Canadian Privacy Law Review

VOLUME 20, NUMBER 2 Cited as (2023), 20 C.P.L.R. JANUARY 2023

• BILL C-26: RIGHTS GROUPS OPPOSE CANADA'S NEW CRITICAL INFRASTRUCTURE PROTECTION LAW •

Brent J. Arnold, Partner, Gowling WLG

• In This Issue •

BILL C-26: RIGHTS GROUPS OPPOSE CANADA'S NEW CRITICAL INFRASTRUCTURE PROTECTION LAW
Brent J. Arnold 17

BILL C-27: THE IMPACT OF PROPOSED CHANGES ON THE PROVINCIAL (ALBERTA) PRIVACY LEGISLATION
John Sanche and Emeka Ezike-Dennis 22

SEVEN SURVIVAL GUIDE LESSONS FROM A FORMER CHIEF PRIVACY OFFICER
Roland Hung 26

HOUSE OF COMMONS COMMITTEE RECOMMENDS NATIONAL PAUSE ON THE USE OF FACIAL RECOGNITION TECHNOLOGY
Latisha Cohen and Sigma Khan 29

Brent J. Arnold

In June 2022, the federal government introduced its first-ever federal cyber security law of general application aimed at protecting critical infrastructure. The reaction was, at first, muted but positive. The bill has not moved past first reading, and since Gowling WLG's initial review of the bill,[1] damning critiques have emerged from many groups.

WHAT DOES BILL C-26 DO?

Bill C-26, formally titled *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*,[2] implements positive cyber security (as opposed to privacy) obligations on operators of critical infrastructure. There are two portions to the bill:

1. Amendments to the *Telecommunications Act*: C-26 amends the federal *Telecommunications*

CANADIAN PRIVACY LAW REVIEW

Canadian Privacy Law Review is published monthly by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.

ISBN 0-433-44417-7 (print) ISSN 1708-5446
ISBN 0-433-44650-1 (PDF) ISSN 1708-5454
ISBN 0-433-44418-5 (print & PDF)

Subscription rates: $420.00 per year (print or PDF)
$636.00 per year (print & PDF)

Please address all editorial inquiries to:

General Editor
Professor Michael A. Geist
Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law
E-mail: mgeist@uottawa.ca

LexisNexis Canada Inc.
Tel. (905) 479-2665
Fax (905) 479-2826
E-mail: cplr@lexisnexis.ca
Web site: www.lexisnexis.ca

Act to allow the federal government to impose obligations on telecommunications service providers to "secure the Canadian telecommunications system"; and

2. *Critical Cyber Systems Protection Act* (the "CCSPA"): The bill also introduces an entirely new law empowering government to designate services or systems as "vital" and to impose data protection obligations on their operators, require mandatory reporting of cyber security incidents, and facilitate threat information exchange "between relevant parties."

Schedule 1 to the CCSPA designates the following services and systems (all areas of existing federal jurisdiction under the constitutional division of powers) as vital:

1. Telecommunications services;
2. Interprovincial or international pipeline and power line systems;
3. Nuclear energy systems;
4. Transportation systems that are within the legislative authority of Parliament;
5. Banking systems; and
6. Clearing and settlement systems.

Enforcement mechanisms under the CCSPA include:

1. The power to issue compliance orders;
2. The power to order an operator to conduct internal audits to assist the regulator in determining the extent of an operator's compliance with the CCSPA and regulations;
3. The power to conduct searches of premises (evidently without warrants, except where the search is to be conducted at a "dwelling-house," i.e., private residence) to verify compliance or prevent non-compliance with the CCSPA and regulations, and in the process of such a search, to access any "cyber system" located and to access information contained on it to copy and/or remove documents or records located;
4. The ability to obtain *ex parte* warrants to conduct searches of dwelling-houses;

5. Where authorized by warrant, the power to use force to carry out searches of dwelling-houses;
6. The ability to impose administrative monetary penalties of up to:
   a. $1 million per individual (i.e., an officer or director who "directed, authorized, assented to, acquiesced in or participated in the commission of [a] violation"), or
   b. $15 million per organization.

The CCSPA also establishes summary and indictable criminal offences for violations of provisions of the CCSPA (including, for example, failure to establish, implement and maintain a cyber security program may be an indictable offence).

The statute provides an exemption from liability for officers and directors where they have performed their duties under the CCSPA in good faith despite the occurrence of a breach. A defence of due diligence is available for violations of the CCSPA.

THE CIVIL RIGHTS CRITIQUE

In late-September 2022, the Canadian Civil Liberties Association, along with a collective including the International Civil Liberties Monitoring Group, the Privacy & Access Council of Canada, and several other groups and academics, released their "Joint Letter of Concern Regarding Bill C-26."[3] [4] While stating the collective's agreement with the goal of improving cyber security, the Joint Letter goes on to state that the bill "is deeply problematic and needs fixing" because it "risks undermining our privacy rights, and the principles of accountable governance and judicial due process."

The Joint Letter outlines several areas of concern, including the following:

- Increased surveillance: The bill allows the federal government to "secretly order telecom providers" to "do anything or refrain from doing anything… necessary to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption". While this portion of the bill (s.15.2(2)) goes on to list several examples of what "doing anything" might entail—including, for example, prohibiting telecom providers from using specific products or services from certain vendors or requiring service providers to develop security plans—the collective expresses the concern that the power to order a telecom to "do anything" "opens the door to imposing surveillance obligations on private companies, and to other risks such as weakened encryption standards."
- Termination of essential services: C-26 allows government to "bar a person or company from being able to receive specific services, and bar any company from offering these services to others, by secret government order", which raises the risk of "companies or individuals being cut off from essential services without explanation."
- Undermining privacy: The bill provides for collection of data from designated operators, which could potentially allow the government "to obtain identifiable and de-identified personal information and subsequently distribute it to domestic, and perhaps foreign, organizations."
- Lack of "guardrails to constrain abuse": The bill would allow government to act without first being required to perform proportionality, privacy or equity assessments to hedge against abuse, which is concerning to the collective given the severity of the penalties available under the statute.
- Secrecy impairing accountability, due process and public regulation: Many of the collective's concerns stem from the fact that government orders issued under the bill may be made in secret, without public reporting requirements, making it impossible for rights groups and the public to monitor and challenge how power is exercised under the bill. The secrecy attaching to such orders could impair the ability of operators subject to orders to challenge them in court, because key evidence about secret orders (which would be required for a court challenge) could also be kept secret from the operators.
- Potential for abuse by CSE: The CCSPA would grant the Communications Security Establishment

(the federal agency responsible for cyber security, but more prominently, signal intelligence) access to large volumes of sensitive data, but would not constrain its use of such data to its cyber security mandate.[5]

Citizen Lab, an academic research laboratory studying digital threats to civil society, released a report[6] on the Joint Letter. Focusing on the bill's amendments to the *Telecommunications Act* in particular, the report raises several additional concerns about Bill C-26, including the following:

- Compliance costs: As not *all* telecom service providers are large companies, the cost of complying with orders made under the amended statute (which could include having to change service providers and/or swap out already-purchased equipment) "may endanger the viability of smaller providers";
- Vague language: The report notes that:
  - Key terms in the bill such as "interference," "manipulation", and "disruption" (which trigger the government's ability to make orders binding on telecom service providers) are undefined;
  - The Minister of Industry's scope of power to make orders is undefined; and
  - The bill does not explain how personally identifiable information about individual Canadians (which attracts privacy law obligations under both current and proposed federal privacy laws) is to be handled and protected.

Citizen Lab's report makes no fewer than 30 different recommendations for fixing the myriad problems it identifies in Bill C-26.

THE BUSINESS COMMUNITY CRITIQUE

The Business Council of Canada released its own letter to the Minister of Public Safety[7] expressing the business community's concerns about Bill C-26. Focusing on the proposed CCSPA, the Council's concerns include the following:

- Lack of a risk-based approach: The CCSPA requires the same actions from *all* operators falling under the statute's jurisdiction "irrespective of their cyber security maturity", meaning many critical infrastructure operators that already have robust cyber security programs will have to incur additional costs to comply with the CCSPA "with no associated benefit" to them for doing so.
- Information sharing is one-way: Operators are required to provide information to government, but receive nothing back from the government or other operators, i.e., the bill misses the opportunity to implement an information-sharing regime that could benefit all operators subject to the law;
- The legal threshold for issuing directions is too low: As drafted, the government may issue secret orders to operators "for the purpose of protecting a critical cyber system" (s.20(1)). The Council is concerned that this threshold is vague enough to allow orders to be made even where the threat to a critical system is "negligible, and therefore not a credible danger to Canada's national security".
- Penalties: The Council suggests the proposed monetary penalties and prison terms are "unduly high and unnecessary to encourage" operators to take the measures the CCSPA requires to improve their cyber security posture.
- Brain drain: The prospect of personal liability for certain breaches of the CCSPA could dissuade cyber security professionals from taking jobs in Canada (the Council points out that there are already over 25,000 unfilled positions in the field in Canada).

In all, the Council's letter proposes 21 measures for improving the CCSPA and four recommendations for changing the proposed amendments to the *Telecommunications Act*.

CONCLUSION

While more groups are likely to comment on the bill in the weeks to come, the emerging stakeholder consensus appears to be that Bill C-26 contains myriad flaws ranging from the technical to the conceptual

and fundamental. It will be interesting to see whether and how the bill emerges from the Committee stage of its review.

[***Brent J. Arnold*** *is a partner practising in Gowling WLG's Advocacy department, specializing in cyber security and commercial litigation. Brent heads the firm's Commercial Litigation Technology sub-group. In 2019, he co-authored the Canada chapter of Chambers Global Practice Guide: Data Protection & Cybersecurity, 2nd ed. In 2022, he co-authored the Canada chapter of the Chambers FinTech 2022: Trends and Developments report. Brent's experience includes cyber breach coaching, cyber risk analysis, class actions defence, Web3 (including cryptocurrency and Metaverse) and other technology, software and e-commerce disputes, administrative and insolvency law, shareholders' rights, class actions, employment contracts, and general contractual disputes.*]

---

1 Brent J. Arnold, Naïm Antaki & Latisha Cohen, "Bill C-26: Canada's Critical Infrastructure Cyber Security Law", *Gowling WLG* (June 20, 2022), online: https://gowlingwlg.com/en/insights-resources/articles/2022/canada-s-critical-infrastructure-cybersecurity-law/.

2 Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess., 44th Parl., first reading June 14, 2022, online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/first-reading.

3 Letter from Brenda McPhail, Director, Privacy, Technology & Surveillance Program at Canadian Civil Liberties Association to the Honourable Marco E.L. Mendocino, Minister of Public Safety (September 28, 2022), online: ttps://ccla.org/privacy/joint-letter-of-concern-regarding-bill-c-26/.

4 Brenda McPhail is credited as the author of the letter on the CCLA's website. McPhail gave a lengthy interview about the bill on law professor Michael Geist's podcast, Law Bytes, which helpfully explains with examples the collective's concerns about the bill: "The Law Bytes Podcast, Episode 142: CCLA's Brenda McPhail on the Privacy and Surveillance Risks in Bill C-26" (October 17, 2022), online: https://www.michaelgeist.ca/2022/10/law-bytes-podcast-episode-142/.

5 While not stated in the Joint Letter, the director of CCLA's Privacy, Technology and Surveillance Program has publicly raised the concern that CSE might share this data with foreign intelligence authorities and would not be able to control how those authorities use the data. She raises the historical example of information being shared with U.S. authorities resulting in the torture of Canadian Maher Arar. Brenda McPhail, "The Law Bytes Podcast, Episode 142: CCLA's Brenda McPhail on the Privacy and Surveillance Risks in Bill C-26" (October 17, 2022), online: https://www.michaelgeist.ca/2022/10/law-bytes-podcast-episode-142/.

6 Christopher Parsons, "Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the *Telecommunications Act*", *The Citizen Lab* (October 18, 2022), online: https://citizenlab.ca/2022/10/a-critical-analysis-of-proposed-amendments-in-bill-c-26-to-the-telecommunications-act/.

7 Letter from Goldy Hyder, President and Chief Executive Officer, Business Council of Canada to the Honourable Marco E.L. Mendocino, Minister of Public Safety (September 14, 2022), online: https://thebusinesscouncil.ca/publication/enhancing-the-resiliency-of-canadas-critical-cyber-systems/.

• BILL C-27: THE IMPACT OF PROPOSED CHANGES ON THE PROVINCIAL (ALBERTA) PRIVACY LEGISLATION •

John Sanche, Partner, and Emeka Ezike-Dennis, Special Projects Counsel,
Burnet, Duckworth & Palmer, LLP

John Sanche

Emeka Ezike-Dennis

Bill C-27 (*An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*) (Bill C-27) passed its first reading in the House of Commons on June 16, 2022 and is currently at its second reading.

If passed into law, Bill C-27 will bring sweeping changes to the Canadian private sector privacy law landscape, to modernize it for the digital age. The changes may also lead to a loss of the exemption status currently extended to some provinces that have enacted their own private sector privacy laws that are substantially similar to the federal *Personal Information Protection and Electronic Document Act* (PIPEDA), unless these provinces update their laws to align with the anticipated changes in the relevant parts of Bill C-27. This article will highlight some of the steps taken by the Alberta Legislature to comply with these changes.

Bill C-27 will result in the enactment of three new statutes:

1. The *Consumer Privacy Protection Act* (CPPA), which will repeal and replace parts of the PIPEDA to reflect current technological changes in the processing of private sector personal information;
2. The *Personal Information and Data Protection Tribunal Act* (PIDPTA), which will establish the Personal Information and Data Protection Tribunal; and
3. The *Artificial Intelligence and Data Act* (AIDA), which will establish rules around the responsible deployment of Artificial Intelligence (AI) technologies, including establishing an AI and Data Commissioner to be responsible for assessing and mitigating the risks of harm and bias, and outlining criminal offences and penalties relating to the use of AI technologies.[1]

RELATIONSHIP WITH THE PROVINCIAL PRIVATE SECTOR PRIVACY LAWS

To provide some background, PIPEDA was enacted in 2001 to apply to organizations that collect, use, or disclose personal information in the course of commercial activity. It applies in any of the following instances:

- The protection of personal information belonging to clients and employees of federally regulated organizations, such as airports, banks, inter-provincial transportation companies, telecommunications companies, radio broadcasters, etc., that conduct business in Canada;
- Organizations that, in the course of their commercial activities, collect, use, and disclose personal information within a province, except where the province has privacy laws that are deemed to be "substantially similar" to PIPEDA (as is the case in the following provinces - Alberta, British Columbia, and Québec); and
- All businesses handling information that crosses either a provincial or the national border, in the course of commercial activities, regardless of the province.

The federal government's power to enact PIPEDA derives from its authority to regulate trade and commerce under section 91(2) of the *Constitution Act, 1867* (the Constitution). In 2004, the government of Québec initiated a reference case to challenge the constitutionality of PIPEDA, arguing that it impinged the legislative competence of the provinces over property and civil rights within the provinces (s. 92(13)). This raised a constitutional issue, but was later dropped.[2]

The argument for federal authority for PIPEDA by some constitutional lawyers is that in pith and substance, it is primarily concerned with regulating the commercial exploitation of personal information. Therefore, any effects on provincial matters are subsidiary to this primary federal objective and a necessary incident of the exercise of the federal government's extra-provincial trade and commerce power.[3]

To avoid constitutional challenges to the legislation, the drafters of PIPEDA struck a compromise by giving the opportunity to the provinces for exemption, on the condition that they adopt substantially similar laws (section 26(2)(b) of PIPEDA). As it stands, the following provinces have enacted their own private sector privacy laws: Alberta enacted its *Personal Information Protection Act* (Alberta's PIPA);[4] British Columbia enacted its own *Personal Information Protection Act* (BC's PIPA); and Québec has *An Act Respecting the Protection of Personal Information in the Private Sector* (Québec Privacy Act). Consequently, organizations that, in the course of commercial activities, manage personal information within these provinces are governed by their respective provincial privacy legislation in areas where the provincial legislation overlaps with PIPEDA.

THE CPPA

Just as PIPEDA before it, section 6(2)(b) of the proposed CPPA brings under its purview all personal information collected, used, or disclosed by an organization in the course of its commercial activities within a province "to the extent that the organization is not exempt from the application of this Act under an order made under paragraph 122(2)(b)".[5]

The referenced paragraph 122(2)(b) gives the Governor in Council the power to make an order if it is satisfied that the legislation of a province that is substantially similar to the CPPA applies to an organization or an activity, and as a result, exempt such organization or activity from the applicability of the CPPA.

What this means is that provinces with their own private sector privacy laws must update their laws to comply with the new CPPA, otherwise the exemption status currently enjoyed by the province under PIPEDA will likely effectively be revoked when the proposed CPPA comes into full effect. At the same time, the other Canadian provinces and territories that have not enacted their own private sector privacy legislation will be subject to the new CPPA in place of the repealed PIPEDA.

It is not clear if any grace period will be extended to those provinces currently with their own private sector privacy laws to enable them update their laws prior to section 6(2)(b) coming into effect. However, section 122(3) gives the Governor in Council the power to make regulations establishing applicable criteria and the process for determining that a provincial privacy law is substantially similar to the CPPA. One expects that the Governor in Council will use these broad powers to help make the transition a seamless one for the provinces concerned.

Québec has enacted new legislation in Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* (Quebec's Bill 64), overhauling its current private sector privacy laws. Quebec's Bill 64, also known as Law 25, received royal assent on September 22, 2021 and will replace the current Québec Privacy Act in a phased manner until late 2023 when most of the changes will become operational.[6]

On December 9, 2020, the B.C. legislature appointed a special committee to review BC's PIPA.

As part of the exercise, the B.C. Commissioner submitted recommendations to this special committee, most of which were in alignment with, or went further than, the changes anticipated in the former Bill C-11, *An Act to enact the Consumer Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts* (Bill C-11), a predecessor of Bill C-27, which died in the 2021 legislative session.[7]

CALLS FOR CHANGES IN ALBERTA

Alberta, the last of the three jurisdictions with its own private sector privacy legislation, now has some work to do to bring its current legislation into alignment with the anticipated changes at the federal level.

In her November 2020 letter to the Minister of Service Alberta, the former Information and Privacy Commissioner (the IPC) called for reforms in Alberta's privacy laws. She emphasized the need to bring Alberta's PIPA in line with the now-defunct Bill C-11, in order to avoid any impact on Alberta's PIPA's "substantially similar" standing federally. Included in the commissioner's letter, were some ideas for modernizing Alberta's PIPA, many of which reflect the changes proposed in the CPPA.

While presenting the 2020-21 Annual Report, the IPC also commended the flexibility of the existing framework and its support for robust assessment of new technologies. However, she admitted that new technologies are straining the existing legislative models beyond their limits. She reported that consultations are currently ongoing within the Alberta government on engaging the general public and other stakeholders to bring about the needed changes to the laws to mirror the changes in other parts of Canada.[8]

OVERVIEW OF THE REVIEW PROCESS IN ALBERTA

Section 63 of Alberta's PIPA provides for a comprehensive review of its provisions by a special committee of the Legislative Assembly every six years after the date on which the previous special committee submitted its final report. In compliance with this provision, the Alberta Legislature passed Government Motion 29 on May 25, 2022, referring Alberta's PIPA to the Standing Committee on Alberta's Economic Future (the Committee), to serve as the special committee for conducting a comprehensive review, as required by Alberta's PIPA, and to allow for stakeholder input from the public through written submissions. The committee is expected to present its report to the Legislative Assembly within 18 months of inception, in accordance with section 63(2) of Alberta's PIPA.

The Committee met on September 27, 2022, and according to the meeting transcript posted on its webpage, discussed seeking a full and adequate understanding of Alberta's PIPA by inviting technical briefings from Service Alberta (the ministry responsible for administering Alberta's PIPA) and the office of the IPC at a future meeting of the committee. The committee adjourned its meeting, acknowledging its commitment to conclude its work and present a report to the Legislative Assembly by March 27, 2024.[9]

CONCLUSION

Proponents of provincially-enacted privacy legislation have given reasons for their preference for exemption from the federal statute. Some of these reasons include the broader scope of the provinces' property and civil right power (s. 92(13)) as compared to the federal government's trade and commerce power; the confusion that results from determining which law applies when there's a breach and to which oversight body the complaint should be directed; and the need for timely recalibration of principles in response to rapid technological changes in the market-place, etc.[10] As Bill C-27 makes its way through the legislative rounds, the sweeping changes anticipated could result in the revocation of Alberta's PIPA for not being substantially similar to the proposed CPPA. It is hoped that the Alberta Legislature will close

the gap soon enough with a revision of Alberta's PIPA that aligns it closely with the new CPPA, so that organizations in Alberta can continue to enjoy exemption (in applicable circumstances) from the proposed CPPA when it comes into effect, on account of Alberta's "substantially similar" standing.

[***John Sanche*** *is a Partner at Burnet, Duckworth & Palmer, LLP. His focus is on intellectual property and technology, commercial transactions, start-ups and early-stage companies, anti-corruption and bribery, and franchises, dealerships, and distributorships.*

Emeka Ezike-Dennis *is Special Projects Counsel at Burnet, Duckworth & Palmer, LLP. Emeka is an internationally trained lawyer and was called to the Alberta Bar earlier this year. He is experienced in advising clients on corporate commercial transactions, intellectual property law, foreign investment and regulatory matters. Emeka also has a background in procurement of projects in the Canadian construction and energy sectors.*]

---

1 Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, 1st Sess., 44th Parl., 2022, first reading June 16, 2022, online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading.

2 Teresa Scassa, "Fresh Questions about the Constitutionality of PIPEDA?", *Teresa Scassa* (January 17, 2012), online: https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=96:fresh-questions-about-the-constitutionality-of-pipeda?&Itemid=80.

3 Josh Nisker, "PIPEDA: A Constitutional Analysis" (2007) 85-2 Canadian Bar Review 317, online: https://www.canlii.org/en/commentary/doc/2007CanLIIDocs108#!fragment//BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoByCgSgBpltTCIBFRQ3AT0otokLC4EbDtyp8BQkAGU8pAELcASgFEAMioBqAQQByAYRW1SYAEbRS2ONWpA.

4 *Personal Information Protection Act*, S.A. 2003, c. P-6.5.

5 Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, 1st Sess., 44th Parl., 2022, first reading June 16, 2022, online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading.

6 Adam Kardash, Michael Fekete & Maryna Polataiko, "Canada's freight train of privacy legislative reform continues", *Osler* (December 31, 2021), online: https://www.osler.com/en/resources/regulations/2021/canada-s-freight-train-of-privacy-legislative-reform-continues.

7 Office of the Privacy Commissioner of Canada, "Comparison of BC OIPC's Submissions on PIPA reform and OPC Submission on C-11", online: https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/bc_20210622/comp_bc_20210622/.

8 Office of the Information and Privacy Commissioner of Alberta, *2020-21 Annual Report* (November 2021), online: https://oipc.ab.ca/wp-content/uploads/2022/01/Annual-Report-20-21.pdf.

9 Legislative Assembly of Alberta, Standing Committee on Alberta's Economic Future, "Personal Information Protection Act Review" (September 27, 2022), online: https://docs.assembly.ab.ca/LADDAR_files/docs/committees/ef/legislature_30/session_3/20220927_0900_01_ef.pdf.

10 Letter from Patricia Kossein, Information and Privacy Commissioner of Ontario, to the Honourable Lisa M. Thompson, Minister of Government and Consumer Services (October 16, 2020), online: https://www.ipc.on.ca/wp-content/uploads/2020/10/2020-10-16-ipc-private-sector-consultation-submission.pdf.

• SEVEN SURVIVAL GUIDE LESSONS FROM A FORMER CHIEF PRIVACY OFFICER •

Roland Hung, Counsel, Torkin Manes LLP

Roland Hung

With the recent wave of privacy reforms sweeping across Canada and abroad, including changes to the privacy legislation in Quebec with Bill 64 ("Quebec Privacy Law") and the proposed reform to the federal private sector privacy legislation with Bill C-27, the role privacy officers play in organizations has garnered significant attention. Having gained substantial leadership experience as a privacy officer, what follows in this article is the perspective I gained in these unique and essential roles. Each mandate, while quite different in practice, harvested similar lessons that I believe every practitioner working in the privacy sector should adopt to maximize their effectiveness within their organization. The following are seven key lessons every privacy officer or practitioner should know.

1. OBTAIN SUPPORT FROM THE TOP

For any privacy officer to be effective in their role, they must be supported from the top, a principle that was codified by the Quebec Privacy Law, which clearly states that an organization has to ensure that its privacy officer has the authority to ensure that the organization is in compliance with the Quebec Privacy Law. The Quebec Privacy Law appoints the CEO as the privacy officer by default, unless the CEO delegates this responsibility to someone else in the organization.

Unlike the Quebec Privacy Law, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") and other similar privacy legislation in Canada do not explicitly state that the individual "exercising the highest authority in the organization" is accountable for ensuring compliance. However, it is important for an organization to empower the privacy officer with the necessary authority to obtain and uphold compliance and act as the face of privacy compliance for the company.

Quite simply, if the privacy officer does not have support from the top, it is unlikely they will be able to perform their role effectively.

2. ALIGN THE PRIVACY OFFICE WITH THE ACTUAL RISK EXPOSURE OF THE ORGANIZATION

The privacy office must be customized and tailored to the organization. There are many factors that should be taken into consideration when building the privacy office, including the following:

- Size of the organization;
- Resourcing and budget that the organization can allocate to the privacy office;
- Type of personal information collected, used and disclosed by the organization;
- Actual privacy risk exposure of the organization; and
- Type of stakeholders (customers, investors, patients, employees, etc.).

There is no "one size fits all" model for building a privacy office that aligns with every organization's culture and infrastructure. The privacy office should also be adaptable and flexible to evolve and change with the organization over time. For example, as the organization's products and service offerings change,

the privacy office must be able to adapt to those changes in tandem.

Taking into consideration the factors outlined above, here are three different privacy office models to consider:

- **Low Risk Exposure**. In smaller organizations, where the actual privacy risk exposure is low, the organization may appoint an executive or their delegate with a central and cross-cutting role (most commonly, the COO, CFO or CEO) as the privacy officer. The challenge with this model is that often the executive or their delegate may not have the expertise or knowledge to fully perform the duties of the privacy office. One way to address this issue is to ensure that the privacy officer receives ongoing training.
- **Medium Risk Exposure**. In medium to large organizations where there is a general counsel or legal team, the general counsel or more senior counsel may be appointed as the company's privacy officer. My two in-house positions adopted this model, extending the legal role to include that of the privacy officer. There is a natural affinity between the legal department and privacy office, since the legal team is already responsible for legal compliance with the relevant privacy regulatory framework, while the privacy office is responsible for operationalizing the privacy compliance framework.
- **High Risk Exposure**. In larger organizations where privacy risk exposure is high (such as financial institutions), the organization may want to consider appointing a dedicated privacy officer or creating a separate privacy office.

Regardless of model, the privacy office should be not be treated as a mundane part-time function that is tacked onto existing responsibilities if the goal is to establish a proper privacy compliance program.

3. DEFINING PRIORITIES

The first and most important step I took after accepting the roles of Chief Privacy Officer of the emerging technology company, and later, as Global Privacy Officer of the multinational, was taking time to understand the business and define my priorities in each role. To achieve this, I examined the companies' stakeholders and how they collected, used and disclosed personal information. After stepping back to see the big picture, the privacy officer needs to synthesize his or her priorities, which may be divided into monthly priorities, annual priorities, or five-year priorities. It is difficult to access unlimited resources to enable a privacy officer to achieve an endless list of priorities. To address this reality, I built priorities and then allocated resources towards each phase. Aligning the privacy priorities with available resources enables the achievement of tangible goals.

To the extent possible, the privacy officer's priorities should align with the priorities of the organization. For example, a shared priority of the privacy office and the organization may be to deliver a better customer experience by building trust. United by this goal, the privacy office can work with the organization to build trust by being transparent about its privacy practices.

4. SPECIALIZING IN CRISIS MANAGEMENT

An important goal for any privacy officer is to become a crisis management specialist, taking the lead in managing crises and investigations and, with unwavering support from the top, making decisions that elicit compliance across the organization.

Part of becoming a crisis management specialist is anticipating a series of potential crises before they arise and pre-emptively preparing written plans, procedures, and/or policies on how to respond to a certain type of crisis; building and training the crisis team; testing those plans, procedures, and/or policies in a mock setting to see how well they work; and revising them as necessary after obtaining feedback from the test.

Periodic training on how to most effectively respond to any given crisis is also helpful. For example, table exercises on responding to a data breach and/or ransomware attack will assist the privacy officer

(and the cross-functional team) in developing the skills necessary to respond to a real data breach or ransomware attack.

Becoming a crisis management specialist elevates and reinforces the importance of a privacy officer's position in an organization, making them an invaluable resource especially when confronted with crises.

5. USE THE PRIVACY COMPLIANCE PROGRAM TO BUILD TRUST WITH CUSTOMERS

The role of the privacy officer is not strictly about regulatory compliance. In my roles, I quickly learned that, from a business perspective, the value-add of the privacy office is the way the privacy compliance program can be used to build customer trust and enhance the company's reputation.

Especially for technology companies that handle personal health data, building customer trust and creating a sense of transparency are vital to customer experience, and ultimately, to the success of the company. Because building trust with the customers was so important to us, the privacy office communicated regularly with the communications, sales, product and marketing teams to find strategic ways to educate customers and communicate how the company collects, uses and discloses personal health information, as well as protects and safeguards the personal health information provided.

6. DEVELOP A ROBUST PRIVACY COMPLIANCE PROGRAM WITH THE CHIEF INFORMATION SECURITY OFFICER ("CISO")

In my experience, aligning goals and priorities with the CISO's priorities is a key consideration when developing a more robust privacy compliance program.

The responsibilities and skills of the CISO often complement the responsibilities and skills of the privacy officer. To successfully operationalize privacy compliance programs, an organization needs both regulatory expertise and technical knowledge. Oftentimes, privacy officers possess the regulatory expertise, while the CISO brings the technical expertise on data security, networks, data governance and infrastructure. The goal is to marry the two skillsets, which creates a comprehensive function to effectively operationalize an organization's privacy compliance programs.

Areas where a privacy officer may collaborate with a CISO include:

- Data breach incident response policy and procedure;
- Employee privacy and cybersecurity training;
- Data classification and management;
- Data retention; and
- Vendor due diligence and contract negotiations.

Neither the security nor privacy office would be effective operating as silos. The CISO and their team are vital to safeguarding personal information, breach response, and general compliance with applicable privacy laws. I was fortunate to have had good relationships with the CISOs with whom I worked. Together, CISOs and privacy officers are to achieve far greater results than when the two groups operate independently.

7. EVOLVING PRIVACY LAWS

Privacy laws are always changing and evolving, and the privacy officer is responsible to remain informed on changing privacy laws and how they may affect their organization.

As the Chief Privacy Officer of the health analytics company, I had to keep abreast of all current health information legislation across Canada and the US. Similarly, during my tenure as the Global Privacy Officer, the international focus of my role meant that I had to keep abreast of changing privacy laws in the UK, EU, Argentina, Chile, Bolivia, Uruguay and Canada. Of note, the GDPR and Brexit came into force during my tenure, which meant that my team had to navigate the EU GDPR and the UK GDPR.

However, beyond keeping up with ever-evolving privacy laws, to the extent that your organization has a change management team, use that team

to operationalize the required changes. If your organization does not have a change management team, learn how to operationalize change effectively. The most effective privacy officers understand how to drive change effectively within an organization.

[***Roland Hung*** *is Counsel in Torkin Manes' Business Law and Technology, Privacy & Data Management Groups. His practice encompasses all aspects of corporate and commercial law, with emphasis on technology, privacy compliance, cybersecurity and data management. Prior to joining Torkin Manes, Roland was the Chief Legal Officer and Chief Privacy Officer of Vivametrica Ltd., a large multinational, and the Senior Legal Counsel and Global Privacy Officer of Finning International Inc., a technology company.*]

• HOUSE OF COMMONS COMMITTEE RECOMMENDS NATIONAL PAUSE ON THE USE OF FACIAL RECOGNITION TECHNOLOGY •

Latisha Cohen, Associate, and Sigma Khan, Articling Student, Gowling WLG

Latisha Cohen

Sigma Khan

Is your use of facial recognition technology in line with the evolving legal landscape? While official regulation of these technologies is scarce, new guidance and recent developments are telling of where the law is likely heading, and you will want to be on trend. It is no secret that the use of facial recognition technologies is under-regulated and there is uncertainty with regard to the extent to which these technologies can be utilized without infringing on the privacy rights of individuals. However, recent developments and suggestions to Parliament by the House of Commons Standing Committee on Access to Information, Privacy and Ethics ("the Committee") provide some guidance.

In October 2022, the Committee issued 19 recommendations to Parliament in a report (the "Report") addressing facial recognition technologies ("FRT"). The recommendations are an attempt to persuade legislators that the law should evolve to become equipped to handle the unique challenges that come with the widespread use of FRT. The Committee suggested that the government impose a national pause on the use of FRT until there is an appropriate legal framework in place.[1]

The Report recommends that the legal framework for FRT be bolstered through amendments to the *Privacy Act* and the *Canadian Human Rights Act*.[2] Additional recommendations include the implementation of an opt-in-only requirement for the collection of biometric information by the private sector and strengthening the ability of the Privacy Commissioner under the *Personal Information Protection and Electronic Documents Act (*"PIPEDA") to levy meaningful penalties on governments and private entities whose use of FRT violates Canadian privacy law.

In late 2021, FRT were the subject of a high-profile joint investigation by the Office of the Privacy Commissioner of Canada ("OPC") and its provincial counterparts in Alberta, British Columbia and Quebec. The case involved the investigation of an FRT software company and the RCMP. The latter utilized the company's data to conduct hundreds of biometric searches across Canada.[3] The investigation resulted in findings of violations of the PIPEDA and the *Privacy Act.* There were more than three billion images of faces gathered from the internet without users› consent.[4] The investigation concluded that such an action represented mass surveillance and deduced that there were violations of section 4 of Canada's *Privacy Act.*

It is startling to think how prevalent FRT is and how little guidance exists to regulate its use. The average individual interacts with FRT multiple times a day to unlock their smartphones, access banking apps, and to apply social media filters. Beyond the more mundane use of this technology, FRT has far-reaching impacts and implications due to the ubiquity of cameras. FRT has also been extremely useful in the delivery of critical services. Transportation companies use FRT to reduce traffic congestion, the healthcare field utilizes the technology to diagnose and monitor patients, and the government border services uses it to ensure travel security. The list keeps growing. However, the value of these technologies is greatly diminished, and potentially counter-productive, without organizations being able to regulate their use under comprehensible and transparent mandates. So how can companies rely on these technologies to deliver key services within the parameters of acceptable use?

First, use the decisions from the PCO and the Committee's Report as guidance for your policies and to determine what is likely acceptable. How are you using the data, and is it for the purpose for which consent was obtained? It is likely prudent to have an opt-in policy, especially for sensitive biometric data. For further guidance, industries that intend to rely on FRT can also look to examples in the United States.

FRT in the United States has been more widely employed and legislated than in Canada. In Illinois, for example, the laws require healthcare collectors of biometric identifiers, such as facial features, to provide notice, obtain consent, and to maintain a retention schedule.[5] It would not hurt to consider similar policies, especially for highly sensitive biometric data.

Finally, keep an eye out for new developments and constantly consider whether your use of FRT is on trend with the evolution of the law. It does not hurt to get ahead of the trend – but it may cost to lag.

[***Latisha Cohen*** *is an associate in Gowling WLG's Toronto office. Latisha completed her JD at Osgoode Hall Law School. Prior to law school, Latisha founded a program called Sisters of the Soil, which facilitates solidarity initiatives between Indigenous women and their non-Indigenous allies. Latisha has a particular interest in Aboriginal law and advocacy. She participated in the 2017 Julius Alexander Isaac Diversity Moot, where her team took first place in the finals and she received the top prize for best oralist.*

Sigma Khan *is an articling student in Gowling WLG's Toronto office. Throughout Sigma's legal studies, she has been involved in the research stages of broad cross-border commercial litigation and class actions matters. Sigma has a special interest in privacy and technology litigation. She is currently pursuing her CIPP/C designation.*]

---

1 Pat Kelly, Chair, *Facial Recognition Technology and the Growing Power of Artificial Intelligence: Report of the Standing Committee on Access to Information, Privacy and Ethics* (October 2022), online: https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf.

2 Pat Kelly, Chair, *Facial Recognition Technology and the Growing Power of Artificial Intelligence: Report of the Standing Committee on Access to Information, Privacy and Ethics* (October 2022), online: https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf.

3 Pat Kelly, Chair, *Facial Recognition Technology and the Growing Power of Artificial Intelligence: Report of the Standing Committee on Access to Information, Privacy and Ethics* (October 2022), online: https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf.

4 Office of the Privacy Commissioner of Canada, "Police use of Facial Recognition Technology in Canada and the way forward" (June 10, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

5 Odia Kagan, "Illinois' Biometric Information Privacy Act Is Coming for Hospitals, Long-Term Care Providers", *JDSupra* (March 2, 2022), online: https://www.jdsupra.com/legalnews/illinois-biometric-information-privacy-9254443/.