

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. <i>Distribution List</i>
☐
☐
☐
☐

THE LAW OF PRIVACY IN CANADA

McIsaac, Klein, Brown
Release No. 9, October 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 4. Regulation and Protection of Personal Information in the Canadian Private 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

This publisher's note may be scanned electronically and photocopied for the purpose of circulating copies within your organization.

Highlights:

Chapter 4. Regulation and Protection of Personal Information in the Canadian Private Sector—V. Québec—This section includes updated commentary on guidance from Quebec’s privacy commissioner about Law 25 now that it has been in force. Recent Commission decisions illustrate a strict approach taken to biometric technologies. In a 2024 decision involving facial recognition for workplace access control, the Commission found that photographs of employees’ faces and their mathematical coding were sensitive biometric personal information. Although building security was a legitimate objective, the enterprise had not established a real and important need for facial recognition or that less intrusive access-control methods were insufficient. Recent Commission oversight decisions confirm that the necessity requirement remains a substantive, evidence-based constraint on collection. The enterprise bears the burden of demonstrating that the objective pursued is legitimate, real and important, and that the privacy intrusion is proportionate. In a 2026 decision involving rental applications, the Commission held that verifying identity, creditworthiness and rental history may be legitimate, real and important objectives, but that collection must remain proportionate. The Commission’s current guidance emphasizes that the necessity criterion must be assessed before consent is sought, since valid consent does not cure a collection, use or communication that is not necessary. In January 2026, the Commission published guidance for enterprises on preventing confidentiality incidents. The guide emphasizes that prevention forms part of an enterprise’s accountability obligations and should be integrated into the life cycle of personal information, from collection to destruction.