Canadian Privacy Law Review

VOLUME 22, NUMBER 3 Cited as (2025), 22 C.P.L.R. FEBRUARY 2025

• PRIVACY AND DATA-RELATED LAW REFORM IN CANADA: OUTLOOK FOR 2025 •

Joanna Fine, Partner, Adam Kardash, Partner, Andy Nagy, Associate, and Maryna Polataiko, Associate, Osler, Hoskin & Harcourt LLP

Joanna Fine

Adam Kardash

Andy Nagy

Maryna Polataiko

Over the past several years, privacy legislative reform in Canada has seen significant activity, particularly at the provincial level, while federal legislative reform efforts have seen very limited progress. This legislative reform has been focused on the introduction of significantly enhanced enforcement regimes, including potentially severe financial penalties for contraventions of privacy requirements. These initiatives also introduce new requirements for documented internal governance mechanisms, requirements for enhanced transparency regarding personal information practices and provisions that facilitate individuals' control over their data.

More broadly, a growing array of privacy and data obligations are being introduced in sector-specific and other legislative proposals.

Given the significant compliance costs and the threat of severe monetary fines for violations of privacy obligations, it is more important than ever for companies doing business across Canada to have a thorough understanding of their personal information

• In This Issue •

LexisNexis®

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)

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

and data practices. Equally important is the implementation of documented internal governance mechanisms and other compliance tools that may be required to meet their obligations under these updated and pending laws.

QUÉBEC'S PRIVATE SECTOR PRIVACY REGIME CONTINUES TO EVOLVE

Québec's private sector privacy legislation introduced potentially severe penalties for non-compliance. Failure to comply with the *Act respecting the protection of personal information in the private sector* ("***Québec Privacy Act***") exposes organizations to fines of up to the greater of $25 million and the amount corresponding to 4% of worldwide turnover for the preceding fiscal year. Non-compliance can also expose organizations to administrative monetary penalties of up to the greater of $10 million and the amount corresponding to 2% of worldwide turnover for the preceding fiscal year.

To date, the Québec privacy regulatory authority, the Commission d'accès à l'information du Québec ("**CAI**"), has not imposed any fines or penalties on a company. However, the CAI is currently involved in multiple regulatory investigations that are expected to conclude in 2025. The highly anticipated decisions in these investigations will provide early indications of the CAI's enforcement approach, especially with respect to the quantum of monetary penalties that may be awarded.

This past year, there were two significant changes to the Québec privacy regime.

First, in May 2024, the Québec *Regulation respecting the anonymization of personal information* introduced prescriptive requirements for organizations when anonymizing records containing personal information. Organizations must carry out anonymization under the supervision of a "qualified" person, assess the risks of re-identification, implement appropriate anonymization techniques and other measures to reduce these risks and periodically re-assess the risks of re-identification to ensure that data remains anonymized.

Second, in September 2024, the final amendments to the Québec Privacy Act came into effect and introduced the first "data portability" right under Canadian privacy laws.

Based on the experience of companies under the European Union's General Data Protection Regulation ("**GDPR**"), the process of responding to data portability requests may prove operationally challenging and costly. Companies will have to ensure that personal information subject to portability requests is both readily accessible and in a "structured, commonly used and technological format." The Québec Privacy Act does not specify acceptable formats, but recent guidance issued by the Québec government indicates that open and interoperable formats such as CSV, XML and JSON are considered suitable, while formats such as PDF would not be acceptable. To respond effectively to data portability requests in 2025 and beyond, companies may have to engage in a time-consuming, technically complex and resource-intensive process of standardizing data across systems that may use proprietary and incompatible data or file formats.

As of January 1, 2025, organizations will also have to maintain a register with detailed information about the information that was anonymized, the purposes for which this information will be used, the anonymization techniques and the dates of the original, as well as any subsequent re-identification risk analyses.

NEW HEALTH PRIVACY LAW INTRODUCED IN QUÉBEC

In July 2024, Québec also introduced onerous health privacy legislation. Québec was previously one of the only provinces without dedicated provincial health privacy legislation. The *Act respecting health and social services information* sets out a comprehensive set of rules governing the collection, use and communication of "health and social services information" by "health and social services bodies." This term broadly captures various organizations involved in delivering health and social services, such as public health and social services institutions, private health facilities, laboratories, specialized medical centres, health communication centres and centres for assisted reproduction.

Complying with this new health privacy law may be expensive and resource-intensive. Organizations will need to address a series of requirements regarding the protection of personal health information similar to those mandated by the Québec *Privacy Act*. The legislation also imposes certain unique obligations, such as a requirement for health and social services bodies to use "certified" technological products and services in certain circumstances. The certification procedure and the circumstances in which certified products and services must be used will be set out in regulation, which has not yet been published.

Organizations that operate in the health sector, including service providers, will need to review this new legislation carefully to determine whether the legislation applies. If so, it will be necessary to conduct a thorough review of their personal health information practices to ensure compliance with these new prescriptive obligations.

FEDERAL AND PROVINCIAL PRIVACY LEGISLATIVE REFORM

During 2024, Bill C-27, which would replace existing federal privacy legislation ("**PIPEDA**") and create the first AI law in Canada, remained before the Standing Committee on Industry and Technology. Given the precarious minority status of the federal government and the high likelihood of an early election, it is doubtful that the bill, in its current form, will be enacted. If enacted, Bill C-27 would impose significant penalties for non-compliance, including fines of up to the greater of $25 million or 5% of gross global revenue for the preceding fiscal year. Administrative monetary penalties of up to the greater of $10 million or 3% of gross global revenue for the preceding fiscal year could also be imposed.

In 2025, legislative amendments in other provinces are likely to follow, starting with Alberta. The review of the *Alberta Personal Information Protection Act* ("**PIPA**") commenced on January 22, 2024. The

Office of the Information and Privacy Commissioner of Alberta ("**OIPC**") submitted a *detailed review* of PIPA to the reviewing committee in May 2024. The reviewing committee's report must be concluded within 18 months. Consistent with trends elsewhere, the OIPC's recommendations include significantly stronger enforcement powers, including potentially severe financial penalties for contraventions of the statute. Other recommendations include requirements for enhanced transparency, a data portability and data mobility right, regulation of automated decision-making and AI, de-identification and anonymization standards and the introduction of protections for children's privacy.

Progress has also been made in reforming provincial privacy and access to information laws in the public sector. On November 25, 2024, Ontario passed Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*. Once proclaimed into force, this legislation will enact the *Enhancing Digital Security and Trust Act* ("**EDSTA**") and amend Ontario's existing *Freedom of Information and Protection of Privacy Act* ("**FIPPA**"). These changes will impose new obligations on public sector entities, including enhanced privacy and cybersecurity measures and specific requirements for the use of AI systems.

Similarly, on December 5, 2024, Alberta enacted Bills 33 and 34, which will replace the existing *Freedom of Information and Protection of Privacy Act* ("**FOIP**") with two new statutes: the *Protection of Privacy Act* ("**POPA**") and the *Access to Information Act* ("**ATIA**"). These Acts, set to come into force by proclamation, introduce enhanced data governance and accountability measures, mandatory breach reporting, and specific requirements for data practices such as automated decision-making, anonymization and data matching. Supporting regulations are anticipated in the spring of 2025.

PRIVACY-RELATED REFORMS IN SECTOR-SPECIFIC REGULATORY REGIMES

In 2025, we can also expect further privacy, security and other data-related requirements to be embedded within a growing array of new sector-specific legislative proposals.

CYBERSECURITY REQUIREMENTS FOR CRITICAL INFRASTRUCTURE

By way of example, in 2025, the federal government may continue advancing its proposal to bolster the cybersecurity framework for the country's critical infrastructure. However, as with other federal legislative initiatives, the timing is now quite uncertain and the likelihood of the proposal's enactment in its current form prior to an election is increasingly doubtful. If enacted, Bill C-26, the *Critical Cyber Systems Protection Act*, would create new powers for the federal government to respond swiftly to national security threats affecting federal critical infrastructure systems. The proposed legislation includes new requirements relating to the implementation of robust cybersecurity programs, incident reporting and record-keeping that would apply to vital services and systems. Those identified as vital currently include telecommunications services, interprovincial or international pipeline and power line systems, nuclear energy systems, transportation systems within federal legislative authority, banking systems and clearing and settlement systems.

The Act provides for administrative monetary penalties of up to $15 million for each violation.

PROTECTION OF CHILDREN FROM ONLINE HARM

Consistent with legislative initiatives in the E.U., the United Kingdom, Australia and the Asia-Pacific region, the Canadian federal government will likely continue its push to enact Bill C-63, the *Online Harms Act* ("**OHA**").

If enacted, the OHA would impose duties on social media services, adult content services and live streaming services, including an obligation to protect children through an obligation to integrate design features respecting the protection of children. The OHA would also introduce significant penalties for non-compliance, subject to a due-diligence defence.

OPEN BANKING

In 2024, the federal government enacted a legislative scheme for "open banking" in the form of the *Consumer-Driven Banking Act* ("**CDBA**"). The CDBA is not yet in force and its status remains uncertain, but the federal government's stated goal is to implement the governance framework needed for this legislation by 2025.

The CDBA is an "open banking" initiative designed to enhance consumer access and control over their financial data and to facilitate innovative financial services. The proposed open banking framework in the CDBA is, in effect, a consent-based data portability regime.

PACE OF REFORM WILL LIKELY CONTINUE INTO 2025

Significant privacy and data-related legislative reform in Canada will continue in 2025 and beyond. These legislative initiatives will enhance the legal, financial and reputational risks for companies, with potentially severe financial penalties for non-compliance. To mitigate these risks, organizations across all sectors must develop or bolster their data governance practices. Organizations must focus on ensuring they have a thorough understanding of their personal information holdings and practices to address the expanding array of data obligations.

[***Joanna Fine*** *is a partner in the Privacy and Data Management group at Osler, Hoskin & Harcourt LLP. She advises organizations across all sectors, from large multi-national companies to emerging companies, and regularly assists clients in identifying and managing privacy risks associated with complex and innovative data collection and use initiatives, including interest-based advertising, "big data" analytics, AI, surveillance technologies, and anti-fraud initiatives. Joanna also assists clients with security incident response and privacy regulatory investigations.*

Adam Kardash *is an acknowledged Canadian legal industry leader in privacy and data management; he co-leads the national Privacy and Data Management practice at Osler, Hoskin & Harcourt LLP. Adam has been lead counsel on many of the most significant privacy matters in Canada. He advises Fortune 500 clients in their business critical data-protection issues, compliance initiatives and data governance. He regularly represents clients on regulatory investigations and security breaches. Adam is Special Counsel to the Interactive Advertising Bureau of Canada and counsel to the Digital Advertising Alliance of Canada.*

Andy Nagy *is an associate in Osler's Privacy and Data Management group, based in the firm's Montréal office. He advises businesses on a wide range of privacy-related matters, including regulatory investigations, privacy risk assessments and the development and implementation of data governance programs. Andy also regularly advises on complex legal issues related to emerging technologies, including artificial intelligence, biometrics and IoT.*

Maryna Polataiko *is an associate in the Privacy and Data Management Group at Osler, Hoskin & Harcourt LLP. Her practice includes advising on regulatory investigations, product counseling, and data subject requests and complaints. Maryna helps clients navigate federal and provincial privacy laws, as well as the evolving landscape of online platform regulation. She regularly advises on matters relating to biometric data, algorithmic decision-making, children's privacy, and online safety.*]

• LEGAL CONSIDERATIONS IN CANADA RELATED TO "VOICE CLONING" •

Pablo Tseng, Partner, Aki Kamoshida, Articling Student, and Carina Chiu, Partner, McMillan LLP

Pablo Tseng

Aki Kamoshida

Carina Chiu

In late 2023, a song entitled "NostalgIA" and "featuring" Justin Bieber, Bad Bunny and Daddy Yankee went viral on the Internet. If you have been keeping up with pop culture news, you may know that this "dream collaboration"[1] never happened. Rather, "NostalgIA" was a song generated using artificial intelligence and "voice cloning" technology. Voice cloning (also known as audio deepfake) is a process of creating a synthetic copy of one's voice and speech pattern based on a sample audio recording. Such a copy can then be used to create convincing audio clips containing the likeness of the voice of the person whose voice was "cloned". According to news reports,[2] Bad Bunny became particularly upset that a song that he never made but incorporated the likeness of his voice was circulating on the Internet.

In this article, we discuss some potential causes of actions that one may have in Canada if they become victim of voice cloning.

STATUTORY CAUSE OF ACTION: VIOLATION OF PRIVACY

Provinces across Canada have laws to protect privacy interests of individuals. In particular, some provinces like British Columbia, Saskatchewan, Manitoba, Québec, and Newfoundland and Labrador have statutory causes of action pertaining to the violation of one's privacy.[3] These causes of action are based on the unauthorized use of someone's likeness, and most of these pieces of legislation explicitly identify the unauthorized use of someone's voice as an actionable tort.[4] For example, the *Privacy Act* in Manitoba states the following:

> 2(1) A person who substantially, unreasonably, and without claim of right, violates the privacy of another person, commits a tort against that other person.
>
> 3 Without limiting the generality of section 2, privacy of a person may be violated
>
> […]
>
> (c) by the unauthorized use of the name or likeness or voice of that person for the purposes of advertising or promoting the sale of, or any other trading in, any property or services, or for any other purposes of gain to the user if, in the course of the use, that person is identified or identifiable and the user intended to exploit the name or likeness or voice of that person;[5]
>
> [emphasis added]

Although, as of the date of this bulletin, there has not been a reported decision in Canada related to the application of a statutory right to privacy in the context of voice cloning, it is clear that, at least in some provinces, there is a statutory basis for advancing a claim that one's privacy has been violated should one be a victim of voice cloning in such provinces.

APPROPRIATION OF PERSONALITY

In Canada, the tort of "appropriation of personality" is committed when one's personality has been exploited for a commercial purpose without one's consent.[6]

The term "commercial purpose" has been interpreted in Canada to exclude any expression that predominantly serves a social function which is valued by the protection of free speech.[7] For example, in *Gould Estate v. Stoddart Publishing Co.*,[8] the court cited the following passage from a United States decision[9] in its reasoning, ultimately denying the plaintiff's claim that the defendants had appropriated the personality of a famous pianist:

> Thus, the purpose of the portrayal in question must be examined to determine if it predominantly serves a social function valued by the protection of free speech. If the portrayal merely serves the purpose of contributing information, which is not false or defamatory, to the public debate of political or social issues or of providing the free expression of creative talent which contributes to society's cultural enrichment, then the portrayal generally will be immune from liability. If, however, the portrayal functions primarily as a means of commercial exploitation, then such immunity will not be granted.[10]

Note, however, that the facts of a case ultimately determine whether the content created using voice cloning technology would be excluded from the scope of this tort.

A claim pursuant to this tort may also require that the exploitation which a complaining party complains of clearly refers to the complaining party. For example, in *Joseph v. Daniels*, the court stated that a picture of someone's torso, without identifying them by name or face, is not sufficient to meet this part of the test, as it did not point to the plaintiff's "name, reputation, likeness or some other component of the plaintiff's individuality or personality which the viewer associates or identifies with the plaintiff".[11] On the other hand, a photograph of a person's face accompanied by such person's name being featured on flyers was considered sufficient to meet this part of the test.[12]

Recently, the scope of this tort was expanded in British Columbia to provide remedies for not only celebrities, but also professionals whose professional identities had been used and commercially exploited without their permission.[13]

COMMON LAW TORT: FALSE LIGHT

In our previous bulletin, What Has the Law Done About "Deepfake", we discussed the tort of false light as a potential recourse for victims of deepfake technology.[14] The tort of false light is a relatively new tort recognized in Ontario and British Columbia,[15] and targets the wrong of publicly misrepresenting a person.

In claiming that one has been placed in a "false light", one must establish the following:

a. the false light in which the person was placed would be highly offensive to a reasonable person; and
b. the individual had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.[16]

Courts have emphasized that the first step of the above test can be met by showing that "a reasonable person would find it highly offensive to be publicly misrepresented as they have been," and that such misrepresentation does not need to amount to defamation.[17] Further, the courts have noted that the "wrong is in publicly representing someone, not as worse than they are, but as other than they are".[18]

The tort was first recognized in Ontario in *Yenovkian v. Gullian*, a family law proceeding where the respondent sought damages from her ex-husband who had engaged in a long campaign of cyberbullying against her. The cyberbullying involved creating websites and social media posts accusing the wife and her parents of various illegal acts including child abuse, kidnapping and fraud.[19]

The tort of false light was recently recognized by the British Columbia Supreme Court in *Durkin v. Marlan*,[20] a case in which the plaintiff claimed defamation and invasion of privacy torts related to an article authored by the defendant. In particular, the plaintiff argued that the defendant's article placed him

in a misleading light by portraying him as a thief.[21] The Court held that the plaintiff's false-light claim was "legally tenable" but noted that in the circumstances of the case, the plaintiff had failed to prove all of the elements of the tort.[22]

While, as of the date of this bulletin, there are no reported cases in Canada in which the tort of false light has been applied to voice cloning, the potential application of this tort to issues related to voice cloning technology appears to be inevitable.

CONCLUSION

There are several causes of action that may be available for victims of voice cloning, including violation of privacy, appropriation of personality and false light. With the expanding use of deepfakes, including voice cloning, in many aspects of daily life, the likelihood of deepfake technology crossing paths with tort law appears inevitable.

McMillan LLP continues to monitor the developments in generative AI and the law, including their implications on civil liability.

[***Pablo Tseng*** *is a seasoned intellectual property lawyer specializing in patent and trademark prosecution, IP portfolio management, and IP commercialization. Leveraging his background in chemistry, Pablo focuses his practice on the chemical, technology, energy, and agriculture industries.*

Carina Chiu *specializes in complex corporate commercial disputes and commercial leasing matters. She handles shareholder disputes, contract breaches, fraud, and civil conspiracy actions. Carina also represents landlords, tenants, and real estate developers in resolving commercial leasing disputes.*

Aki Kamoshida *recently completed her Juris Doctor at the Peter A. Allard School of Law at UBC. During law school, she held leadership roles in the UBC Law Students' Society and the Alma Mater Society, as well as participated in the UBC Business Law Clinic. Aki holds a Bachelor of Arts in Global Political Economy from Waseda University in Tokyo.*]

---

1 Such collaboration may be a "dream collaboration" to some, but may not be a "dream collaboration" to all.

2 https://www.bbc.com/news/newsbeat-67355245.

3 *Privacy Act*, R.S.B.C. 1996, c. 373; *The Privacy Act*, R.S.S. 1978, c. P-24; *The Privacy Act*, C.C.S.M. c. P125; Article 35 *Civil Code of Québec*; *Privacy Act*, R.S.N.L. 1990, c. P-22.

4 Note that British Columbia's *Privacy Act*, R.S.B.C. 1996, c. 373 focuses on the unauthorized use of one's "portrait". Such term is defined in Section 3(1) of the Act.

5 *The Privacy Act*, C.C.S.M. c. P125, ss 3-4.

6 While in Ontario, the tort is recognized under common law, in some provinces such as British Columbia, appropriation of personality is pled under the provincial *Privacy Act*, as seen in *Poirier v. Wal-Mart Canada Corp*., [2006] B.C.J. No. 1725, 2006 BCSC 1138.

7 *Gould Estate v. Stoddart Publishing Co.*, 30 O.R. (3d) 520, 1996 CanLII 8209 (ON SC).

8 *Ibid.*

9 *Presley v. Russen*, 513 F.Supp. 1339 (U.S. Dist. Ct. D.N.J. 1981).

10 *Gould Estate*, supra note 7 at para 16; the same passage was also cited in *Wiseau Studio, LLc et al. v. Harper et al.*, [2020] O.J. No. 1909, 2020 ONSC 2504 at para 212.

11 *Joseph v. Daniels*, [1986] 1 S.C.R. 103, 1986 CanLII 1106 (BC SC).

12 *Poirier* supra note 6.

13 For example, in *Bao v. Welltrend United Consulting Inc.*, [2023] B.C.J. No. 1753, 2023 BCSC 1566, the tort was applied where a lawyer's identity was used without his consent to submit immigration-related documents.

14 https://mcmillan.ca/insights/what-has-the-law-done-about-deepfake/

15 In a recent decision, the Manitoba King's Bench has noted that the tort has yet to be recognized in Manitoba (*Galton Corporation v. Riley*, [2023] M.J. No. 123, 2023 MBKB 73).

16 *Yenovkian v. Gulian*, [2019] O.J. No. 6702, 2019 ONSC 7279 at para. 170.

17 *Yenovkian*, supra note 16 at para. 171.

18 *Ibid*.

19 *Yenovkian*, supra note 16 at para. 23.

20 *Durkin v. Marlan*, 2022 BCSC 193.

21 *Ibid* at para 23.

22 *Ibid* at para 22.

• BIOMETRICS IN THE WORKPLACE: ISSUES AND LEGAL FRAMEWORK IN QUEBEC •

Natalie Bussière, Partner and Florence Bourque, Associate Blake, Cassels & Graydon LLP

Natalie Bussière

Florence Bourque

Employers are increasingly interested in the use of biometrics in the workplace. In fact, Quebec's privacy regulator, the Commission d'accès à l'information ("**CAI**"), indicates in its 2023-2024 Annual Activity and Management Report (available in French only) that it has received 124 declarations of biometric data collection, which is a 59% increase from 2022-2023.

Biometric systems are used in the workplace to improve the safety and efficiency of human resource management processes. They include various tools that collect data such as fingerprints and hand shapes, as well as facial and voice recognition systems. Current legislation in Quebec regulates the use of these systems by requiring employers to comply with certain specific obligations aimed at protecting employee privacy. Employers in Quebec are also required to demonstrate that they are using these systems for legitimate purposes.

Biometric data is regarded as sensitive personal information and is therefore subject to privacy legislation applicable to the public and private sectors, regardless of the purpose of its use. Given its composition of distinctive characteristics and identifiers, such data is considered intimate information and should be processed carefully.

PRIOR NOTICE TO THE CAI

Employers are required to notify the CAI at least 60 days before collecting biometric data.

ASSESSING THE NECESSITY OF COLLECTING BIOMETRIC DATA

Employers are also required to assess the necessity of collecting biometric data. Pursuant to applicable legislation, the purpose of any such collection must be to address concrete issues and be legitimate, important and real. Here are a few questions to guide this assessment:

- Why is the biometric data being collected?
- For what purpose is the biometric data being used?
- Is there a documented issue that justifies the collection?

The mere convenience or practicality of using biometric data does not, in the CAI's view, constitute a valid justification.

EMPLOYEE PRIVACY

Employers must also consider the risk of intrusion on employee privacy. According to the CAI, employers are required to explore means other than the use of biometrics to address identified issues. An employee's consent to the collection and use of their biometric data does not allow the employer to use this information without proper justification. The CAI has also stated that such consent must be clear, free, informed, given for a specific purpose and valid for a limited period only. Furthermore, employers are required to implement other means of collecting data from employees who do not consent to having their biometric data collected.

DATA PROTECTION AND EMPLOYEE ACCESS

Employers are responsible for putting in place measures that protect the biometric data collected from their employees. Such data must also be destroyed in

a secure manner when no longer useful. In addition, employees should be able to access their personal information and request corrections if necessary.

While the benefits of using biometric data in the workplace are undeniable for workplace safety and efficiency, such use is governed by a strict legal framework that seeks to protect the personal information of employees. Employers can take full advantage of these benefits by complying with reporting requirements, carefully assessing the need for data collection and ensuring data protection.

LEGISLATIVE AMENDMENT

Pursuant to Quebec's *Act respecting the Protection of Personal Information in the Private Sector* organizations may anonymize, for serious and legitimate purposes, personal information they have collected once the initial purpose for which such information was collected or used is achieved. Information is to be considered anonymized if it is, "at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows [a] person to be identified directly or indirectly." Organizations must anonymize personal information "according to generally accepted best practices" and "the criteria and terms determined by regulation."

Furthermore, Quebec's *Regulation respecting the anonymization of personal information*, which came into force on May 30, 2024, establishes criteria and terms applicable to the process of anonymizing personal information in Quebec. Section 9 of the Regulation, which comes into force on January 1, 2025, introduces new provisions for the anonymization of personal information. It provides that any organization that anonymizes personal information must record the following in a register:

1. A description of the anonymized personal information
2. The purposes for which the organization intends to use the anonymized information
3. The anonymization techniques used by the organization
4. The protection and security measures established by the organization
5. The date on which the re-identification risk analysis is completed, as well as the date on which the update of such analysis is completed

There is no doubt that the use of biometrics will become more widespread in the coming years. Employers that abide by the parameters established in the applicable legislation will be able to implement systems that truly improve workplace safety and efficiency.

[***Natalie Bussière*** *is a Partner at Blake, Cassels & Graydon LLP, practising in employment and labour law. Natalie works extensively in the field of employment and labour relations, including negotiating employment contracts, collective agreements and other agreements.*

Florence Bourque *is an Associate at Blake, Cassels & Graydon LLP. Her practice covers all aspects of labour and employment law, advising employers on a wide range of issues, including hiring and termination and employment-policy development, implementation and compliance.*]