November 3, 2026

The Intersection between Privacy Law and Contract Law: Consent and Public Policy Concerns in the Age of Patronscan

By: Jassmine Girgis

Matter Commented On: CBC article, "Woman flagged by ID scanner as nationwide 'public safety concern' after incident in Winnipeg bar"

Access to goods and services increasingly comes at the cost of disclosing personal information. Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5 (*PIPA*) regulates private organizations' collection, use, and disclosure of that personal information through requirements governing consent and reasonable purpose. *PIPA* does not, however, expressly address every concern that arises when individuals must accept standardized terms to obtain a service.

Contract law offers a different perspective on the assessment of standardized contractual terms and practices. Its principles governing consent and public policy provide a framework for examining both the implications of unequal bargaining power and the broader consequences of the growing normalization of the collection of personal information. In particular, they offer a basis for considering how the widespread acceptance of certain practices may influence the standards against which their reasonableness is measured. This post explores how those principles might inform the assessment of personal information practices under *PIPA*.

The following discussion concerns information on a driver's license, which includes the holder's name, photograph, birth date, signature, physical description, and driver's license number. This information constitutes personal information, and its collection and use are therefore subject to *PIPA*. See Collection of Driver's License Numbers Under Private Sector Privacy Legislation from the Office of the Privacy Commissioner of Canada, 2008-12-12 and *Leon's Furniture Limited v Alberta (Information and Privacy Commissioner)*, 2011 ABCA 94 (CanLII).

PIPA and Contract Law

This analysis arises from a situation in which an individual was required to let a bar scan her driver's license as a condition of entry. This bar participates in a network that uses the services of Patronscan, an ID scanning company that tracks entry into venues for "security, compliance, and incident reporting" and shares this information across participating establishments. Its network of bars and clubs is known as "Barwatch".

Entry into a bar participating in Barwatch involves a transaction, though not in the conventional sense of an exchange of goods or services for money. As a condition of entry, patrons provide

personal information that may subsequently be used in the Barwatch network. This relationship also includes continuing obligations: the bar is subject to the requirements set out in the applicable signage while patrons must comply with its code of conduct. A failure to comply may result in the individual being barred not only from that establishment, but from other bars in the Barwatch network.

The transaction at the door – entry to the bar in exchange for providing personal information – raises privacy concerns, but it also raises questions under the law of contract. In particular, it invites consideration of whether patrons consented to the applicable terms, and whether the resulting arrangement is consistent with public policy. Although *PIPA* regulates consent and the reasonableness of the collection of personal information, contract law offers additional principles for examining the circumstances in which consent is obtained and the implications of standardized terms imposed in situations where individuals may have little practical ability to refute them.

Background

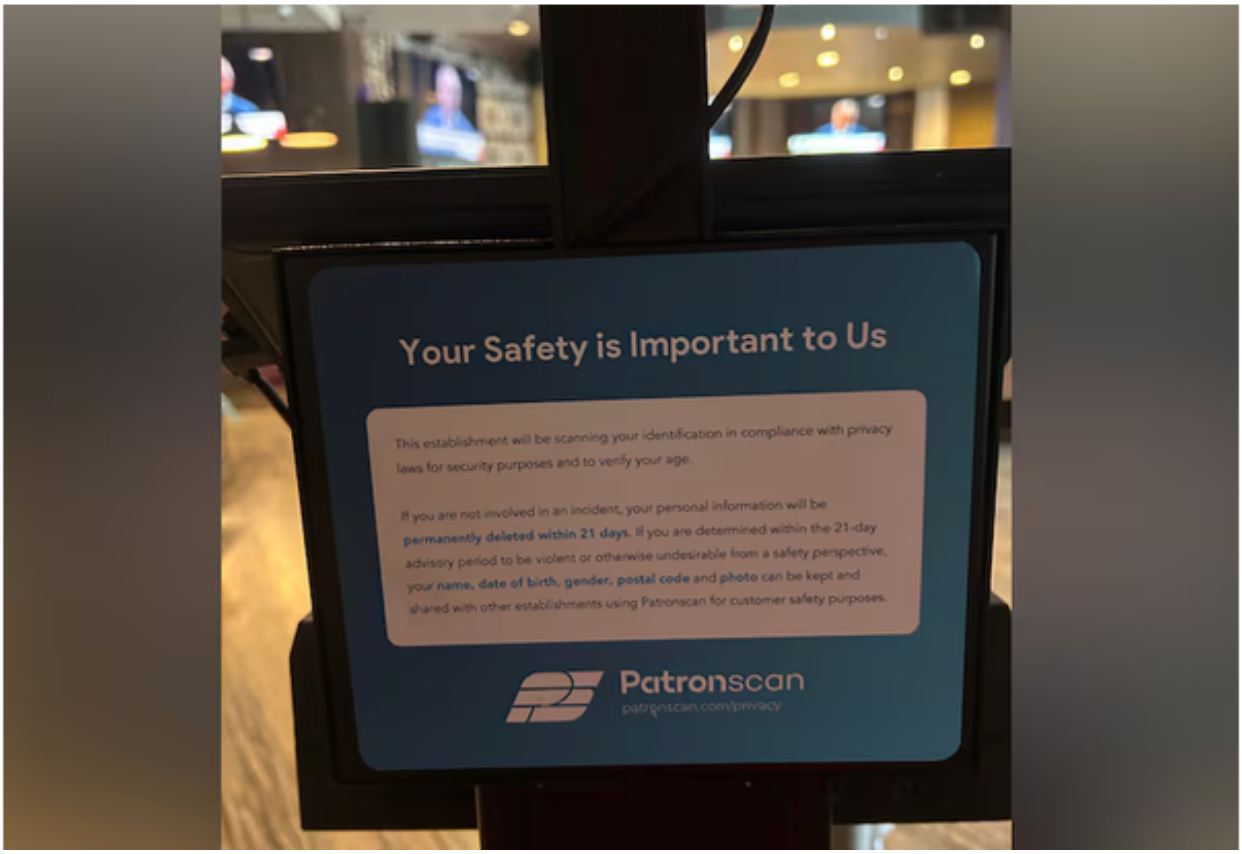
On August 24, 2026, a CBC article, "Woman flagged by ID scanner as nationwide 'public safety concern' after incident in Winnipeg bar" ("CBC article"), reported the experience of Alexandra, a Toronto-based lawyer, whose encounter with an ID scanning system at a Winnipeg bar resulted in her being flagged as a public safety concern at an unrelated establishment in Calgary.

On June 6, 2026, Alexandra visited Riverside bar in St. Vital, Winnipeg, where a security guard scanned her driver's license at the door using a Patronscan device. Alexandra maintains that she was not told why her ID was being scanned. Later that evening, feeling unwell, she went to the nearest restroom. She was subsequently asked to leave the bar and did so without incident.

On July 9, Alexandra attended at a Stampede function in Calgary but was denied entry after her ID was scanned using the same system. The person scanning told Alexandra that she had a "criminal record", which was not the case.

Alexandra subsequently learned that Patronscan had flagged her as a "public safety concern" with a "serious" severity rating. This was based on the allegation that she entered the men's bathroom and refused to leave. An incident at a bar in Winnipeg had thus resulted in Alexandra being identified as a serious public safety concern at an unrelated venue in Calgary, more than a month later.

The Patronscan sign in the Riverside bar is posted below (copied from the CBC article).



The sign says:

> Your Safety is Important to Us
>
> This establishment will be scanning your identification in compliance with privacy laws for security purposes and to verify your age.
>
> If you are not involved in an incident, your personal information will be **permanently deleted within 21 days** (emphasis in original). If you are determined within the 21-day advisory period to be violent or otherwise undesirable from a safety perspective, your **name, date of birth, gender, postal code** and **photo** (emphasis in original) can be kept and shared with other establishments using Patronscan for customer safety purposes."

Issue 1: Using Contract Law Principles, are Individuals Consenting to the Usage of their Personal Information by Patronscan?

Under *PIPA*, consent to the collection of personal information may be express or deemed, but is negated where an individual is misled by an organization (ss 7(1), 8(1), 8(2), and 10). The question is whether presenting a driver's license and entering a participating establishment constitutes

meaningful consent to Patronscan's subsequent collection, use, retention, and sharing of personal information across a network of establishments. Contract law principles may help illuminate this question, particularly where the individual has limited ability to negotiate or refuse the terms.

Consent to the collection of the information is a requirement under both *PIPA* and common law contract principles; any voluntary transaction requires parties' consent to the agreement, and that consent presumes that parties know its contents. Under contract law, finding consent does not mean requiring parties to be notified of every provision of an agreement, but they must have reasonable notice of the more onerous terms. And as noted in *Apps v Grouse Mountain Resorts Ltd*, 2020 BCCA 78 (CanLII), "the more onerous the exclusion clause the more explicit the notice must be" (at para 62).

In this case, the notice arguably needed to be prominent, given the nature of the information collected as well as the broad powers establishments acquire once an individual's license is scanned. The Patronscan system collects an individual's name, date of birth, gender, postal code and photo. Where an establishment determines that an individual meets the criteria for inclusion in the system, it appears that it may retain this information for an unspecified period of time and may share it with other establishments. The criteria governing these decisions also leave establishments with a considerable amount of discretion.

A customer may reasonably expect to be asked to leave if they cause trouble in a bar. It is less apparent that a customer would expect that causing trouble could result in the retention and sharing of personal information across a network of establishments, potentially affecting their access to other establishments in the future. The question, then, is whether the procedure at the door, or the sign itself, provides the type of notice necessary to satisfy the reasonable notice requirement? It seems unlikely.

First, the environment in which the sign is presented does not lend itself to the degree of attention necessary to understand the nature and consequences of the terms. People visit bars for social purposes, as opposed to circumstances in which they would ordinarily expect to be presented with contractual or privacy notices. There may be a lineup at the door, creating an expectation to move quickly through the entrance. Unlike an airport, where security procedures and signage signal that important information may need to be reviewed, a bar setting does not alert patrons to the significance of having their IDs scanned. At a minimum, these circumstances suggest that a bar would need to take steps to draw the sign to individuals' attention. Here, Alexandra said that the security guard did not explain why he was scanning her ID.

Second, the presentation of the sign itself does not draw attention to its most onerous terms. According to the CBC article, the sign was located at the entrance, "below eye level and posted under the machine that scans the identification". Additionally, the relevant information is not particularly prominent. The larger font at the top of the sign addresses safety, while the bold blue text concerns the information collected and its permanent deletion. The onerous provisions – those addressing the retention and sharing of the information– are neither bolded nor presented in larger font.

Taken together, the presentation of the sign and the manner in which its terms are displayed suggest that the bar did not provide reasonable notice of the onerous consequences of submitting to the Patronscan system, meaning it is not at all clear that patrons consented to the collection, retention, or use of their personal information.

Issue 2: Public policy

PIPA seeks to balance individuals' rights to control their personal information against organizations' rights to collect, use or disclose it for reasonable purposes (s 3). In *Clearview AI Inc v British Columbia (Information and Privacy Commissioner)*, 2026 BCCA 67 (CanLII), the Court of Appeal, in considering the equivalent statute in British Columbia, *Personal Information Protection Act*, SBC 2003, c 63, discussed that statute's reliance on consent in achieving that balance (at para 16). Assuming the organization's purpose for collecting the information is reasonable, the organization cannot collect any information beyond what is necessary to provide the product or service (s 7(1)).

Even if an organization's purposes are found to be reasonable under *PIPA*, the broader implications of that conclusion warrant consideration. When individual business practices are assessed in isolation, the cumulative effect of those practices may escape scrutiny. As more organizations make the provision of personal information a condition of accessing goods and services, individuals may become increasingly accustomed to surrendering information they would not otherwise share. Over time, this may shift the perceived boundary between what organizations may reasonably demand and what individuals should reasonably be expected to disclose.

Consider a restaurant that asks customers for their phone numbers while they wait to be seated, despite having no apparent need for the information to provide a table. A customer may comply because they may not realize that refusal is an option or because providing a number has become routine. Repeated across countless transactions, such practices may foster a collective acquiescence to the idea that access to ordinary goods and services requires the disclosure of personal information.

The concern is not simply that any one practice may be unreasonable, but that the cumulative effect of individually accepted practices may diminish individuals' expectations of privacy and their willingness to challenge further demands. Those changing expectations may, in turn, influence how the reasonableness of subsequent practices is understood and assessed, such that the prevalence of a practice comes to be accepted as evidence of its acceptability, rather than a reason to question it. Yet prevalence cannot itself establish that a practice is legally or normatively unobjectionable, particularly where it has become embedded in transactions that individuals cannot realistically avoid. In other words, the normalization of a practice can change the very standard against which reasonableness is judged. The reasonableness of an organization's practices should therefore be assessed by focusing not only on the circumstances of the individual transaction, but also the broader social and normative implications of practices that have become commonplace.

This post may be cited as: Jassmine Girgis, “The Intersection between Privacy Law and Contract Law: Consent and Public Policy Concerns in the Age of Patronscan” (3 November 2026), online: ABlawg, http://ablawg.ca/wp-content/uploads/2026/11/Blog_JG_Patronscan.pdf

To subscribe to ABlawg by email or RSS feed, please go to http://ablawg.ca

Follow us on Twitter @ABlawg