Canadian Privacy Law Review

VOLUME 22, NUMBER 1 Cited as (2024), 22 C.P.L.R. DECEMBER 2024

• QUÉBEC'S NEW DATA PORTABILITY LAW: KEY FEATURES YOU MUST KNOW •

Amir Kashdaran, Partner, McMillan LLP

• In This Issue •

Amir Kashdaran

On September 22, 2024, Québec's new data portability law took effect, introducing additional obligations on companies subject to the *Act respecting the protection of personal information in the private sector* ("Quebec Privacy Act").

This data portability law was introduced by the *Act to modernize legislative provisions respecting the protection of personal information* (commonly known as "Law 25"), amending the Quebec Privacy Act.

Law 25 introduced various amendments to the Quebec Privacy Act slated to take effect in three phases. As of September 22, 2022, the first phase of the obligations set out under Law 25 took effect followed by a second phase on September 22, 2023. This year, starting on September 22, 2024, the third and final phase of the amendments to the Quebec

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

Privacy Act, as provided by Law 25, will take effect, namely the data portability law.

In this article, we will provide you with an overview of the new data portability law requirements in the private sector under the Quebec Privacy Act, allowing you to take the proper compliance measures.

Let's get started.

1. WHAT IS THE LEGAL BASIS FOR THE NEW DATA PORTABILITY LAW IN THE PRIVATE SECTOR?

The legal basis for the new portability law in the private sector is the new Article 27 of the Quebec Privacy Act, which reads as follows:

> Every person carrying on an enterprise who holds personal information on another person must, at the request of the person concerned, confirm the existence of the personal information, communicate it to the person and allow him to obtain a copy of it.
>
> At the applicant's request, computerized personal information must be communicated in the form of a written and intelligible transcript.
>
> Unless doing so raises serious practical difficulties, computerized personal information collected from the applicant, and not created or inferred using personal information concerning him, must, at his request, be communicated to him in a structured, commonly used technological format. The information must also be communicated, at the applicant's request, to any person or body authorized by law to collect such information.
>
> If the person concerned is handicapped, reasonable accommodation must be provided on request to enable the person to exercise the right of access provided for in this division.

Now, let's break it down in detail.

2. WHO IS SUBJECT TO THE PORTABILITY LAW?

The new portability law applies to "every person carrying on an enterprise" who holds personal

information on another person. The notion of "every person carrying on an enterprise" is defined broadly under Quebec laws. In essence, Article 1525 of the *Civil Code of Quebec* states that the "carrying on by one or more persons of an organized economic activity, whether or not it is commercial in nature, consisting of producing, administering or alienating property, or providing a service, constitutes the operation of an enterprise." In other words, if you do business in Quebec or engage in activities, commercial in nature or not, and hold personal information on an individual, you will need to comply with the new portability law.

3. WHAT IS THE RIGHT TO DATA PORTABILITY?

The right to data portability means that any individual can request that an organization:

1. confirm the existence of their personal information; and
2. require that their personal information be communicated to them; or
3. allow them to obtain a copy of their personal information.

With the right to data portability, individuals are put in the driver's seat with respect to the control of their personal information, allowing them to request and receive the communication of their personal information.

4. ARE THIRD PARTIES AUTHORIZED TO RECEIVE THE COMMUNICATION OF PERSONAL INFORMATION?

Article 27 of the Quebec Privacy Act states that an individual's personal information must be communicated, at the individual's request, "to any person or body authorized by law to collect such information." Consequently, we could broadly interpret the authorized data recipient to include third parties such as an individual's spouse, relative, or other persons designated by the individual, any governmental body or agency authorized by law to collect the individual's personal information.

5. WHAT TYPE OF PERSONAL INFORMATION IS SUBJECT TO DATA PORTABILITY RIGHTS?

The new portability law specifically states that "computerized personal information" that is "collected from the applicant" and which is "not created or inferred using personal information" of the individual is subject to portability rights.

Let's break down each of the required elements.

A) Computerized Personal Information

The first element to consider here is that portability rights concern "computerized personal information." In other words, we can consider that personal information relating to an individual held on information technology systems is targeted by the portability obligation. Also, since the law specifically uses the term "computerized" to refer to the medium where the information is held, we could consider that other media may be excluded, such as personal information contained in "paper" format or handwritten documents.

B) Personal Information Collected from the Applicant

The second element to consider is that the computerized personal information must have been collected "from the applicant." This means that an individual can make a data portability request with respect to computerized personal information that they provided to the organization, either manually or through automated means.

C) Information that is Created or Inferred by the Organization

The third element to consider is that information that was "created or inferred" by the organization

using personal information is specifically excluded. In other words, an individual can only request that an organization provide their computerized personal information in its original condition. This legal exclusion is intended to protect companies from having to share information that may be considered their business confidential information, trade secrets, or more broadly, their intellectual property.

6. HOW MUST AN ORGANIZATION COMMUNICATE THE PERSONAL INFORMATION TO AN INDIVIDUAL?

The new Article 27 of the Quebec Privacy Act states that an organization must communicate an individual's computerized personal information in "the form of a written and intelligible transcript".

Although the notion of a written and intelligible transcript is not specifically defined in the Quebec Privacy Act, we can look at Articles 19 and 23 of the *Act to establish a legal framework for information technology* in an attempt to better interpret these terms. We could consider that the term "written" refers to information that is accessible by means of a written document, and the term "intelligible" refers to information that a person can understand.

Putting all of this together, the Quebec Privacy Act requires that the organization communicate an individual's personal information in written form and in a manner that the individual can understand.

7. IN WHAT FORMAT WILL THE ORGANIZATION NEED TO COMMUNICATE AN INDIVIDUAL'S PERSONAL INFORMATION?

According to the Quebec Privacy Act, companies must communicate an individual's personal information in a "structured" and "commonly used technological format." The notions of "structured" and "commonly used" along with "technological format" are not specifically defined. As such, we could turn to comparable privacy legislation to interpret their meaning.

Here is what the United Kingdom's Information Commissioner's Office says:

> "Where no specific format is in common use within your industry or sector, you should provide personal data using open formats such as CSV, XML and JSON. You may also find that these formats are the easiest for you to use when answering data portability requests."[1]

As such, companies could use CSV, XML, and JSON as generally accessible formats to communicate an individual's personal information.

The notion of "structured" could refer to information that is easily accessed and processed by individuals where data elements are clearly defined and separated.

The notion of a "commonly used" format could refer to a file format that is easily accessible to the public, widely adopted, and would not require specialized tools to access. We could also get inspiration from the notion of a "machine-readable format" used under the *General Data Protection Regulation* in Europe referring to a format that can be easily parsed by a computer and is interoperable with other technological systems.

Putting all of this together, we could say that an organization must communicate an individual's personal information using a file format that is easily accessible to the general public, where the data elements are structured, and that individuals can access their personal information without needing to use specialized software or tools.

8. CAN ORGANIZATIONS REFUSE TO COMMUNICATE PERSONAL INFORMATION FURTHER TO A DATA PORTABILITY REQUEST?

In certain circumstances, organizations may refuse to comply with an individual's data portability request, particularly when doing so "raises

serious practical difficulties." This means that if an organization would incur significant costs or have to deal with significant complexities to communicate the individual's personal information in a structured and commonly used technological format, then they could refuse to comply with the data portability request. However, in the event of a complaint, organizations will bear the burden to demonstrate that the costs or complexities adequately justified their decision to refuse an individual's data portability request.

Organizations could also rely on any exceptions applicable to an individual's right to access their information. For example, an organization could refuse access to information where disclosure of the information would be likely to reveal the identity of a third party who has not consented to it, cause serious harm to the same, affect ongoing legal proceedings, or when the request is manifestly unfounded, excessive, or abusive.

9. ARE THERE RESTRICTIONS THAT MAY APPLY TO PORTABILITY RIGHTS?

We could reasonably identify a couple of instances where there may be restrictions applicable to an individual's exercise of data portability rights, particularly when it relates to anonymous data and information that falls in the realm of a company's proprietary information.

With respect to anonymous data, since the information can no longer allow the identification of an individual or an identifiable individual, then that information will no longer be portable. Also, information that has been significantly transformed or created in a way that involves intellectual property rights, may be excluded from portability to protect the company's rights.

Organizations should exercise care in ensuring that they balance their privacy obligations and the protection of their proprietary interests, bearing in mind that the existence of intellectual property rights might not serve as a "blanket" argument to deny an individual's portability rights. The law specifically exempts organizations from communicating information that was "created" or "inferred" using an individual's personal information. However, the exclusion does not necessarily extend to the personal information underlying the created or inferred information.

CONCLUSION

In conclusion, Quebec's new data portability law marks an important shift in how personal information is handled within the province. By empowering individuals with the right to access and transfer their data, the Quebec Privacy Act reinforces the importance of transparency and control over personal information. For businesses, this law brings new obligations that must not be overlooked.

Ensuring compliance with these regulations is not just a legal necessity but a crucial step in building trust with your customers. Organizations operating in Quebec or subject to the Quebec Privacy Act should take the time to understand their new data portability obligations and update their data management practices accordingly. Doing so will not only allow them to meet their statutory obligations, but also strengthen their privacy posture as responsible custodians of personal information.

[***Amir Kashdaran*** *is a Partner in Tech & Privacy at McMillan LLP, practicing in Quebec, Canada. He offers a full range of legal advisory services to national and international companies in various fields, including technology, intellectual property, and privacy and data protection. He advises on matters such as complex software licensing, technology monetization, smart products, the development or use of artificial intelligence technologies, and other technological tools.*]

---

1 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-data-portability/?q=purpose (accessed on August 30, 2024)

• LOOKING TO BALANCE ANONYMITY WITH ACCOUNTABILITY, ONTARIO SUPERIOR COURT ORDERS DISCLOSURE OF WHISTLEBLOWER'S IDENTITY •

Jordan Deering, Partner, Regan Christensen, Associate, Ryan Hamieh, Associate, DLA Piper LLP


Jordan Deering


Regan Christensen


Ryan Hamieh

In *Taylor v. Metrolinx*, the Ontario Superior Court of Justice addressed a contentious application for a Norwich order, a legal remedy often sought to compel third-party disclosure of key information. The Applicants, Brandon and Sarah Taylor and their company JAAX Inc., sought to uncover the identity of an anonymous whistleblower who had made serious allegations against them, including fraud, embezzlement, and racketeering. These allegations were reported to Metrolinx, a Crown Corporation accountable for how public funds are spent on construction projects, where Metrolinx reported such allegations to Brandon's employer, Dufferin Construction Company, and its subsidiary, Mosaic Transit Contractors.

The Applicants argued that they needed the complainant's identity to pursue claims for defamation, intentional infliction of mental distress, and economic interference. Metrolinx opposed the application, pointing to confidentiality agreements and the potential risk to the safety of the anonymous complainant if their identity were disclosed. Applying the test established by the Supreme Court of Canada for granting a Norwich order, the Court considered whether the Applicants had a bona fide claim, whether Metrolinx was involved in the matter and the only practical source for the information, and whether public interest justified breaching the complainant's privacy.

In its examination, the Court concluded that the Applicants had sufficient grounds for their claims and rejected the argument that the complainant's identity was protected by confidential source privilege, reasoning that the communication was not confidential in nature under the Wigmore test criteria. Ultimately, the Court ruled in favor of disclosure, highlighting that the public interest in accessing the truth outweighed Metrolinx's concerns about confidentiality and safety. In considering the four Wigmore factors, the Court emphasized that the complainant's communication did not meet the criteria for confidential source privilege, predominantly since the communication

was unsolicited and the complainant did not have an expectation of confidentiality when making the complaint. The Court concluded that the privacy policy contemplated that the personal information could be disclosed and that "this is not an individual acting in the capacity of employee seeking to take advantage of protections available to a corporate whistleblower."

IMPACT OF A ROBUST POLICY

Metrolinx's privacy policy was crucial in determining the outcome of this decision, as it was published on the Metrolinx website and provided explicit guidance on how personal information would be collected, used, and disclosed. A robust policy not only informs individuals of their rights and what to expect when they submit personal data but also protects the organization by clarifying the boundaries of consent and disclosure.

In this case, the clear language of the policy allowed the Court to conclude that the complainant had consented to the use and potential disclosure of their information, negating any claim to privilege or anonymity. Without a strong, clear policy, organizations risk misunderstandings, legal disputes, and breaches of trust with individuals who provide sensitive information.

IMPLICATIONS FOR WHISTLEBLOWER CONFIDENTIALITY

The *Taylor v. Metrolinx* ruling has significant implications for the use of Norwich orders in defamation and related claims. The Court found that no assurances of confidentiality were in fact provided to the complainant through the policy, and drew a distinction between a member of the general public submitting an unsolicited report of alleged misappropriation of funds and an employee seeking the protections available to a corporate whistleblower. By granting the Applicants access to the complainant's identity, the Court reinforced the principle that individuals making serious allegations cannot insist on their identity being withheld without a strong legal basis for doing so and should be wary in making potentially damaging claims. This decision also serves as a reminder that if an organization seeks to provide whistleblowers with confidentiality protections, they should do so explicitly in their privacy policy by utilizing clear and express language.

[***Jordan R.M. Deering*** *is a Partner and the Chair of DLA Piper's Canadian Corporate Crime, Compliance and Investigations Group. Jordan's practice has focused on litigation, investigations and regulatory proceedings involving all aspects of fraud and corporate misconduct. She regularly acts for financial institutions and corporate clients in respect of these sensitive, high stakes mandates.*

Regan Christensen *is a member of DLA Piper's Canadian Corporate Crime, Compliance and Investigations Group. Regan's practice focuses primarily on investigations and litigation related to fraud, bribery, corruption, compliance, and white-collar crime. He also maintains a broad commercial litigation and alternative dispute resolution practice. A skilled negotiator and advocate, Regan has represented a wide range of clients from major banks and public institutions to small and medium-sized businesses.*

Ryan Hamieh *is a member of DLA Piper's Canadian Corporate Crime, Compliance and Investigations Group and has a broad commercial litigation practice that focuses on personal and institutional fraud recovery, director and officer liability, compliance and contractual disputes. Ryan conducts meticulous, business-focused investigations and is committed to providing strategic guidance and practical solutions that enables companies to navigate complex legal issues effectively.*]

• PRIVACY COMMISSIONER DECISIONS IMPOSE SWEEPING NOTIFICATION REQUIREMENTS FOR RANSOMWARE AND EMAIL ACCOUNT COMPROMISE INCIDENTS •

Alex Cameron, Partner, Daniel Fabiano, Partner, Dongwoo Kim, Articling Student, Fasken LLP


Alex Cameron


Daniel Fabiano


Dongwoo Kim

The Information and Privacy Commissioner of Ontario ("**IPC**") recently issued four landmark decisions that impose sweeping notification requirements in respect of ransomware attacks and email account compromise incidents.

In three of the decisions, the IPC adjudicator found that notification to individuals is required where information is rendered inaccessible to an organization because of ransomware encryption, even if the attacker does not exfiltrate, access or view the information and the information is later restored by the organization. In the fourth decision, the IPC adjudicator found that notification to individuals is required where an attacker gains access to an email account containing personal information and the organization cannot rule out the possibility that the attacker viewed information in the account.

In this bulletin, we review the IPC decisions and discuss the implications of the decisions for organizations in Ontario and across Canada.

BACKGROUND

The IPC decisions arose pursuant to the *Ontario Personal Health Information Protection Act* ("**PHIPA**") and *Child, Youth and Family Services Act* ("**CYFSA**").

Entities subject to PHIPA are required to notify individuals "at the first reasonable opportunity" if personal health information is "stolen or lost or if it is used or disclosed without authority." Entities subject to CYFSA are subject to the same requirement in respect of breaches of personal information collected for the purpose of providing a service pursuant to that law.

Neither PHIPA nor CYFSA include a harm-based threshold for notification. In other words, unlike the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") and other laws, which require notification to individuals only in cases where there is a "real risk of significant harm" resulting from a breach, notification under PHIPA and CYFSA is required in each instance where the applicable information is "stolen or lost or if it is used or disclosed without authority."

RANSOMWARE DECISIONS

PHIPA Decisions 253 and 254 and CYFSA Decision 19 involved cybersecurity attacks where information was encrypted with ransomware.

In the former decisions, the IPC adjudicator determined that ransomware encryption attacks, which made "personal health information unavailable and inaccessible to authorized users of that information" constituted "handling" or "dealing with," and therefore were an unauthorized "use" of, the information.[1] The adjudicator noted that this

unauthorized "use" is established "whether or not the threat actor actually views or accesses specific files of personal health information held within the affected containers, or exfiltrates that information […]."[2]

The adjudicator also concluded that there was a "loss" of personal health information triggering the duty to notify on the basis that, as a result of the ransomware encryption, the "information is made unavailable to the authorized user of that information because of an unauthorized activity."[3] The adjudicator distinguished ransomware attacks from "other routine or non-routine disruptions" such as a scheduled software or hardware maintenance or power outage.[4]

The adjudicator further held that neither the recovery of the encrypted information following the payment of ransom for the decryption key, nor the restoration of the information from backups, negates the fact that there had been a "loss" and unauthorized "use" of personal health information as a result of the attack.[5]

In each of the above decisions, the adjudicator determined that the organizations' public communications about the incidents technically did not comply with PHIPA's notification obligation because they did not include a statement that individuals had a right to complain to the IPC (and in PHIPA Decision 254 the organization's statements fell short in other respects).[6] However, in both cases, the adjudicator concluded that there would be no useful purpose in ordering that further notification be given.[7]

CYFSA Decision 19 addressed a ransomware encryption incident against a social services organization involving the personal information of minors collected pursuant to CYFSA. Following the reasoning above, the adjudicator determined that the encryption constituted an unauthorized "use" and "loss" that triggered a duty to notify pursuant to CYFSA. However, the adjudicator adopted a flexible approach to notification, in part because more than two years had passed since the incident. The adjudicator ordered that the organization could provide indirect notification of the breach "through means such as posting a notice on its website or issuing a public release".[8]

EMAIL ACCOUNT COMPROMISE DECISION

PHIPA Decision 255 involved unauthorized access to an employee email account containing unencrypted personal health information for a period of one hour.

The organization was able to demonstrate that attacker did not use the account to download emails or send or forward any emails. However, the organization acknowledged that it was not possible to know whether the attacker searched the inbox, or viewed or opened the emails in the account containing personal health information. On this basis, the IPC adjudicator concluded that, on a balance of probabilities, the attack involved unauthorized "disclosure" and "use" of personal health information requiring notification to individuals pursuant to PHIPA.[9]

In addition, while the respondent organization had notified individuals in this case, the adjudicator held that the organization failed to meet its obligation to do so "at the first reasonable opportunity" as the notices were sent a year after the incident.[10]

CONFLICT WITH EXISTING PRACTICES

The IPC decisions are at odds with the practices of many organizations. For example, with respect to ransomware cases, where information is not viewed or taken by an attacker but is merely encrypted by the ransomware program, and is later recovered through decryption or from backups, many organizations typically consider that there has been no "loss" or unauthorized "use" of the information triggering notification to individuals; rather, the information was only temporarily inaccessible.

In addition, PHIPA Decision 255 suggests that where there is a *potential* breach of personal health information because the organization is not able to rule out the possibility that information was viewed by an attacker or other unauthorized individual, organizations must nonetheless treat that as a breach and notify individuals accordingly. This is inconsistent with the practices of many organizations. Moreover, the IPC's rationale could seemingly be applied to *any* scenario, not just email compromise cases, where: (a) an unauthorized individual is *able* to access

personal information; and (b) the organization cannot rule out the possibility that the personal information was accessed.

IMPLICATIONS OF THE DECISIONS

All organizations subject to PHIPA and CYFSA should be mindful of the IPC's expansive interpretation of when the obligation to notify individuals is triggered under those laws, particularly in respect of ransomware and email compromise incidents. Where possible, such organizations should seek to gather evidence to distinguish the IPC decisions from the incidents that they experience.

Also, organizations subject to PHIPA and CYFSA should not assume that the IPC will adopt a flexible approach to notifications in future. While the IPC was prepared to adopt a flexible approach in the cases discussed above, particularly given that years had passed since the incidents in question, the IPC plainly expects, and PHIPA requires, that notification be made in the prescribed manner "at the first reasonable opportunity".

Beyond PHIPA and CYFSA, it remains to be seen whether the above IPC decisions may influence other Canadian privacy regulators' interpretation of when a privacy breach is considered to occur.[11] Most Canadian privacy laws applicable to the private sector, public sector, and health sector, including PIPEDA, contain privacy breach notification provisions. The definition of when a breach occurs under such statutes is similar to the definition under PHIPA and CYFSA. Organizations should anticipate the possibility that the IPC decisions may influence other regulators to expansively interpret the circumstances that qualify as a breach. In their investigation and response to incidents, organizations should seek to identify facts that will help distinguish such incidents from those addressed in the IPC decisions.

On the other hand, it should be noted that, unlike PHIPA and CYFSA, almost all privacy laws in Canada, including Ontario's proposed amendments to its public sector privacy law, include a harms-based threshold for determining whether an organization must notify individuals about a breach. In PIPEDA and other statutes, for example, a breach must give rise to a "real risk of significant harm" or similar threshold, before organizations are required to notify individuals. This threshold may limit the extent to which other Canadian privacy regulators are influenced by the IPC decisions. However, given that the IPC decisions expansively interpret what qualifies as a breach, organizations should ensure that legal advice is obtained in determining whether notification is required pursuant to privacy laws that include a harm-based threshold. This determination could have a very significant impact on the scope of notifications, if any, that may be needed in a given case. Privacy breach plans and incident response plans should be updated in light of the above.

[***Alex Cameron*** *is co-leader of the Privacy and Cybersecurity Group at Fasken. He is widely recognized as one of Canada's leading cybersecurity and privacy lawyers. Clients from all sectors, including numerous Fortune 100 and 500 companies, consistently turn to Alex in cybersecurity, privacy and related matters, including for cybersecurity attacks, regulatory proceedings and in defence of landmark privacy class action litigation. He is consistently ranked in the highest band in legal rankings guides and was recognized by his peers as the Privacy and Data Security Law "Lawyer of the Year" in Toronto in The Best Lawyers in Canada 2024.*

Daniel Fabiano *is a partner at the Fasken law firm. His business law practice focuses on privacy/information protection and data commercialization. He advises a wide range of clients on novel data-sharing arrangements, legal compliance and risk management – including responding to privacy breaches and regulator investigations. His practice also focuses on the unique considerations arising under provincial health sector privacy laws.*

Dongwoo Kim *is an articling student in Fasken's Toronto office. He graduated from the University of Toronto's Faculty of Law, where he pursued research in AI and data privacy. Dongwoo managed a research program focussed on digital/technology policies at a national think tank prior to law school. He holds*

degrees from the University of Alberta (BA), the University of British Columbia (MA), and Peking University (MA), where he was part of the Yenching Scholars program.]

---

1 PHIPA Decision 253 at para 40. See also PHIPA Decision 254 at para 29.

2 *Ibid* at para 42. See also PHIPA Decision 254 at para 30.

3 *Ibid* at para 50. See also PHIPA Decision 254 at para 36.

4 *Ibid* at para 51. See also PHIPA Decision 254 at para 37.

5 *Ibid* at paras 36 and 49. See also PHIPA Decision 254 at para 36.

6 *Ibid* at para 65; PHIPA Decision 254 at para 48.

7 *Ibid* at para 65; PHIPA Decision 254 at para 49.

8 CYFSA Decision 19 at para 75.

9 PHIPA Decision 255 at para 25.

10 *Ibid* at paras 58-59.

11 The determination that a breach has occurred will trigger record-keeping obligations in a number of Canadian privacy laws, including PIPEDA. As discussed below, whether notification and reporting obligations are triggered will depend on a harm-based threshold under most Canadian privacy laws.