Privacy Jurisprudence Review

Fifth Edition
2026

OSLER

Table of contents

Editor's note

In an era marked by digital innovation and constant connectivity, personal information has never been more accessible and easily sourced. In this environment, Chief Privacy Officers (CPOs), in-house counsel and compliance professionals have become indispensable in managing increasingly complex matters involving privacy and data management. This report explores the latest developments in Canadian privacy law, highlighting notable judicial decisions and legal trends shaping privacy law in Canada. With a curated collection of case law and emerging topics, we aim to provide CPOs with the foundation necessary to manage evolving legal standards, technological advancements and business priorities.

Through expert commentary, we examine how organizations can ensure compliance and prepare to confront the challenges that come with developing technologies and changing regulatory landscapes.

Thought leadership initiatives on the AccessPrivacy by Osler platform bring together Osler's specialized Privacy Disputes team and National Privacy and Data Management practices. Collaboration draws on the unique perspectives of both groups providing integrated insights on privacy and data litigation issues. These include Data Litigation Roundtable events on the AccessPrivacy monthly call that complement the *Privacy Jurisprudence Review*, as well as workshops and roundtables discussing emerging trends in artificial intelligence and governance.

With profound expertise in litigation and privacy law, Osler can help organizations stay informed in the rapidly evolving privacy space.

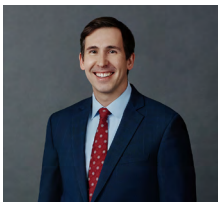
The authors wish to thank Tamara Kljakic, Victoria Luxford, Simone Penney, Clare Barrowman, Marie-Laure Saliah-Linteau and Josy-Ann Therrien for their contribution to this publication.

Commentary contributors

Kristian Brabander

Partner, Disputes

kbrabander@osler.com
514.904.8107



Robert Carson

Partner, Disputes

rcarson@osler.com
416.862.4235

Tommy Gelbman

Partner, Disputes

tgelbman@osler.com
403.260.7073

Jessica Harding

Partner, Disputes

jharding@osler.com
514.904.8128

Craig Lockwood

National Chair and Partner, Disputes

clockwood@osler.com
416.862.5988

Julien Morissette

Partner, Disputes and Insolvency & Restructuring

jmorissette@osler.com
514.904.5818

Privacy class action: data breaches

Tucci v. Peoples Trust Company, 2025 BCSC 816

Read the case details

Facts

This class action, certified in August 2017, arose from allegations that Peoples Trust Company (Peoples Trust) failed to implement adequate safeguards to protect sensitive customer information collected through its online application portal.

On this application, the plaintiff, Mr. Gianluca Tucci, applied to amend the certification order to add a new common issue: whether the members of the class in British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador were entitled to damages for breach of the privacy statutes of those respective provinces.

Mr. Tucci relied on the Court of Appeal decisions, *G.D. v. South Coast British Columbia Transportation Authority*, 2024 BCCA 252 *(G.D.)*, and *Campbell v. Capital One Financial Corporation*, 2024 BCCA 253 (*Campbell*), which held that intentional or reckless cybersecurity practices that facilitate a threat actor gaining access to a database could sustain a breach of privacy claim against a data custodian under the *Privacy Act*, R.S.B.C. 1996, c. 373 (B.C. *Privacy Act*).

Mr. Tucci argued that the holdings in *G.D.* and *Campbell* should apply by extension to similar privacy statutes in other jurisdictions.

Peoples Trust opposed the plaintiff's application on several grounds, including: the application was an abuse of process; there were no facts pleaded to support the claim; the limitation period had expired; Mr. Tucci had not amended the pleadings; the claim was foreclosed by a limitation of liability clause; there were too many individual issues; and the claim required interpretation of extra-provincial statutes.

Decision

The Court granted the plaintiff's application, amending the certification order to include the common issue of entitlement to damages without individual proof under provincial privacy statutes and creating a subclass for class members resident in the other class jurisdictions.

The Court found no abuse of process, holding that the decisions in *G.D.* and *Campbell* clarified the scope of liability under the B.C. *Privacy Act* for data custodians that are victims of cyberattacks by threat actors. The Court was satisfied that the pleadings, which had alleged that Peoples Trust was wilfully reckless in its handling of class members' personal information, were sufficient to ground a claim under the B.C. *Privacy Act* and the analogous privacy statutes in the other jurisdictions.

On the limitation period argument, the Court held that since the original pleadings established the facts for the statutory tort, the claim had been tolled. The Court rejected the *forum non conveniens* and lack of commonality arguments, noting that the earlier certification decision had allowed a Canada-wide class proceeding and that *Campbell* held British Columbia has jurisdiction to adjudicate all the statutory torts.

Key takeaways

The Supreme Court affirmed that jurisprudential developments that occur in the course of ongoing class proceedings can serve to broaden the scope of the proceeding, in this case, even post-certification. The decision leaves open the possibility that the timing of such an application might be precluded if there is prejudice to the defendants, but the threshold to amend a certification order remains low in B.C.

Harguindeguy c. Suncor Énergie inc. (Petro-Canada), 2025 QCCS 3072

Read the case details

Facts

The plaintiff, Esteben Harguindeguy (Harguindeguy), a participant in Petro-Canada's loyalty program known as "Petro-Points" (the program), sought the authorization to institute a class action on behalf of all individuals residing in Québec whose personal information, held by the defendants Suncor Énergie Inc. and Produits Suncor Énergie, S.E.N.C. (collectively, Petro-Canada), was compromised during a data breach that occurred on or around June 21, 2023.

This incident involved an unauthorized third-party gaining access to Petro-Canada's IT systems and extracting account holders' personal information, including names, email addresses, phone numbers, dates of birth, and in certain cases, credit cards or banking information. Petro-Canada publicly disclosed the incident on June 24, 2023, and provided further details on July 6, 2023, describing the exposed information as "basic contact information".

Harguindeguy alleged that Petro-Canada failed to adequately protect the personal information of program members, acted negligently in securing its IT systems and delayed notifying affected individuals about the breach. He also claimed that Petro-Canada failed to offer credit monitoring services and minimized the seriousness of the incident.

Harguindeguy's claims were based on several grounds, including contractual liability under the *Civil Code of Québec*, C.Q.L.R., c. CCQ-1991 (the CCQ), alleged violations of the *Act respecting the protection of personal information in the private sector*, C.Q.L.R., c. P-39.1 (the Québec Private Sector Act), false or misleading representations under the Québec *Consumer Protection Act*, C.Q.L.R., c. P-40.1 (the Québec CPA), and unlawful interference with the right to privacy under section 5 of the *Québec Charter of Human Rights and Freedoms*, C.Q.L.R., c. C-12 (the Québec Charter). In addition to compensatory damages, Harguindeguy sought an injunctive order compelling Petro-Canada to provide permanent credit monitoring and fraud protection services to class members.

Decision

The Superior Court of Québec authorized the class action for all damages-related claims but denied the injunctive relief sought.

On contractual liability, the Court concluded that allegations of negligence in protecting personal information, combined with unauthorized third-party acquisition of data, appeared sufficient even without specific allegations regarding the acts or omissions that enabled the data breach.

The Court also held that claims of false or misleading representations under section 219 of the Québec CPA appeared sufficient, noting Petro-Canada's communications appeared to downplay the severity of the incident and the existence of a non-functional telephone line.

On punitive damages, the Court found an appearance of right under section 49 of the Québec Charter, section 272 of the Québec CPA and section 93.1 of the Québec Private Sector Act.

However, the Court rejected Harguindeguy's request for permanent injunctive relief including ongoing credit and fraud monitoring service, as well as anti-tracking equipment for their electronic devices linked to the compromised data. The Court concluded that insufficient allegations prevented Harguindeguy from meeting the burden of proof required under section 509 of the *Code of Civil Procedure*, C.Q.L.R., c. C-25.01 (CCP).

Key takeaways

This decision confirms that in privacy class actions arising from data breaches, vague allegations of negligence combined with evidence of compromised data can satisfy the authorization criteria.

The decision also highlights the importance of prompt responses to privacy incidents. Under the Québec CPA, claims of false or misleading representations may arise if businesses are perceived as minimizing the severity of a data breach, fail to disclose the full extent of compromised data, or fail to provide adequate support to affected individuals.

While this case has not yet been decided on these merits, this decision serves as a reminder for businesses of the importance of implementing strong data protection measures, establishing comprehensive incident response plans, and prioritizing transparent and timely communication with stakeholders following such incidents.

Privacy class actions: expectation of privacy

Hvitved v. Home Depot of Canada Inc., 2026 BCCA 39

Read the case details

Facts

The plaintiff, Lasse Hvitved, alleged that Home Depot violated customers' privacy rights by collecting their email addresses and purchase information — ostensibly provided for the purpose of receiving electronic receipts — and disclosing this information to Meta Platforms Inc.

The plaintiff sought to certify four claims: breach of privacy legislation (British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador); intrusion upon seclusion; unjust enrichment; and breach of contract. The chambers judge certified the breach of privacy claim but struck the remaining three causes of action.

The plaintiff appealed the decision to strike the breach of contract claim only, and Home Depot cross-appealed certification of the breach of privacy claim.

Decision

The Court of Appeal dismissed both the appeal and the cross-appeal.

With respect to Home Depot's cross-appeal, the Court held:

- The contextual nature of a privacy inquiry under subsection 1(1) of the *Privacy Act*, R.S.B.C. 1996, c. 373 (the B.C. *Privacy Act*) does not preclude a finding of commonality where there is some basis in fact for a common experience among class members. The Court found that in this case, the chambers judge had identified a common experience among class members, namely the type of purchasing information collected, how it was collected and the use made of it.

- Non-Facebook users should not be excluded from the defined class. The Court found there was some basis in fact — on the face of the defendant's own pleadings and evidence — that Home Depot shared information about most, if not all, of the proposed class members, and the mere fact of a transfer of personal information constituted a potential breach.
- Corporations should not be excluded from the defined class. The Court agreed with the chambers judge that the question of whether a corporation can advance a claim under provincial privacy legislation in the absence of an express exclusion is best left for trial.

With respect to the plaintiff's appeal, the Court confirmed that the pleading did not include material facts, including with respect to the formation of the contract, the contract's form or scope, or specific contractual terms governing the collection, use, maintenance, protection and non-disclosure of personal information.

Key takeaways

This case demonstrates that B.C. courts are prepared to strike claims based on deficient pleadings, in this case, characterized as "boiler plate". A warning to plaintiffs, claims that are not properly pleaded appear less likely to withstand scrutiny. A caution to defendants, this decision affirms that a contextual inquiry under provincial privacy statutes does not rule out commonality if there is some factual basis for a shared experience among class members. The decision leaves open the question of whether corporations may advance claims under the B.C. *Privacy Act*.

Lam v. Flo Health Inc., 2025 BCSC 993

Read the case details

Facts

Having been partially successful in her initial certification application, in *Lam v. Flo Health Inc.*, 2024 BCSC 391, the plaintiff filed an amended pleading (the Amended FANOCC) and sought certification in respect of breach of express and implied contractual terms relating to the protection of personal information and breaches of the duty of good faith and honest performance.

The plaintiff alleges that the defendant, Flo Health Inc. (Flo), the company that operates the Flo Health & Period Tracker application (the App), intentionally disseminated highly sensitive personal information with which users had entrusted, including menstrual cycle dates, pregnancy status, and symptoms. To use the App, users had to consent to a standard-form agreement that incorporated Flo's terms of use and privacy policy (the Privacy Policy). The Privacy Policy had been amended 13 times during the class period.

Decision

The Court certified the additional causes of action, together with corresponding common issues, finding as follows:

- Lam adequately pleaded express and alternatively implied terms of the contract, relying on language in the Privacy Policy stating that personal information would "never be sold or rented out to third parties" as well as the presumed intentions of the parties that Flo would protect the personal information users input into the App as being necessary to give business efficacy to the contract. Lam also adequately pleaded breach of the duty of good faith and honest performance. Flo's argument that the Privacy Policy permitted some disclosure effectively asked the Court to interpret the Privacy Policy at the certification stage, which would not be appropriate in the absence of an evidentiary record.

- Lam's claim that Flo breached the contract by failing to obtain meaningful consent to the disclosure was not bound to fail. The Amended FANOCC alleged that the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (*PIPEDA*), as mandatory legislation, governs whether Flo obtained proper consent to its data-sharing practices. Lam's claim that any consent Flo argues they had to sharing of information was made without consent to the extent such consent was not compliant with *PIPEDA*, was novel but was not bound to fail.

- It was not plain and obvious the remedy of disgorgement could not succeed. Lam pleaded that Flo used class members' personal information for profit and to grow its business and revenues from targeted advertising. The Court accepted that class members may have a legitimate interest in preventing Flo from profiting from their personal information where they did not agree to its use in that manner.

- On commonality under paragraph 4(1)(c) of the *Class Proceedings Act*, R.S.B.C. 1996, c. 50 (the *CPA*), the 13 iterations of the Privacy Policy did not preclude common resolution. Material differences between the policies would merely give rise to subclasses, which is not a bar to certification under section 7 of the *CPA*.

Key takeaways

The threshold to amending pleadings, even post-certification, remains low in B.C. Breach of contract claims in privacy class actions can survive certification where the plaintiff pleads specific express or implied contractual terms with sufficient particularity, rather than relying on generic assertions. The availability of disgorgement as a remedy in privacy-related breach of contract claims remains a live issue, particularly where users did not pay a fee for the service and compensatory damages may be minimal, but where the defendant allegedly profited from the very conduct constituting the breach.

Nagar c. Desjardins sécurité financière, Compagnie d'assurance-vie, 2025 QCCS 2720

Read the case details

Facts

The plaintiffs, Arielle Nagar (Nagar) and Giovana Feth (Feth) (collectively, the Plaintiffs), students at Concordia University and McGill University, respectively, were automatically enrolled in a group insurance plan and unknowingly paid the associated premiums. They sought authorization to institute a class action on behalf of all students enrolled in a CÉGEP or university who were automatically enrolled in a health, medical or dental insurance plan, for which they paid premiums either directly to the defendants or for the defendants' benefit.

The proposed class action was brought against Desjardins Financial Security Life Insurance Company (the Insurer), *Alliance pour la santé étudiante au Québec inc.* (ASEQ), Concordia University (Concordia) and McGill University (McGill) (collectively, the Defendants).

In their application, the Plaintiffs raised five causes of action against the Defendants:

- the illegality of automatic enrollment without the class members' informed consent
- failure to adequately inform students of the insurance's optional nature and the opt-out mechanism
- abusive and arbitrary opt-out deadlines
- violations of the Québec *Consumer Protection Act*, C.Q.L.R., c. P-40.1 (the Québec CPA) and
- communication of the class members' personal information to the Insurer without consent, in violation of privacy rights

With regard to the privacy-related claim, the Plaintiffs alleged violations of section 5 of the *Act respecting the protection of personal information in the private sector*, C.Q.L.R., c. P-39.1 (the Québec Private Sector Act), asserting that the Defendants did not lawfully collect or communicate their personal information, and that class members never consented to its sharing with or between ASEQ and the Insurer. They also invoked that the Defendants' conduct breached class members' privacy rights under section 5 of the *Charter of Human Rights and Freedoms*, C.Q.L.R., c. C-12 (the Québec Charter).

Decision

The Superior Court of Québec authorized the class action and found that the Plaintiffs had arguable claims regarding the legality of automatic enrollment in group insurance, the adequacy of information provided about the opt-out right and related deadlines and the allegedly abusive nature of those deadlines. It also held that the Plaintiffs could invoke the Québec CPA against the universities under sections 228 and 230, alleging unsolicited insurance charges and inadequate disclosure on tuition invoices, and that ASEQ and the Insurer could plausibly be held extracontractually liable for their role in the automatic enrollment mechanism.

On the communication of class members' personal information to the Insurer, the Court found a *prima facie* appearance of right, noting that this claim was inherently linked to the legality of automatic enrollment and the extent of ASEQ's authority to act as a representative, even though the Plaintiffs did not allege specific damage resulting from the communication.

The Court also authorized the punitive damages claim under section 49 of the Québec Charter, finding that the Plaintiffs' allegations — including the Defendants' conduct regarding the class action and concerns raised by students — were sufficient in appearance to support the alleged intentional conduct.

On November 13, 2025, the Québec Court of Appeal granted leave to appeal the authorization judgment.

Key takeaways

This decision illustrates that a court may authorize a class action where the plaintiffs alleged that the communication of the class members' personal information to a third party, without the class members' prior consent, constitutes a violation of their privacy rights, even if the plaintiffs did not allege specific damage resulting from such communication.

It also highlights that businesses that collect and communicate personal information in the context of automatic enrollment or opt-out mechanisms, should ensure that informed consent is obtained before communicating personal information to third parties to limit litigation exposure.

Option Consommateurs c. Home Depot of Canada inc., 2026 QCCA 149

Read the case details

Facts

The appellant, Option Consommateurs, appealed a decision from the Superior Court of Québec partially authorizing a class action against Home Depot of Canada Inc. The dispute originated from the Home Depot's alleged communication of clients' personal information to Facebook and Meta Platforms Inc. (collectively, Meta).

During the relevant period, Home Depot collected clients' email addresses to send an electronic receipt for in-store and online purchases. The plaintiff alleges that Home Depot then communicated hashed versions of these email addresses, along with purchase details, to Meta.

On January 26, 2023, the Office of the Privacy Commissioner of Canada (OPC) published a report concluding that Home Depot had failed to obtain informed consent before disclosing client information.

The Superior Court authorized the class action solely for punitive damages under the *Charter of Human Rights and Freedoms*, C.Q.L.R., c. C-12 (the Québec Charter), denying authorization for compensatory damages on behalf of certain clients and individuals without a Facebook account. It also dismissed causes of action under the Québec *Consumer Protection Act*, C.Q.L.R., c. P-40.1 (the Québec CPA) and the *Competition Act*, R.S.C. 1985, c. C-34.

Decision

The Québec Court of Appeal partially granted the appeal.

On compensatory damages, the Court of Appeal held that the authorization judge erred in finding no demonstrated prejudice. It found that it was neither frivolous nor manifestly unfounded to argue that clients' personal information had a value, which could give rise to compensation. While acknowledging limited allegations concerning the value of the personal information, and that, at first glance, Home Depot may have agreed to provide it without monetary compensation, the Court of Appeal emphasized that, at the authorization stage, Option Consommateurs needed only to demonstrate a mere "possibility" of success on the merits — not a "realistic" or "reasonable" one.

With regard to clients who purchased online, the Court of Appeal held that the authorization judge exceeded its role by assessing the probative value of the evidence and ruling on the intentional nature of the privacy violation, a question belonging to the merits. Noting that Home Depot's privacy policy did not indicate that personal information could be shared with third parties for targeted advertising, the Court of Appeal expanded the class to include clients who purchased online. However, it upheld the exclusion of individuals without a Facebook account, as sharing a hashed email of such a person did not involve sharing personal information.

The Court of Appeal also found it unnecessary to address the Québec CPA claims, as compensatory and punitive damages claims were already defendable, reiterating that a single defensible claim on one legal basis suffices at the authorization stage. Nonetheless, it noted that the authorization judge erred in limiting sections 219 and 228 of the Québec CPA to the pre-contractual phase. The Court of Appeal also found that the authorization judge set an overly high threshold under the *Competition Act* and authorized claims against Home Depot for allegedly misleading customers about email use for commercial gain.

Key takeaway

This decision illustrates the low threshold for authorizing a privacy class action in Québec involving the alleged commercial use of personal information without consent. The Court of Appeal confirmed that it is arguable at the authorization stage that personal information communicated to third parties for commercial purposes has a monetary value, and that such claims should be left for the merits judge to decide. The decision also confirms that the authorization judge need only verify that at least one claim is arguable on one legal basis.

This decision further underscores that businesses sharing personal information with third parties for commercial purposes, including advertising measurement and targeted advertising, must obtain clear and informed consent, as vague or generic privacy policies may not meet that standard.

RateMDs Inc. v. Bleuler, 2025 BCCA 329

Read the case details

Facts

RateMDs.com hosts health professionals' profiles — including contact information, anonymous ratings, reviews and third-party comments — and ranks them in comparison to other professionals offering similar health care services. The site generates revenue through paid subscriptions and third-party advertising.

The plaintiff, Dr. Ramona Bleuler, a B.C. physician, commenced a putative class action alleging that the website RateMDs.com, operated by the appellants RateMDs Inc., VerticalScope Holdings Inc. and VerticalScope Inc., violated the *Privacy Act*, R.S.B.C. 1996, c. 373 (the B.C. *Privacy Act*). She alleged RateMDs.com violated both section 1 of the B.C. *Privacy Act* (violation of privacy) and subsection 3(2) (unauthorized use of name or portrait of another). The proposed class included all health professionals in British Columbia and other provinces with statutory privacy torts who had a profile on RateMDs.com.

Dr. Bleuler alleged she discovered a profile had been created for her on RateMDs.com without her authorization; it contained numerous reviews. She pleaded that: the appellants' conduct violated her rights to be left alone and to be free from unwanted publicity; and health professionals have an expectation that information they provided to regulators or patients would not be exploited by a for-profit company. The chambers judge certified the action as a class proceeding (with the exclusion of Québec residents), finding it was not plain and obvious that Dr. Bleuler's pleaded privacy claims could not succeed.

On appeal, the appellants challenged the judge's certification decision. The respondent filed a cross-appeal contesting the exclusion of Québec residents from the class.

Decision

The Court of Appeal allowed the appeal, setting aside the certification order and dismissing the action. The Court held that Dr. Bleuler's pleading did not disclose a cause of action for the privacy torts under the B.C. *Privacy Act*.

Regarding the claim for violation of privacy, the Court concluded that the plaintiff had not pleased material facts to establish that she had a reasonable expectation of privacy in respect of the information posted on RateMDs.com. The Court rejected Dr. Bleuler's argument that her claim was based on "privacy as control" — the right of an individual to determine when, how, and to what extent information about them is communicated. While acknowledging that the right to control the use of personal information is an aspect of the right to privacy, the Court held that this right arises only in respect of information that can properly give rise to a reasonable expectation of privacy.

Regarding the claim for unauthorized use of name, the Court held that it was plain and obvious the claim was bound to fail because there were no material facts pleaded to establish that the appellants had commercially exploited Dr. Bleuler's identity to promote sales. Applying the "sales versus subject" distinction from *Gould Estate v. Stoddart Publishing Co.* (1996), 30 O.R. (3d) 520 (Gen. Div.), the Court found that health professionals are the "subject" of their profiles on RateMDs.com, in the same way that a biographical subject is the focus of a biography. The website provides information of value to the public about health professionals who provide a public service and does not use the health professionals' names to commercially exploit their identities for the purpose of promoting sales.

Key takeaway

The right to control the use of personal information does not exist independently of a reasonable expectation of privacy in the underlying information. Professionals who offer services to the public cannot claim a reasonable expectation of privacy over publicly available information about their professional services simply because they do not wish to have that information compiled on a third-party website.

The decision clarifies that subsection 3(2) of the B.C. *Privacy Act* (unauthorized use of name or portrait of another) is not designed to capture any use of a plaintiff's name or portrait by a defendant who expects to profit from that use. Depictions that serve a public interest in providing information about a plaintiff falls outside the scope of subsection 3(2).

Donegani v. Facebook Inc., 2025 ONSC 6020

Read the case details

Facts

The plaintiffs alleged that Facebook shared user data with various third-party applications and device makers. The plaintiffs sought certification of a national class. The Court's decision followed the *third* certification hearing in this action. The Court had previously addressed the causes of action and common issues criteria in a December 2024 decision and directed the plaintiffs to propose a new class definition and to return for further argument on various criteria, including preferability.

Decision

The Court declined to certify the proceeding.

First, the proposed class definition was not workable. It was both over- and under-inclusive, and there was no evidentiary basis in the record that the underlying data would exist to construct the proposed Master Class List (an element of the plaintiffs' proposed approach for identifying proposed class members with claims).

Second, a class proceeding was not the preferable procedure. The Court found that certifying a proceeding where the only remedy sought was nominal damages would not advance access to justice, behaviour modification, or judicial economy. The Court added that regulatory proceedings are a preferable mechanism for pursuing behaviour modification.

The Court also found that nominal damages could not be certified as a common issue because determining liability for nominal damages required individualized inquiries into which class members' data had been shared.

Key takeaways

Ontario courts continue to find that a class proceeding seeking only nominal damages will typically not satisfy the preferable procedure criterion.

Trueman v. Rogers Communications Canada Inc., 2025 ONSC 5972

Read the case details

Facts

The plaintiff brought a proposed class action against Rogers Communications and Rogers Bank on behalf of approximately eight million customers in Ontario, Alberta and Québec. The plaintiff alleged that Rogers Communications assisted Rogers Bank in obtaining credit reports of Rogers Communications customers from Trans Union Canada Inc., a Canadian credit reporting agency, without those customers' knowledge or consent. Rogers Bank, a separate legal entity from Rogers Communications, then used the credit checks to decide whether to promote its credit cards to Rogers Communications customers. The plaintiff discovered the practice when reviewing his credit report and complained to Rogers. The plaintiff also filed a complaint with the Office of the Privacy Commissioner of Canada, which launched an investigation.

Decision

The Court certified the class action on the basis of four asserted causes of action: breach of contract, breach of confidence, the tort of intrusion upon seclusion, and breaches of the *Civil Code of Québec*, C.Q.L.R., c. CCQ-1991, and the Québec *Charter of Human Rights and Freedoms*, C.Q.L.R., c. C-12. Justice Leiper held that the Office of the Privacy Commissioner of Canada's complaint process did not represent a preferable alternative to a class proceeding, since the organization will not provide "substantive access to justice" to class members or address common law tort claims. Justice Leiper rejected the defendants' argument that no compensable harm existed because the credit checks did not impact the credit scores of Rogers Communications customers. Justice Leiper held that general damages are available for an injury to an intangible interest such as a privacy right and noted that "the right to control one's personal information is harmed by an intrusion whether there is any mental distress or upset, or even knowledge by the person concerned that the breach has taken place."

The Court dismissed the defendants' partial summary judgment motion seeking to enforce an exclusion clause in the Rogers Communications standard form consumer agreement that excluded certain categories of damages, including "breach of privacy" damages relating to its services "or any advertisements". Justice Leiper applied the test related to the application of exclusion clauses from *Tercon Contractors Ltd. v. British Columbia (Transportation and Highways)*, 2010 SCC 4, and found that the second and third elements of the test — related to the unconscionability and whether the clause should be unenforceable on public policy grounds — should be decided based on a complete record. Accordingly, he held that the case was not appropriate for summary judgment.

Key takeaways

This decision underscores that exclusion clauses in standard form agreements may face heightened scrutiny on grounds of unconscionability or public policy in cases where intentional statutory privacy violations are alleged. The court re-affirmed that the harm that can arise from the mere loss of control over personal information, even without tangible financial impact, is sufficient to ground a claim in a class action proceeding.

Badji c. Zenleads inc., 2026 QCCS 5

Read the case details

Facts

The plaintiff, Cheikhou Badji (Badji), sought authorization to institute a class action on behalf of all Québec residents whose personal information was held, collected, used, communicated or commercialized without their consent by the defendant Zenleads Inc. (Zenleads), the operator of Apollo.io, a business intelligence platform.

Badji claimed that his Apollo.io profile disclosed personal information (including his full name, employer, job title, contact information and full professional history), along with a link to his LinkedIn profile, without his consent. Badji further claimed that Zenleads deploys a network of contributors to access client relationship management systems, email inboxes and electronic calendars to collect third-party personal information without knowledge or consent, intercepts electronic communications, uses a Google Chrome extension to circumvent LinkedIn privacy settings and engages in algorithmic profiling.

Badji alleged violations of the *Act respecting the protection of personal information in the private sector*, C.Q.L.R., c. P-39.1 (the Québec Private Sector Act), the *Civil Code of Québec*, C.Q.L.R., c. CCQ-1991 (the CCQ), and the *Charter of Human Rights and Freedoms*, C.Q.L.R., c. C-12 (the Québec Charter).

Zenleads contested the authorization of the class action, arguing that Apollo.io is a "business-to-business" platform for the exchange of digitalized business cards derived from public sources, and that the "professional information" exception under the Québec Private Sector Act applied.

Decision

The Superior Court of Québec authorized the class action and held that the information collected about Badji constituted personal information within the meaning of the Québec Private Sector Act and the CCQ and rejected Zenleads' argument that the "professional information" exception applied. The Court further observed that Badji's profile on Apollo.io could include extensive personal details, including a cellphone number and full professional history, and noted Zenleads' admission that it did not obtain individual consent for profiles and that it profited commercially from this information.

The Court also found that disclosure of cellphone numbers and algorithmic profiling methods could plausibly violate privacy rights under the Québec Charter. However, the Court dismissed the claims based on professional secrecy as too hypothetical, and rejected reputation claims due to insufficient evidence of a personal violation.

The Court held that the allegations showed plausible harm from the commercial use of personal data, including loss of control and algorithmic profiling, warranting compensable damages. With respect to punitive damages, the Court concluded that the allegations were sufficient, noting that section 93.1 of the Québec Private Sector Act provides for punitive damages of at least $1,000 when unlawful and intentional violation causes prejudice.

Therefore, the Court authorized the class action regarding most of the claims for punitive and compensatory damages but dismissed certain claims under the Québec Charter.

The Québec Court of Appeal granted leave to appeal on March 6, 2026.

Key takeaways

This decision highlights the significant legal exposure associated with alleged unauthorized data collection, use and resale, particularly in an era where personal data is increasingly recognized as a valuable corporate asset.

Notably, the Court's refusal to apply the "professional information" exception under the Québec Private Sector Act in the context of this matter reflects a restrictive interpretation, which could be an indication that information traditionally categorized as professional in nature may be subject to privacy protections when used for purposes that extend beyond the original business context.

Use of biometric data and facial recognition technology

Société 13859380 Canada Inc., 1031833-S, May 20, 2025

Read the case details [PDF]

Facts

The *Commission d'accès à l'information* (the CAI) launched an investigation following a complaint regarding the use of a bidirectional video surveillance system installed in delivery vehicles by 13859380 Canada Inc. (the company), a wholesale distributor of pipes, valves and related products operating under the trade name Crane Supply.

The system captured images from both the interior and exterior of vehicles. Drivers were required to identify themselves by entering a personal identification code on their company-provided cellphone before operating a vehicle, thereby associating the recorded images with the specific driver.

The system also incorporated artificial intelligence (AI) functionalities designed to detect specific in-cabin events — including cellphone use while driving, failure to wear a seatbelt, smoking, potential collisions, tailgating, excessive idling and speeding — and generate daily incident reports shared with branch managers. These reports listed detected events and drivers involved but did not include video footage or images.

According to the company's internal policy, access to the recorded images was restricted to three senior managers. The company justified the data collection by stating that it was necessary to achieve certain objectives, namely: to ensure driver safety and property protection, to prevent and detect highway safety code infractions, to facilitate accident investigations and to improve driver training.

Decision

The CAI found that the company's data collection objectives outweighed the privacy harm to drivers but concluded that the company failed to implement sufficient measures to minimize the privacy intrusion.

In its reasons, the CAI confirmed that the *Act respecting the protection of personal information in the private sector*, C.Q.L.R., c. P-39.1 (the Québec Private Sector Act) applied to the company and that the images captured inside vehicle cabins constituted personal information. Under section 5 of the Québec Private Sector Act, the CAI determined that the company's objectives were real, legitimate and important, thereby satisfying the necessity requirement.

The CAI distinguished between vehicle types: for heavy vehicles, their inherent dangerous nature and a documented history of accidents substantiated the legitimacy of safety-related objectives; for pick-up trucks, the company failed to prove they were disproportionately involved in accidents, though the CAI acknowledged the inherent risk of driving on public roads, which is heightened in collisions involving pick-up trucks.

Despite agreeing with the stated objectives, the CAI concluded that the company had not taken sufficient reasonable steps to minimize the privacy intrusion. The CAI noted that the company did not adequately evaluate less intrusive alternatives; the system continued collecting images for 20 minutes after engine shutdown, including during driver breaks; and there were inconsistencies between the company's policy and its stated practices regarding access to and use of the collected images. The CAI ordered the company, within 90 days, to:

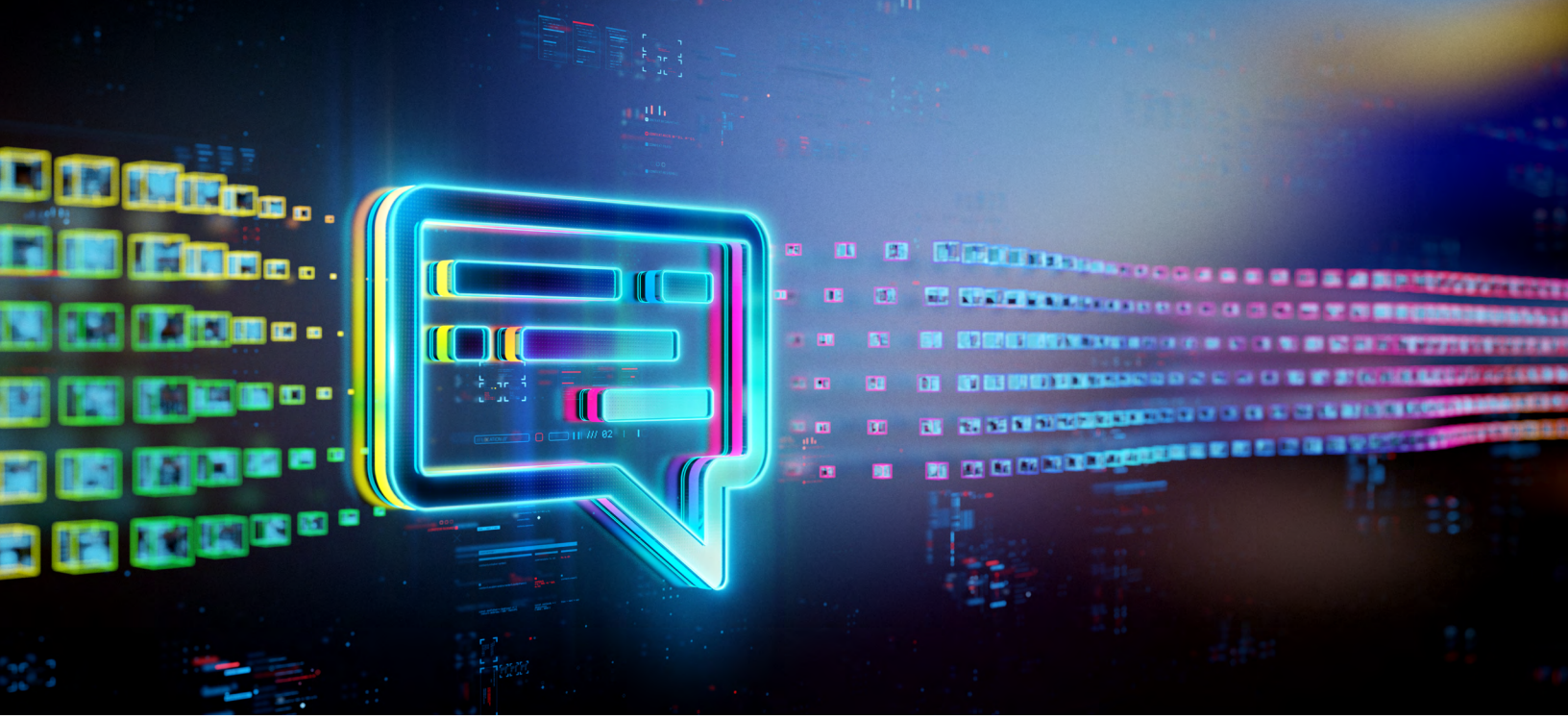
- limit interior cabin image collection to a limited number of seconds before and after a determined incident, or, cease collecting interior images entirely
- cease collecting interior images after engine shutdown and
- destroy any interior cabin recordings exceeding the sequence related to an accident or significant incident

The CAI also recommended that the Company revise its policy to restrict access to interior cabin images to cases of accidents or significant incidents.

Key takeaways

This decision provides important guidance to employers on the necessity requirement under the Québec Private Sector Act for video surveillance systems in commercial vehicles.

While the CAI recognized that safety-related objectives in the transportation context can be legitimate and may outweigh the resulting privacy intrusion, employers must take reasonable steps to minimize the collection of personal information, evaluate less intrusive alternatives, and ensure their policies clearly indicate and limit the circumstances in which recorded images may be accessed, used and by whom.



Privacy in procedural matters

Samoukovic c. Postmedia Network Inc., 2025 QCCS 4726

Read the case details

Facts

The plaintiff, Gordan Samoukovic (Samoukovic), a cardiothoracic surgeon described as a world-renowned expert, sued Postmedia Network Inc. (Postmedia), owner of the *National Post*, and reporter Ari David Blaff (Blaff) (collectively, the Defendants) for defamation and infringements to the *Charter of Human Rights and Freedoms*, C.Q.L.R., c. C-12 (the Québec Charter). Samoukovic claimed that an article published by the *National Post* on August 30, 2024 (the article) portrayed him as an antisemite in the context of the Hamas-Palestine-Israel dispute and sought moral and punitive damages, including for alleged violation of his privacy rights.

During pre-trial examinations, the Defendants sought various undertakings relating to Samoukovic's social media activity and private communications. Samoukovic had posted "stories" on his Instagram account — posts that disappear within a short period — some of which referred to the Hamas-Palestine-Israel dispute and were later reproduced in the article. His Instagram account had approximately 525 individually approved followers, and comments or "likes" on his stories were visible only to him.

Samoukovic raised objections spanning four categories, namely social media, private communications related to his professional life and third-party rights, private communications related to his personal life and third-party rights, and disproportion and fishing expedition. His objections were based on the legitimate expectation of privacy of third parties under section 5 of the Québec Charter and sections 35 and 36 of the *Civil Code of Québec*, C.Q.L.R., c. CCQ-1991 (the CCQ). The Defendants argued that no privilege prevented disclosure, that an account accessible to approximately 525 people could not be considered private, and that Samoukovic's own posts may have caused the harm he alleged.

Decision

The Superior Court of Québec rendered a nuanced decision, maintaining certain objections of Samoukovic's while dismissing others.

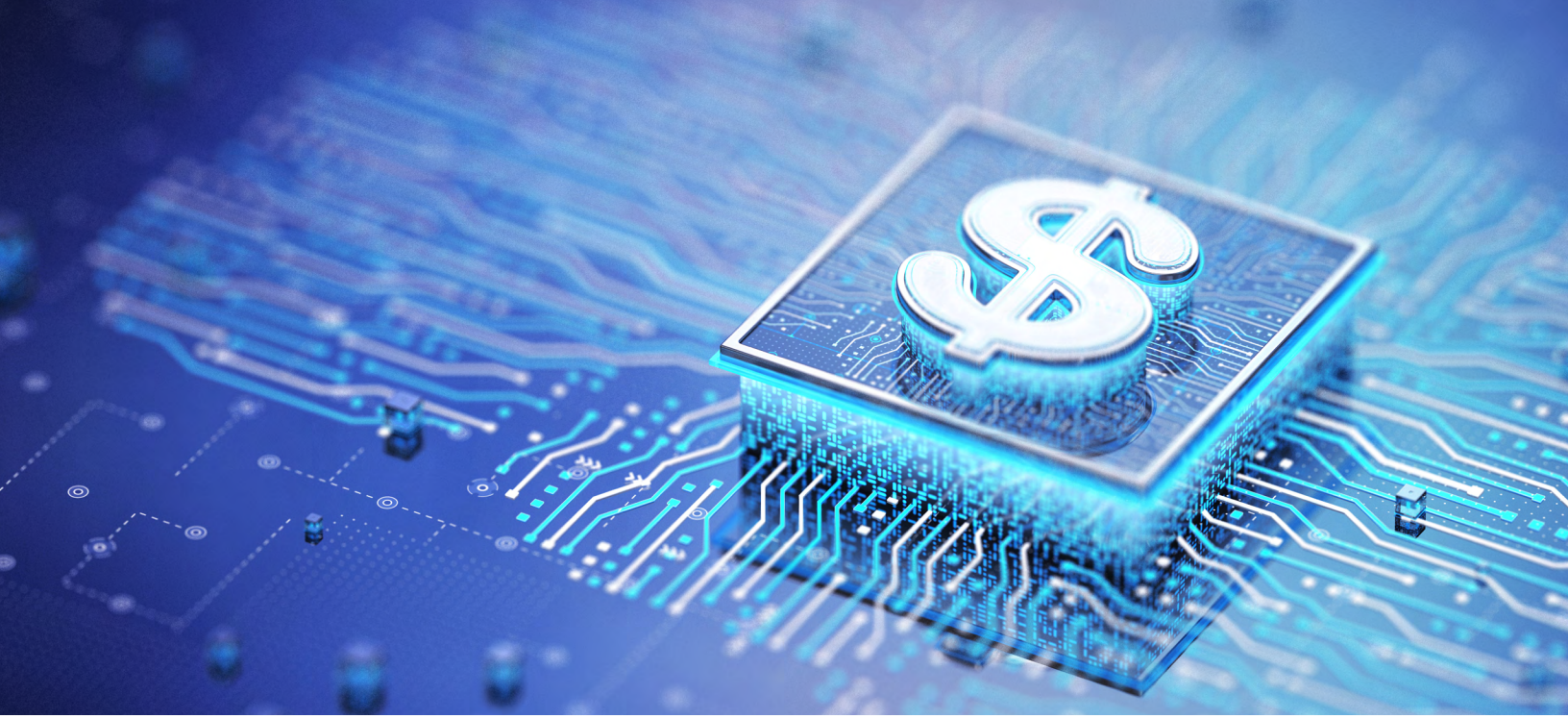
The Court first set out the legal principles governing pre-trial examinations under section 221 of the *Code of Civil Procedure*, C.Q.L.R., c. C-25.01 (the CCP), which allows examination on any fact relevant to the dispute. The Court noted that the right to privacy in Québec is grounded in section 5 of the Québec Charter and sections 35 and 36 of the CCQ. While the governing principle requires disclosure of all relevant information to the opposing party, courts must protect a party's right to privacy where applicable.

Regarding the requests for the names of Samoukovic's Instagram followers from the medical community, the Court maintained his objections, finding the undertaking carried "the unpleasant odour of a fishing expedition" with no logical connection to the issues in dispute. The Court concluded that the Wigmore criteria, as described by the Supreme Court of Canada in *R. v. National Post*, 2010 SCC 16, were met, and that section 36(6) of the CCQ further supported protecting those third parties' identities. The Court held that the right to privacy may constitute an exception to the principle of prior disclosure under section 228 of the CCP, and that it outweighed the Defendant's right to obtain further names. Similarly, the Court maintained the objection to requests for names of approximately 100 European medical professionals who allegedly became aware of the article, finding the undertaking abusive.

However, the Court dismissed objections to undertakings where names were not specifically requested, including requests for copies of Instagram story comments, written exchanges regarding the posts, and communications with colleagues about the article, reasoning that the absence of a specific request for names did not justify privacy-based objections. Finally, the Court held that all information through the examination on discovery was subject to the implied rule of confidentiality and shall not be disclosed without prior court authorization or the parties' informed consent.

Key takeaways

This decision provides guidance on the application of privacy protections during pre-trial examinations, particularly regarding social media activities. It affirms the fundamental nature of the right to privacy under the Québec Charter and the CCQ, which may constitute an exception to the principle of disclosure governing pre-trial examinations in Québec. While comments and communications on private social media accounts may be subject to disclosure, the identification of third parties who interacted with such posts may be protected.



Access requests

Canada (Attorney General) v. Canadian Civil Liberties Association, 2026 FCA 6

Read the case details

Facts

In February 2022, the Canadian federal government invoked the *Emergencies Act*, for the first time since it was enacted in 1988, in response to the Freedom Convoy protests and related blockades in downtown Ottawa and key international border crossings. The regulations stemming from the federal government's invocation of the *Emergencies Act* criminalized participation in, and financial support of, the protests. The order required banks, credit unions, insurance companies, crowdfunding platforms, and others to freeze the assets and accounts of "designated persons" engaged, directly or indirectly, in the protests. These institutions were also required to determine whether they were in possession of property owned, held, or controlled by or on behalf of a "designated person" and, if they were, to disclose to the RCMP or Canadian Security Intelligence Service (CSIS) prescribed information about the property. The accounts of about 257 "designated persons" were frozen pursuant to the order.

The Federal Court found that the reasons provided for the decision to declare a public order emergency did not satisfy the requirements of the *Emergencies Act*, and that certain measures adopted to deal with the protests infringed sections 8 and 2(b) of the *Canadian Charter of Rights and Freedoms* (*Charter*) (i.e., the right to be secure from unreasonable search and seizures, and the right to freedom of expression). The Federal Court found that the infringements were not justified under section 1 of the *Charter*.

Decision

The Federal Court of Appeal upheld the lower court's finding that the invocation of the *Emergencies Act* was unreasonable and *ultra vires*, and that the measures infringed constitutional rights to free expression and protection against unreasonable search and seizure. The Court found that the order's requirement for financial institutions and

other entities to report information to the RCMP or CSIS and permitted the federal government to disclose information to entities infringed section 8 of the *Charter* because there was no warrant requirement or prior authorization by a neutral arbiter. There was also no requirement that the "designated persons" receive any advance notice that their personal financial information would be shared with the RCMP or CSIS.

The Court found that banks, crowdfunding platforms, and other financial institutions were effectively deputized by the order and were required to turn account holders' personal financial information over to the RCMP or CSIS based on the relatively lax "reason to believe" standard. The Court held that individuals have a reasonable expectation of privacy in financial information, which forms part of the "biographical core of personal information," and the information-sharing provisions failed to provide adequate procedural safeguards.

On March 17, 2026, the federal government applied for leave to appeal to the Supreme Court of Canada.

Key takeaways

This decision is significant because it re-affirms that section 8 of the *Charter* protects individuals' privacy interests and confirms that governments cannot conscript financial institutions into warrantless surveillance of account holders without being in violation of section 8 of the *Charter*. It is also noteworthy insofar as the court affirmed a reasonable expectation of privacy in financial information as part of the "biographical core of personal information".

Hospital for Sick Children v. Ontario (Information and Privacy Commissioner), 2025 ONSC 5208

Read the case details

Facts

In 2022, both SickKids and the Halton Children's Aid Society (CAS) were targeted by ransomware attacks that temporarily encrypted their servers, rendering personal information inaccessible. Neither applicant found evidence that any personal information had been viewed, accessed, copied, or exfiltrated by the attackers. Both organizations notified the Information and Privacy Commissioner (IPC) of the attacks but took the position that the statutory requirement to notify affected individuals was not triggered. SickKids publicly disclosed the attack on its website but did not include a statement about individuals' entitlement to complain to the IPC. CAS did not provide any public disclosure. The IPC initiated reviews and concluded that both organizations had failed to comply with notification requirements under the *Personal Health Information Protection Act* (*PHIPA*) and the *Child, Youth and Family Services Act* (*CYSA*), respectively. The IPC determined that the ransomware attacks constituted both an unauthorized "use" and a "loss" of personal information, triggering mandatory notification obligations. SickKids sought judicial review and CAS appealed and sought judicial review of the respective IPC decisions.

Decision

The Divisional Court dismissed both judicial review applications and CAS' appeal. On the question of "use," the Court upheld the IPC's finding that the encryption of containers housing personal information amounted to "handling" or "dealing with" that information, even without direct access to individual files. The transformation of containers by encryption also transformed the personal information within them by making it unavailable to authorized users. The Court rejected the applicants' argument that direct interaction with the information was required to establish "use". On the question of "loss," the Court agreed with the IPC that the temporary inaccessibility of personal information due to a malicious unauthorized action constituted a "loss" within the meaning of the legislation. The availability of backup systems to restore information did not negate the fact that the information was temporarily lost.

The Court rejected the applicants' argument that the IPC engaged in "results-oriented reasoning," finding that the IPC appropriately considered the text, context and purpose of the statutory provisions. The Court also dismissed concerns about "over-notification" and "notification fatigue".

Key takeaways

The Court affirmed the IPC's broad interpretation of the terms "use" and "loss" in the context of ransomware attacks. Importantly, organizations cannot avoid notification obligations simply because attackers did not directly view or access individual files of personal information. The decision emphasizes that the notification requirement is not tied to risk of harm and instead ensures individuals' continuing interest in their personal information.

Ladouceur c. Desjardins assurances générales, 2026 QCCAI 30

Read the case details

Facts

In December 2018, major renovation work on a building adjacent to the building owned by the applicant, Steven Ladouceur (Ladouceur) resulted in the release of significant asbestos dust that infiltrated his building. Following the incident, Ladouceur submitted a claim (the Claim) to his insurer, Desjardins General Insurance (the Company), which was partially accepted.

Ladouceur submitted a request for the entirety of the Company's file regarding the Claim, including all documents, notes and communications. Four months later, the Company refused to provide the requested documents on the grounds that disclosure could impact imminent legal proceedings. Dissatisfied, Ladouceur filed an application under section 42 of the *Act respecting the protection of personal information in the private sector*, C.Q.L.R., c. P-39.1 (the Québec Private Sector Act) before the *Commission d'accès à l'information* (the CAI).

Ladouceur later submitted a second request for the same documents, which the Company again refused on identical grounds, prompting a second application. The CAI decided to hear both applications jointly.

Ahead of the CAI hearing, the Company provided documents to Ladouceur but raised new refusal grounds: litigation privilege and third-party personal information protection. After the CAI's intervention at the hearing, additional documents were shared with Ladouceur. However, Ladouceur set forth an argument that the Company's search was incomplete and insufficient, citing excluded sources, missing documents, and lack of independent confirmation. Separately, Ladouceur initiated Superior Court proceedings, seeking the same documents during out-of-court examinations.

Decision

The CAI had to determine whether the Company had conducted serious and thorough searches to identify all documents covered by the access requests.

At the hearing before the CAI, the Company's Senior Compliance Advisor, Ms. Blais, testified that she processed Ladouceur's access requests and consulted all three systems containing relevant information: two computerized platforms used for claims management and damage assessment, and a call recording platform. She confirmed that all data pertaining to the Claim was extracted, including correspondence between the claims adjuster, Ladouceur, and third parties, photographs taken by third parties, and all relevant calls recordings identified using telephone numbers from Ladouceur's file.

The CAI found that the Company presented compelling evidence that it had identified all relevant documents, placing the burden on Ladouceur to submit concrete and compelling evidence constituting *prima facie* proof of the existence of additional documents.

Ladouceur argued that the Company did not thoroughly explain its research methodology. However, Ms. Blais' testimony clearly identified the steps taken. The CAI concluded that the lack of keyword research did not constitute *prima facie* evidence of insufficient efforts.

Ladouceur further argued that correspondence between the claims adjuster and Company representatives were missing. Although the CAI noted that Ms. Blais could neither access the employees' email inboxes nor their Microsoft Teams platform, the evidence demonstrated sufficient efforts to identify all relevant email correspondence. Regarding a missing call recording from November 1, 2021, the Company demonstrated that such calls between external experts and building appraisers are never recorded. Finally, Ladouceur argued the Company failed to locate documents explaining inconsistencies in expert reports, but the CAI noted that the relevant

information was contained in email correspondence and notes confidentially submitted to the CAI, still in dispute due to interlocutory objections on privilege.

The CAI concluded that the evidence submitted by Ladouceur was insufficient to establish incomplete searches by the Company. The remaining disputed documents, including the Company's objection based on litigation privilege, will be adjudicated by the CAI on the merits.

With respect to the Company's arguments relating to litigation privilege, the CAI agreed to suspend part of the file to allow the Superior Court to rule on the Company's objections on privilege and requested that the parties keep it informed of all developments in the judicial proceedings, as the issue will be decided by the CAI on the merits at a later date.

Key takeaways

This decision clarifies the standard for assessing whether a company conducted a serious and complete search to locate all documents covered by an access to information request under the Québec Private Sector Act. Once a company satisfies its burden of proof, the applicant must present concrete elements constituting a commencement of proof that not all requested documents were located.

This decision also confirms that the absence of keyword searches does not necessarily constitute an incomplete search, particularly when all relevant documents have been extracted from the company's platforms. Finally, while the individual responsible for processing access requests should ideally be able to access all locations that may contain relevant information, the inability to do so is not fatal where prior searches have sufficiently identified the requested documents.

Premier Tech Eau et Environnement c. Investissement Québec, 2025 QCCQ 3063

Read the case details

Facts

The appellant, Premier Tech Eau et Environnement inc., a manufacturer of wastewater treatment systems, appealed a decision of the *Commission d'accès à l'information* (the CAI), refusing access to certain documents (the documents) held by Investissement Québec (IQ) relating to its principal competitor, Technologies Bionest inc., the only other developer of such systems in Québec.

The documents were generated following inspections by the *Bureau des normes du Québec* (the BNQ, currently called the *Bureau de normalisation du Québec*), an administrative unit of IQ responsible for certifying wastewater treatment systems, over approximately 15 years. They included effluent sampling results and communications regarding non-conformities identified during inspections.

IQ refused access relying on section 23 of the *Act respecting Access to documents held by public bodies and the Protection of personal information*, C.Q.L.R., c. A-2.1 (the Québec Access Act), which prohibits disclosure of a third party's trade secret. The CAI dismissed Premier Tech's application, finding that disclosure would reveal Bionest's trade secret regarding the efficiency and evolution of its wastewater treatment process, and that a competitor could use the data to reproduce Bionest's technology through reverse engineering.

Premier Tech appealed the CAI's decision before the Court of Québec, raising three questions: whether the CAI correctly interpreted the notion of "trade secret" under section 23 of the Québec Access Act; whether the CAI committed errors of law or palpable and overriding errors of fact in applying section 23 to the documents; and whether the quantity of documents was itself information protected as a trade secret.

Decision

The Court dismissed the appeal. It held that the CAI had correctly identified and applied the four criteria established by the Supreme Court of Canada in *Merck Frosst Canada Ltd. v. Canada (Health)*, 2012 SCC 3, used to determine whether information constitutes a trade secret:

1. The information must be secret in an absolute or relative sense.
2. The holder must have acted with the intention of treating the information as secret.
3. The information must have a practical application in the industrial or commercial sector.
4. The holder must have an interest worthy of legal protection.

The Court confirmed that the burden of proving the existence of a trade secret rests on the third party claiming protection, not the public body. The Court upheld the CAI's findings that the documents constituted a trade secret, as they revealed the evolution and performance of Bionest's technology over time and had been consistently treated as confidential by the BNQ. The Court also rejected Premier Tech's argument that the CAI should have described Bionest's trade secret in its reasons, noting that doing so would have defeated the very purpose of the protection.

A judicial review of the decision was filed on August 21, 2025, and a judgment has yet to be rendered.

Key takeaways

This decision reinforces the narrow scope of the right to appeal CAI decisions to the Court of Québec under sections 146 and 147 of the Québec Access Act. A party that disagrees with the CAI's application of the established legal criteria to the evidence cannot recast its challenge as a question of statutory interpretation to access appellate review. The appeal process is not an opportunity for a fresh assessment of the evidence.

The decision also provides useful guidance on the trade secret exception under section 23 of the Québec Access Act, confirming that the cumulative effect of otherwise individually unremarkable data may constitute a trade secret where, taken together, it reveals the evolution and performance of a competitor's technology and could enable reverse engineering. This has practical implications for businesses whose proprietary processes are subject to regulatory inspections, as the resulting inspection data may benefit from trade secret protection even when held by a public body.

Statutory privacy and reasonable expectation of privacy

Moon v. International Alliance of Theatrical Stage Employees (Local 891), 2025 BCSC 2238

Read the case details

Facts

The plaintiff, Kelly Moon, held an elected, paid position with Local 891 of the International Alliance of Theatrical Stage Employees (Local 891). Ms. Moon was the subject of an audit report, which found she used her company credit card for personal expenses. All personal expenses were repaid and there was no suggestion that Ms. Moon misappropriated Local 891 funds.

The Local 891 Executive Board released the Audit Report on Local 891's internal website in January 2019, where it was available to all members for approximately one week. A draft of the Audit Report was also illicitly leaked to various members before its official release. Ms. Moon lost her bid for re-election with Local 891, which she attributed to the disclosure of the Audit Report.

Ms. Moon brought a complaint to the Office of the Information and Privacy Commissioner (the Privacy Commissioner) under the *Personal Information Protection Act*, S.B.C. 2003, c. 63 (*PIPA*). The Privacy Commissioner upheld the legitimacy and lawfulness of the disclosure but found that: the unnecessary inclusion of specific transactions in the Audit Report violated *PIPA*; and Local 891 failed to take adequate security measures to prevent unauthorized leaks.

Ms. Moon brought an application seeking damages against Local 891 and several individual defendants who were members of the Executive Board, alleging breach of contract, violation of section 1 of the *Privacy Act*, R.S.B.C. 1996, c. 373 (the B.C. *Privacy Act*), the common law tort of public disclosure of private fact, negligence, conspiracy and a claim under section 57 of *PIPA*. The defendants applied for summary trial.

Decision

The Court found the matter was appropriate for summary trial and dismissed all of Ms. Moon's claims, except as against a John Doe defendant.

On the breach of contract claim, the Court found the Executive Board did not breach the duty of good faith by releasing the Audit Report, finding that the Executive Board had a legitimate purpose in informing its membership about its officer's financial transactions using company credit cards.

On the breach of privacy claim under the B.C. *Privacy Act*, the Court found that while the release of specific transactions in the Audit Report violated Ms. Moon's objectively reasonable expectation of privacy, the breach was not "wilful" within the meaning of section 1 of the B.C. *Privacy Act*. Local 891 had obtained legal advice that releasing the detailed transactions was permissible under *PIPA*. Reliance on a legal opinion, even if incorrect, negates the suggestion of recklessness. The Court also held that unions are not vicariously liable for the actions of their members, and therefore the leak of the draft report by a member did not give rise to liability for the defendants.

The Court declined to recognize a new common law tort of public disclosure of private fact in British Columbia. The Court found that alternative remedies exist in the form of the B.C. *Privacy Act* and *PIPA*, and that creating a new nominate tort without the legislative limits of those statutory schemes would work an indeterminate and substantial change to the legal system. The Court concluded by deferring to the legislature to govern privacy matters: "In my view, it would be irresponsible of me to try to craft a cause of action for the protection of privacy without either political debate or expert assistance."

On the negligence claim, the Court found that although Local 891 owed Ms. Moon a duty of care to protect her personal information, Local 891 had obtained legal advice about whether it could disclose the transactions consistent with *PIPA* and acted within the scope of that advice. Local 891 was therefore not negligent.

On the conspiracy claim, the Court found no evidence that the Executive Board was motivated by anything other than wanting to promote transparency. Even if the Board were motivated by political opposition to Ms. Moon's re-election, it is not tortious to try to accomplish this by lawful means.

On the *PIPA* claim, the Court found that Ms. Moon had not established "actual harm" within the meaning of section 57 of *PIPA*. The *PIPA* violations did not cause Ms. Moon to lose the election. The Court considered the term "actual harm" ostensibly for the first time, concluding that the standard for "actual harm" is high and must be caused by a wilful or reckless breach of privacy. While her psychological distress was real, it was not attributable to the *PIPA* violations and was insufficient to meet the standard of "actual harm".

Key takeaways

This case decides previously unsettled law with regard to whether a common law privacy tort for public disclosure of private fact exists in British Columbia. In doing so, the Court has further limited the scope of relief available for breach of privacy to the B.C. *Privacy Act* and *PIPA*.

Application of privacy legislation to foreign corporations

Clearview AI Inc. v. British Columbia (Information and Privacy Commissioner), 2026 BCCA 67

Read the case details

Facts

This was an appeal of a judicial review application concerning the application of British Columbia's *Personal Information Protection Act*, S.B.C. 2003, c. 63 (*PIPA*) to Clearview AI Inc. (Clearview), a private U.S.-based technology company that sells facial recognition software, primarily marketing these services to law enforcement and other government agencies. Clearview's search engine detects and scans human faces and associated metadata from publicly accessible websites and analyzes each face to produce a numerical biometric identifier. All facial images, associated metadata and biometric identifiers are stored indefinitely on Clearview's servers.

In early 2020, the information and privacy commissioners of British Columbia, Alberta, Québec and Canada commenced a joint investigation into Clearview's activities. The resulting joint report (the joint report), issued in February 2021, concluded that Clearview had violated protection of privacy laws in all four jurisdictions. In December 2021, the British Columbia Information and Privacy Commissioner (the Commissioner) issued a decision finding Clearview had contravened sections 6–8, 11, 14 and 17, of *PIPA*. The Commissioner ordered Clearview to: cease offering its facial recognition services to clients in British Columbia; make best efforts to cease the collection, use and disclosure of images and biometric facial arrays collected from individuals in British Columbia without their consent; and make best efforts to delete such data in its possession (the Order).

Clearview applied for judicial review, which was dismissed by the chambers judge in December 2024. Clearview appealed on three grounds: *PIPA* does not apply to it as a matter of constitutional law; the Commissioner unreasonably interpreted and applied *PIPA* in concluding that the "publicly available" exception did not apply and that Clearview did not have a reasonable purpose for its activities; and the Order was unnecessary, unenforceable or overbroad. Similar judicial review applications were initiated in Alberta and Québec.

Decision

The Court of Appeal dismissed Clearview's appeal, holding that *PIPA* is constitutionally applicable to Clearview. Key findings include:

- *PIPA* constitutionally applies to Clearview because there is real and substantial connection between its online business activities and British Columbia. Even after Clearview ceased marketing activities in British Columbia, its global image crawler continued to collect facial data from individuals in British Columbia, maintaining a sufficient connection to British Columbia for the purposes of the application of *PIPA*. Following a detailed review of the related jurisprudence, the Court concluded that technological advances have led to a proliferation of companies whose business model is based on acquiring information from global internet sites, such that the physical location is of significantly diminished importance to the real and substantial connection analysis, whether that of content providers, servers or end users. In this case, Clearview's business model depends on acquiring facial data globally.

- The Court upheld the Commissioner's conclusion that images obtained from social media websites are not "publications" under the "publicly available" exemption (in contrast to traditional publications like books or newspapers).

- Clearview's collection of facial data was not for purposes a reasonable person would consider appropriate in the circumstances. The joint report found that information Clearview collects to be "extremely sensitive", and the Court agreed that Clearview's purpose was accurately characterized as providing a commercial service to law enforcement and others, but its purpose is not law enforcement and not what those who posted their images intended.

- The Order was reasonable and enforceable. The prohibition on offering services in British Columbia was justified despite Clearview's claimed withdrawal from the Canadian market. An entity ceasing operations in a jurisdiction does not deprive a regulator of its authority to issue orders, including prospective ones, based on the entity's conduct while it operated within that jurisdiction. The Court also upheld the terms requiring Clearview to make "best efforts" to cease collecting and delete facial data, rejecting claims of vagueness. It noted that "best efforts" orders are commonly used to address noncompliance with privacy laws and provide necessary flexibility for enforcement.

Key takeaways

This decision finds that provincial privacy legislation can apply to foreign corporations that acquire personal information of individuals in the province through internet-based activities, even where the corporation has ceased marketing its services in the jurisdiction, provided there is a real and substantial connection between the corporation's activities and the province. This will likely embolden regulators seeking jurisdiction over online businesses with no physical presence in Canada. The decision arguably narrows the interpretation of the "publicly available" exemption under *PIPA*, thereby limiting the type of content that would fit within the exemption.

About Osler, Hoskin & Harcourt LLP

Osler is a leading law firm with a singular focus – your business. From Toronto, Montréal, Calgary, Vancouver, Ottawa and New York, we advise our Canadian, U.S. and international clients on an array of domestic and cross-border legal issues. Our collaborative "one firm" approach draws on the expertise of over 600 lawyers to provide responsive, proactive and practical legal solutions driven by your business needs. For more than 160 years, we've built a reputation for solving problems, removing obstacles, and providing the answers you need, when you need them.

Osler, Hoskin & Harcourt LLP
Toronto Montréal Calgary Vancouver Ottawa New York | **osler.com**

OSLER