S., data protection laws are becoming more stringent as both jurisdictions slowly catch up to Europe's GDPR, which was adopted in 2018 and is considered the global gold standard when it comes to protecting privacy. In Canada, Québec was the first jurisdiction to adopt a data protection law approximately 30 years ago and the first jurisdiction to update its law to align with the new EU privacy framework earlier this year, with other Canadian jurisdictions recently following the lead.

A new type of privacy class action. More than 150 privacy class actions have been filed in Canada in recent years, mostly in Ontario, Québec and B.C. Approximately 70 per

cent are filed following a data security breach. The rest are for "privacy intrusive practices," which are invasions of privacy resulting from:

- A lack of transparency with consumers when collecting or processing their personal information.
- Failing to obtain proper consent.
- Unacceptable practices involving the collection of personal information, including over-collection.
- The use of new technologies involving surveillance or monitoring.

Most privacy class actions alleging intrusive business practices initially targeted tech giants and companies that monetize personal information. Recently, a broad range of companies operating in the retail, telecom, real estate and financial services industries have also been targeted by such lawsuits.

Penalties. New privacy requirements are introducing administrative monetary penalties for non-compliance. Québec was the first in Canada to do this, introducing a new private right of action and administrative monetary regime with potential penalties of up to $10 million or 2 per cent of revenue for non-compliance with the law and penal offenses for certain infractions of up to $25 million or 4 per cent of revenue. In 2022, the Minister of Innovation, Science and Industry introduced Bill C-27, *An Act to enact the Consumer Privacy Protection Act* and the *Artificial Intelligence and Data Act*. Both create significant compliance risks for businesses, including penalties of up to $10 million or 3 per cent of revenue. The most egregious violations receive a fine of up to $25 million or 5 per cent of revenue.

Shareholders' lawsuits: In the U.S., we're seeing more shareholder derivative lawsuits being filed against corporate boards following data breaches. Some of these lawsuits have been dismissed, with Marriott and Capital One being examples. Plaintiffs' lawyers are increasingly filing these claims based on allegations of breach of the duty of oversight. For example, a shareholder derivative suit filed against the board of T-Mobile USA in November 2021 refers to the board's alleged "failure to monitor" and "heed red flags." In 2022, a plaintiff shareholder filed a securities suit against Okta related to the decline in the company's share price following a data breach, finding fault with Okta's actions before and after the breach. While we have not yet seen this trend in Canada, shareholder lawsuits are an emerging risk to watch.

Checklist for data governance and privacy: 11 key recommendations

C-suite and the board need to assume an active role with direct oversight of the privacy and cyber risks affecting their corporation. The following is a checklist of key recommendations to guide actions in a rapidly changing regulatory landscape.

1. Purpose: We understand why we collect and retain personal information.

Under Canadian data protection laws, it is illegal to collect, share or retain personal information not related to business operations. For instance, following the Desjardins 2019 data breach, the Privacy Commissioner of Canada raised its concern that the company had retained old data that was no longer needed.

Canadian data protection laws are consent based. There is a legal distinction between requesting consent from individuals for personal information which is necessary for business operations versus optional uses. Consent for collecting and using personal information for nice-to-have purposes, such as marketing, surveys and, in some cases, analytics, must be optional. Senior leaders must understand why the organization collects personal information so they can ensure the privacy notices provided to customers, investors, applicants, employees, website visitors and others comply with transparency and consent obligations.

2. Strategy: We understand the organization's data privacy strategy and are part of regular conversations about its effectiveness.

Personal information has tremendous value. It can improve customer attraction, customer experience, brand positioning, trust, loyalty, and relationships with stakeholders – all of which offer a competitive advantage. Business analytics and the use of AI to gain insights from this information accelerate innovation. The board must understand the business strategy that underlies the use of personal information so it can have frequent and informed conversations about whether this strategy is effective as the business evolves.

3. Visibility: We know the type of personal information we have and where it is located.

To manage and mitigate compliance risks, the board should ensure that management is aware of these aspects of the personal information it holds:

- type
- sources
- format
- how it is used
- structure and classification according to sensitivity
- whether it is subject to access, deletion, disclosure or other individual rights and requests
- location

Organizations often conduct a data mapping exercise, where they query all relevant business units to better understand the life cycle of personal information from the time it is collected until it is destroyed. This way, a business can better assess its risks and determine the appropriate security measures to comply with relevant legal requirements in the jurisdictions it does business.

4. Program development: We have an appropriate privacy program in place and are prepared for regulatory changes.

The company needs a strong privacy program with the proper policies, procedures, processes and controls in place to mitigate key risks related to personal information management. The board should meet frequently with whoever is legally responsible for the protection of personal information in the company (this may be the CEO, as in Québec, or the privacy officer) to discuss how the privacy program is implemented, monitored and enforced, especially if the company is expanding its data collection and processing.

The privacy program should include quarterly general cyber security training for all employees and targeted training for employees who handle sensitive information or are responsible for contracts with service providers or projects requiring a privacy impact assessment.

It is the board's responsibility to ensure there is a solid governance structure, supported by senior management, to oversee the privacy program, and that the company is on schedule to meet all new legal requirements.

5. Barriers: We have identified our privacy compliance stress points and have sufficient resources for the implementation of our privacy program.

Management should also know the stress points, including time, resources and legal complexity, that may affect the organization's compliance. Using this information, management should assess the severity of compliance risks and determine which best practices should be implemented to improve the privacy program. It should also assess the adequacy of financial and human resources and determine who is accountable for which results.

6. Readiness: We are prepared to provide evidence of compliance to privacy regulators when requested.

All privacy-related policies, procedures, processes and controls should be properly documented and easy to access if requested by privacy regulators. Some Canadian jurisdictions will soon require companies to publish this information on their website. Businesses may also be legally required to maintain a register of all security incidents for a defined period following the breach, with the length of time depending on the Canadian jurisdiction(s) in which the business operates. This register must be provided to privacy regulators upon request to demonstrate compliance.

When Canadian privacy regulators receive a complaint about a business practice, their first question to the business is often, "Can I see a copy of your privacy impact assessment?" A privacy impact assessment (PIA) provides a roadmap for identifying privacy risks and the controls required to mitigate them, and can help demonstrate to privacy regulators that the company has done its homework. A PIA will become mandatory as of September 2023 in Québec for any project to acquire, develop or overhaul an information system or electronic service delivery system involving the processing of personal information, as well as for any cross-border transfer of personal information.

7. Outsourcing: Our approach to outsourcing complies with privacy legislation and adequately mitigates risks.

If outsourcing involves personal information, the board should assess whether the outsourcing policy adequately protects shared information. Typically, this entails conducting a security audit or using a vendor security risk assessment questionnaire as part of due diligence before retaining the service provider.

There are also privacy-related provisions that should be in the contract. These include, at a minimum:

- Compliance with Canada's data protection laws.
- A prohibition to use or disclose the personal information for purposes other than providing the services.
- A prohibition to share the information with third parties or transfer the information to certain foreign jurisdictions.
- A framework for the management of requests from third parties, including government disclosure requests.
- The secure disposal or destruction of the information at the end of the contract.
- Minimum security measures recommended by Canadian privacy regulators through recent data breach or privacy investigations (see lessons learned from recent cases involving Equifax, Loblaw, Desjardins, TD Canada Trust, BMO and Marriott).
- An obligation to report any data breach or security incident involving the outsourced personal information.
- Permission to conduct a review or audit of the service provider's security measures during the contract.

Any provision allowing the service provider to use the information for its own purposes, such as improving its products and services – even if this information is de-identified or anonymized – should be assessed in light of recent concerns raised by the Canadian privacy regulators in a recent case involving Tim Hortons.

8. Adaptability: Our plans for new technologies and data analytics comply with changing data protection laws and public expectations.

The board should ensure management is assessing the privacy impact of new services, products and even partnerships. Given the many grey areas in data protection laws, management should be looking beyond basic compliance to the ethical issues involved in using data. Consent, as I've mentioned, is key to privacy in Canada. The appropriate form of consent depends on the circumstances, sensitivity of the information and the individual's reasonable expectations. These expectations can be difficult to assess, especially since social norms are constantly evolving and individuals may even sometimes change their minds about whether a technology violates their privacy.

Two Canadian examples speak to the importance of context. In one, the privacy commission of Canada concluded that the type of consent obtained in a relevant advertising program launched by a Canadian telecommunications company should have been opt-in instead of opt-out. Canadian privacy regulators also concluded that a company was collecting and using personal information of visitors to its Canadian malls via anonymous video analytics (AVA) technology and mobile device geolocation tracking technologies without valid consent.

The board should discuss with management any business analytics initiatives involving information that will be affected by the Canadian privacy reform, including:

- The use of certain types of sensitive information, such as biometrics.
- Technologies that allow the profiling, location tracking and identification of individuals, including the use of facial recognition, AI and machine learning technology.
- The use of technology to make automated decisions that may have an impact on consumers or employees.

- Different types of legal obligations depending on whether the information is personal, de-identified or anonymized.

9. Business transactions: We have a framework to adequately assess personal information protection and security risks in the context of mergers and acquisitions and investments.

Corporate investments and mergers and acquisitions are two business transactions that introduce cyber and privacy risks, and the board needs to ask if the company has a framework for proper due diligence. When it comes to M&A, cautionary tales abound, and household names like Yahoo!, PayPal, Uber, Asco, Marriott and Okta have experienced negative consequences including fines, reduction in company value, negative impacts on purchase price, and cancellation of deals. These examples illustrate the importance of conducting appropriate data security and privacy due diligence during M&A, especially for transactions involving:

- Business-to-consumer companies.
- The processing of sensitive personal information.
- The monetization of personal information.
- The introduction of novel business practices, products and services.

10. Cybersecurity: We can protect personal information in compliance with applicable laws and respond appropriately to a security incident involving personal information.

Under Canadian laws, businesses must protect personal information against loss, theft, unauthorized access, disclosure, copying, use and modification by employing security safeguards in keeping with the sensitivity of the information. If there is a security breach, privacy regulators will usually verify that the organization had the proper technical measures and relevant policies, practices and procedures in place, including training.

Managing cybersecurity risk is an ongoing exercise that requires constant review and improvement, given that new threat actors and evolving attack techniques reveal new vulnerabilities. Boards should ensure there is an incident response plan with proper documentation of incident response roles and responsibilities and an up-to-date list of stakeholders and contact information. This plan should be tested through simulated breaches and tabletop exercises and updated annually.

In the event of a data breach, the business should consult with the board on all important matters, including ransoms, media interviews and statements to regulatory authorities, law enforcement, impacted customers, employees and other stakeholders.

11. Money: We know the financial risks associated with data privacy and have a plan to mitigate them.

Current financial risks related to data privacy are mostly related to the management of security incidents. Additional financial risks include potential fines for failing to report data breaches and the costs associated with defending or settling privacy disputes. Boards should ensure management is tracking its financial exposure related to data privacy, including monitoring the penalties once new provisions are in force – particularly the dollar value in case of a worst possible event. The board should also discuss cyber liability insurance and coverage amounts on an ongoing basis.

Conclusion

Given the changing regulatory landscape and evolving expectations of consumers and investors, directors and senior officers of Canadian companies will have to allocate more time and resources to ensure their companies are following best practices for data governance and privacy risk.

The checklist above is a good start. You're on the right track if you understand the purpose and strategy for collecting and retaining information; know the type and location of the information you have; develop a robust, adaptable, well-resourced privacy program and know its stress points; are able to easily access relevant information to demonstrate compliance to regulators; have compliant outsourcing contracts; pay attention to privacy risks associated with business transactions; are ready for the inevitable cyber breach; and have a plan to mitigate the financial risks associated with data privacy.

Expertise

Cybersecurity, Privacy & Data Protection, Technology

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