Publisher's Note

An Update has Arrived in Your Library for:

Please circulate this notice to anyone in your office who may be interested in this publication. *Distribution List*
☐
☐
☐
☐

THE LAW OF PRIVACY IN CANADA

McIsaac, Klein, Brown

Release No. 4, April 2026

"The Law of Privacy in Canada" is a comprehensive and thorough treatment of the regulation of the collection and use of personal information in Canada. It is the only publication that includes everything lawyers and business professionals need to know about privacy from privacy protection to tackling issues such as public surveillance to the *Personal Information Protection and Electronics Documents Act* (PIPEDA). While the work focuses primarily on the domestic regulatory scene, the factors that have made privacy such a salient topic have also mandated the inclusion of similar developments in the regulation of the collection and use of personal information in the European Union and in the United States. Important areas of coverage include Technology and Privacy: Challenges and Solutions; Privacy Protection Under the Criminal Law; Privacy Protection in the Civil Context; Workplace Privacy; Health Privacy; Public Sector Regulation; Private Sector Regulation; and International Privacy Issues.

This release features updates to Chapter 2, "Privacy Protection in Canadian Criminal and Civil Law", and Chapter 3, "Regulation and Protection of Personal Information in the Canadian Public Sector".

Thomson Reuters®

Customer Support
1-416-609-3800 (Toronto & International)
1-800-387-5164 (Toll Free Canada & U.S.)
E-mail CustomerSupport.LegalTaxCanada@TR.com

Highlights:

Chapter 3—Regulation and Protection of Personal Information in the Canadian Public Sector—I. Federal—§ 3:2. Application—In *McCarthy v. Canada (Indigenous Services)*, 2025 FC 1843, 2025 CarswellNat 4901, the Court distinguished that the names and titles of the Chief, Council members, and staff of Frog Lake First Nation do not constitute personal information, as these individuals form part of a "government institution" in relation to the applicant in this matter. The applicant, a member of Frog Lake First Nation and a former employee, had previously settled a wrongful termination dispute related to concerns about the management of the Nation's trust funds. Following a news article alleging mismanagement of those funds, he authorized the Canadian Taxpayers Federation (CTF) to submit access to information requests seeking Band Council Resolutions authorizing withdrawals from the trust fund. Around the same time, he also requested financial disclosure documents regarding remuneration and expenses for certain fiscal years that had not been publicly posted as required by legislation. Indigenous Services Canada consulted Frog Lake First Nation, which recommended withholding the records on the basis that they contained confidential financial information. However, the Federal Court in this case drew a distinction between the staff or the Chief and Council of the First Nation and officers or employees of a federal government institution.

Chapter 3—Regulation and Protection of Personal Information in the Canadian Public Sector—I. Federal—§ 3:3. Personal Information—In 2025, the Office of the Privacy Commissioner of Canada released guidance on the processing of biometric information by federal institutions, emphasizing the growing importance of biometrics in the privacy landscape. The guidance outlines federal institutions' privacy obligations when collecting, using, and disclosing biometric data. It begins by defining biometric technology and explains that biometric systems capture and analyze measurable human characteristics that can be converted into data. These systems are commonly used for identification or verification purposes, often by enrolling individuals' biometric templates in a reference database and comparing them with other templates. The guidance further defines biometric information as "information about biometric characteristics that has been extracted from a biometric sample." Such information is considered not only personal information but also highly sensitive, as biometric traits are stable over time, difficult to change, and inherently linked to an individual's identity. The OPC also sets out key steps that federal institutions must follow when handling biometric data. These include ensuring lawful authority for the collection, use, and disclosure of the information; conducting privacy impact assessments; demonstrating necessity and proportionality; limiting the collection, use, disclosure, and retention of the data; implementing safeguards to protect the information against

loss, theft, or unauthorized access, use, disclosure, copying, or modification; maintaining accuracy to reduce the risk of false positives and false negatives; ensuring accountability for information under their control; and being open and transparent about how biometric information is managed. The guidance also highlights that biometric information may remain sensitive even if it is collected or retained only for a short period of time, a point that may become the subject of future investigations.

Chapter 3—Regulation and Protection of Personal Information in the Canadian Public Sector—I. Federal—§ 3:3. Personal Information—In *Cache Computer Consulting Corp. v. Canada (Public Services and Procurement)*, 2025 FC 1515, the dispute arose after a request was made under the *Access to Information Act* (ATIA) for records exchanged between Public Services and Procurement Canada (PSPC) and Cache Computer Consulting Corp. relating to federal contracts. PSPC notified Cache that it intended to disclose the responsive records, including the names of consultants that Cache had supplied to perform work under government contracts. The court stated that disclosing the names in the context of invoices and time sheets would undermine, if not entirely eliminate, their confidentiality. The court contended that this differs from situations in which some names appear in the Government Electronic Directory Services (GEDS) or where a consultant is assigned a Government of Canada email address and phone number. The court explained that the distinction lies in the information revealed: releasing names in invoices and time sheets would disclose each consultant's relationship with Cache, whereas listing names in GEDS or assigning a government email address does not reveal that connection. Accordingly, what removes this information from the general principle that publicly disclosed information is no longer confidential merely because it is available through another source is Cache's evaluation of the consultants' qualifications and its reliance on those qualifications when rating them and proposing them to perform work, under contract, for the government institution.

Chapter 3—Regulation and Protection of Personal Information in the Canadian Public Sector—I. Federal—§ 3:4. Restrictions on Collection and Use—In *R. v. Khoshnood*, 2025 BCSC 132, 2025 CarswellBC 1858, the British Columbia Supreme Court held that the *Privacy Act* cannot, on its own, create new powers to search that do not already exist with respect to the disclosure of personal information to law enforcement. Mr. Khoshnood argued that he had a reasonable expectation of privacy in the information forwarded by the Correctional Service of Canada (CSC) to the police, and that the disclosure constituted a presumptively unreasonable search and seizure. He further contended that the police's acquisition of his personal information was not justified under section 8(2)(f) of the *Privacy Act*. The Court explained that this provision did not provide a sufficient legal basis for the disclosure, reasoning as follows:

> [47] First, with respect to the *Privacy Act* provisions, I am guided by the reasoning in *R. v. Flintroy* 2018 BCSC 1692 and *R. v. Spencer* 2014 SCC 43. In the former case, police requested and received a photo of the accused

and his passport application from Citizenship and Immigration Canada. The same provisions of the *Privacy Act* were invoked by the respondent in *Flintroy*, and Justice Williams found the *Privacy Act*, which is meant to protect the privacy of citizens, was not a search power. In other words, the Act on its own could not create new powers to search that did not already exist. I find this reasoning persuasive. I cannot find that s. 8(2)(f) of the *Privacy Act* is a sufficient basis on its own to find there is no objective expectation of privacy for this applicant's CSC information being provided to police.