Privacy Jurisprudence Review

Fourth Edition – Summer 2025

OSLER

Table of contents

Editor's note

In today's digital era, where personal data flows with unprecedented speed and volume, the role of Chief Privacy Officers (CPOs), in-house counsel, and compliance professionals has never been more critical — or more complex. This publication aims to provide an analysis of the latest developments in Canadian privacy law, offering valuable insights into the judicial decisions and legal trends shaping privacy law in Canada. By examining key case law and emerging issues, our goal is to equip CPOs with the strategic foresight and expertise necessary to navigate the evolving intersection of legal standards, technological innovation, and business priorities.

Through expert commentary, we explore how organizations can achieve compliance and proactively address the challenges posed by rapidly advancing technologies and shifting regulatory landscapes.

Osler's specialized Privacy Disputes team and National Privacy and Data Management practices regularly collaborate on thought leadership initiatives on the AccessPrivacy by Osler platform to provide integrated insights on privacy and data litigation issues that draw from the expertise of both groups. These include the widely attended 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 AI and governance.

By combining deep expertise in litigation and privacy law with a forward-looking approach to technology and governance, Osler remains a trusted partner for organizations striving to stay ahead in the rapidly evolving privacy landscape.

The authors wish to thank Tamara Kljakic, Andrea Korajlija, Brodie Noga, Marie-Laure Saliah-Linteau and Josy-Ann Therrien for their valuable 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

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

Royer c. Capital One Bank (Canada Branch) et al., 2025 QCCA 217

Read the case details

Facts

A security breach allowed a former employee to illegally access the confidential credit card application data of approximately 100 million Americans and 6 million Canadians collected over a 14-year period by the respondents Capital One Bank et al. (Capital One) and hosted on servers of the respondents Amazon Web Services Inc. et al. (Amazon). When informed of the security breach, the appellant, Michael Royer (Royer), sought the authorization to institute a class action.

The authorization (first instance) judge concluded that there was sufficient evidence of contractual fault on the part of Capital One, notably for failing to adequately protect personal information, for unreasonable delay in discovering the leak and informing its customers, and for keeping the data of certain individuals for an unreasonable length of time, particularly those whose credit card applications had been refused.

The authorization judge also concluded that there was sufficient evidence of civil liability on the part of Amazon, notably on the basis of sections 3 and 10 of the *Act respecting the protection of personal information in the private sector*, C.Q.L.R. c. P-39.1.

The authorization judge noted the absence of any allegations of identity theft and dismissed most of the proposed damages claims relating to value of the leaked data and to harm caused by the delay in notifying class members. However, he held that the credit monitoring required as a result of the breach constitutes a compensable harm and the sufficiency of such credit monitoring already offered by Capital One (2 years) was a question for the trial judge. The judge also held that there were sufficient

allegations to allow a claim for punitive damages to proceed as against Capital One, but not as against Amazon.

All parties appealed. Royer criticized the authorization judge for having excluded other damages claims from the class action (the Principal Appeal). Capital One and Amazon argued that the authorization judge should not have allowed claims for damages that the class representative himself did not incur (the Incidental Appeal). Capital one also challenged the authorization of the claim for punitive damages.

Decision

The Québec Court of Appeal allowed the Principal Appeal and dismissed the Incidental Appeal.

The Court held that the class representative's personal case does not need to be a typical example of that of all or a majority of the class members, but must rather demonstrate that they have suffered at least one head of damages. The authorization must not be limited and may cover damages potentially suffered by at least one member of the class.

Moreover, the Court stated that harms suffered by class members as a result of the breach are not necessarily all identical. Some members of the class may have paid credit monitoring costs, while others may have taken other steps and incurred other costs for the same purpose.

Finally, the Court held that it is not necessary to determine, at the authorization stage, the existence of compensable non-pecuniary losses. As long as there are allegations that sufficiently establish the possibility of wrongful infringement leading to compensable consequences, it is up to the trial judge to decide these. The Court therefore authorized the class action for all heads of compensatory damages.

As for punitive damages, the Court held that there were no grounds for review in appeal.

Key takeaway

This decision reinforces the relatively low bar for authorizing class actions in Québec, particularly in cases involving privacy breaches. While the class representative may not have suffered all heads of damages, the class action may include other damages potentially suffered by at least one class member. Although different class members may have experienced different types of losses, these variations do not preclude the authorization of a class action.

This decision also highlights the reality that the threat of financial harm following certain types of data breach can sometimes be sufficient to ground a class action in Québec, even where some form of credit monitoring is offered by the defendant.

InvestorCOM Inc. v. L'Anton, 2025 BCCA 40

Read the case details

Facts

This action relates to an alleged data breach involving data stored on servers operated by InvestorCOM Inc. A proposed class action was filed in British Columbia. A parallel proposed class action had already been commenced in Ontario by different plaintiffs and counsel, seeking certification of a national class action in respect of the same subject matter. The Ontario action was proceeding to a certification hearing.

InvestorCOM and Mackenzie Financial Corporation applied to dismiss the B.C. action for abuse of process, arguing that the existence of the Ontario action rendered the BC proceeding duplicative and unnecessary. The chambers judge dismissed the application. InvestorCOM and Mackenzie appealed.

Decision

The Court of Appeal dismissed the appeals, holding that the mere existence of similar or parallel class actions in different provinces does not, without more, amount to an abuse of process. However, that does not mean that the B.C. action will be allowed to proceed. The Court of Appeal emphasized that duplication concerns are properly addressed at the certification stage under paragraph 4.1(1)(b) of the B.C. *Class Proceedings Act*, with the benefit of a complete certification record. That provision allows the court to refuse certification if it is preferable for the proceeding to be conducted in another jurisdiction.

The Court distinguished this case from situations where a placeholder action is commenced solely as a procedural tactic. The Court also recognized that differences in provincial law, the costs regime, and the plaintiff's residence provided reasons for pursuing the action in B.C.

Key takeaway

It is common for class actions to be started in multiple provinces after a data breach. In B.C., the courts appear to prefer to address the overlap as part of the certification motion. This will typically increase the time and cost required to address the overlap.

Hvitved v. Home Depot of Canada Inc., 2025 BCSC 18

Read the case details

Facts

In his application to certify a proposed class proceeding, the plaintiff alleged that Home Depot violated the privacy rights of customers by collecting their email addresses and purchase information — provided for the purpose of receiving electronic receipts — and disclosing this information to Meta Platforms.

The plaintiff advanced claims under provincial privacy statutes (British Columbia, Saskatchewan, Newfoundland and Labrador, and Manitoba), as well as claims for intrusion upon seclusion, breach of contract, and unjust enrichment. Home Depot opposed certification, arguing that the claims lacked merit and that a class proceeding was not appropriate.

Decision

The Court certified the class action solely in respect of the statutory claims, and struck the claims for intrusion upon seclusion, breach of contract, and unjust enrichment.

Key findings included:

- **Breach of privacy legislation:** The plaintiff's statutory claim was sufficiently pleaded to establish a cause of action for certification purposes. The Court rejected Home Depot's argument that there was no reasonable expectation of privacy in the data shared, relying on *Insurance Corporation of British Columbia v. Ari*, 2023 BCCA 331 to emphasize that privacy must be assessed contextually and not on a piecemeal basis.
- **Intrusion upon seclusion:** The Court held that the pleadings did not meet the higher threshold required for the common law tort of intrusion upon seclusion, as the information shared was less sensitive than that considered in analogous Ontario cases and did not amount to a highly offensive intrusion. In applying the Ontario law, the Court determined that the tort of inclusion upon seclusion has not been made out on the pleadings. The Court declined to adjudicate the question of whether the tort is available in British Columbia.
- **Breach of contract and unjust enrichment:** The Court found the pleadings to be deficient, noting the absence of material facts regarding the existence of express contractual terms, and insufficient allegations to support a claim for unjust enrichment, particularly regarding lost opportunity to sell personal information.

Key takeaway

This decision imposed discipline on the plaintiff's counsel to focus and properly plead causes of action relating to alleged privacy violations, with an apparent preference for statutory claims, which appear more likely to survive certification applications. The Court signalled — but did not determine — doubt as to whether the tort of intrusion upon seclusion is available in British Columbia, continuing the B.C. courts' years-long reluctance to adjudicate the issue. Finally, unlike many other B.C. decisions, the Court did not permit the plaintiff to amend the pleadings that were struck, again, imposing discipline on how class proceedings are framed.

Shriqui v. Blackbaud Canada Inc., et al., 2024 ONSC 6957

Read the case details

Facts

The plaintiff sought certification of a class proceeding following a ransomware attack that compromised personal data from various organizations and individuals utilizing the defendants' services. The attack occurred between February and May 2020, during which data was extracted from Blackbaud, prompting them to pay a ransom. Despite the breach, neither the plaintiff nor any other affected individuals reported any negative consequences from the incident. The class proposed in the action included Canadian residents whose personal information was accessed during the breach.

Decision

The Court found that the action met the criteria for certification under the *Class Proceedings Act*, 1992, including the existence of a common issue regarding the defendants' duty of care. However, the Court found that the likelihood of success in litigation was low as no harm had been demonstrated. The parties reached a settlement of $340,000 which was to be distributed on a *cy-près* basis to two educational institutions focused on internet policy and data security. The Court certified the action for settlement and approved a limited notification plan given the impracticality of identifying class members.

Key takeaway

When a plaintiff cannot demonstrate genuine harm originating from the acts of the defendant, the likelihood of ultimate success on the merits may be low. *Cy-près* settlements may be advisable for data breach cases in which identifying class members is impracticable.

Donegani v. Facebook, Inc., 2024 ONSC 7153

Read the case details

Facts

The plaintiffs alleged that Facebook had misused their data by making it available to certain third-party applications. The plaintiffs sought certification of a national class proceeding, alleging, among other things, intrusion upon seclusion and breach of provincial privacy statutes.

Decision

Justice Akbarali made a variety of findings in respect of the cause of action and common issues criteria of the certification test, but did not ultimately decide the certification motion. The findings included, among others:

- Ontario courts do not have jurisdiction to hear and decide claims under the privacy statutes of B.C., Manitoba and Newfoundland and Labrador.
- The proposed common issues relating to intrusion upon seclusion were not capable of certification in these circumstances.
- Certain of the proposed common issues relating to the contracts between Facebook and its users, and consent, were capable of certification. However, none of the proposed common issues relating to damages could be certified.

Justice Akbarali did not decide the preferable procedure criterion. She ordered the plaintiffs to propose a new class definition and litigation plan, following which the parties will return for further argument.

Key takeaway

The certification motion remains to be decided.

Biometric

Cleaver v. The Cadillac Fairview Corporation Limited, 2025 BCSC 910

Read the case details

Facts

In 2018, Cadillac Fairview Corporation Limited (Cadillac Fairview) installed cameras equipped with Anonymous Video Analytics technology (the Software) supplied by MappedIn Inc. (MappedIn) into wayfinding directories (Directories) at their shopping malls located in several provinces across Canada (the shopping malls).

Cadillac Fairview ran an eight-week pilot project, the purpose of which was to obtain an estimate of the number of visitors to each property and their rudimentary age and gender demographics. It disabled the Software in response to misinformation circulating online suggesting that the Software was "facial recognition" technology. The data obtained from the project was securely held by MappedIn on a decommissioned server. None of the defendants received, or made use of, the data, and the images taken were not retained.

The Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner of British Columbia (collectively, the Commissioners) launched a joint investigation to determine whether Cadillac Fairview was collecting and using the personal information of visitors to its malls.

On October 28, 2020, they released their report concluding that the Software created a unique numerical representation of a particular face, constituting a collection of biometric information. Since these numerical representations were created from images captured by the cameras, the Commissioners found that the creation of the biometric information from those images constituted an additional collection of personal information. It also concluded that the complaint was resolved because the Software had been disabled and all data deleted.

The plaintiffs, Joshua Cleaver and Curtis Kieres (the Plaintiffs), sought to certify a national class action pursuant to the *Class Proceedings Act*, R.S.B.C. 1996, c. 50 (CPA) on behalf of all "persons who viewed a wayfinding directory at one or more of the shopping malls during the relevant periods and any persons including minors, who accompanied them." They alleged that Cadillac Fairview secretly mined biometric data from unsuspecting visitors to their shopping malls, and that the defendants breached the proposed class members' privacy rights by collecting their personal data, namely their facial images, and converting them into numerical data.

Decision

The Court rejected the possibility of certification of the claims for (i) certain alleged statutory breaches; (ii) intrusion upon seclusion in British Columbia and Alberta; (iii) negligence; and (iv) alleged breaches of the Québec Charter.

The Court found that the Plaintiffs satisfied the requirements of paragraph 4(1)(a) of the CPA with respect to some of the causes of action set out in the pleadings notwithstanding the fact that it found there was no "basis in fact" that the defendants captured or stored any biometric or personal data.

However, it concluded that the Plaintiffs had failed to establish that there was an identifiable class of two or more persons, a requirement to certify a class action pursuant to paragraph 4(1)(b) of the CPA. Indeed, there was no factual basis to demonstrate that the class members could self-identify and no rational relationship between the proposed class definition (which had been amended three times) and the fundamental common issues, being that a facial image of an individual was recorded and used to create biometric and personal information about that individual.

The Court also held that the claims of the class members did not raise common issues, another certification requirement pursuant to paragraph 4(1)(c) of the CPA. It notably found no basis in fact that any facial images were recorded by the cameras located at the Directories or that biometric and personal information about class members was created. It also found there was no basis in fact for the allegation that the data contained personal information within the meaning of the relevant statutes, as no individual could be identified from the data.

Finally, the Court was not persuaded that a class action was the preferable procedure for the fair and efficient resolution of the common issues pursuant to paragraph 4(1)(d) of the CPA. Importantly, the Court's analysis considered the lack of evidence of demonstrable harm, the conclusion of the pilot program, and destruction of the data.

Key takeaway

The dismissal of this certification application highlights the challenges plaintiffs face in privacy-related class proceedings. This decision demonstrates that plaintiffs cannot rely solely on regulatory findings and conclusions to substantiate their claims in court, particularly where there is no identifiable data causing the information to be personal, and where the alleged collection of data has ended and the data deleted.

Doan c. Clearview AI inc., 2024 QCCS 3968

Read the case details

Facts

The plaintiff, Ha Vi Doan (Doan), sought the authorization to institute a class action on behalf of all Québec residents whose facial images and personal information were collected, used or disclosed without their consent by the defendant, Clearview AI (Clearview).

Clearview developed a facial recognition algorithm that enables it to create a facial imprint from biometric data taken from a photograph. Its search engine scours the Internet, locates photographs of faces and classifies them in its database according to their respective facial imprints. This software enables Clearview to offer its customers a service capable of assembling in a search report all the facial images whose imprints match a given image, and which are available on the Internet.

Doan alleged that Clearview has violated certain fundamental rights of the class members, including their right to privacy, the right to preserve their dignity and the right to control over use of their image. Clearview was also alleged to have breached its obligations under laws applicable to the collection of personal information. Clearview contested the apparent merits of only some of the causes of action raised, but also argued that the Québec courts lacked jurisdiction.

Decision

The Court held that it has jurisdiction over the proposed class action on behalf of Québec residents, further concluding that the claim that collecting photographs of the class members, using them to create a facial imprint and compiling a file on each of them without their consent constitutes an attack on the safeguard of their dignity pursuant to section 4 of the *Charter of Human Rights and Freedoms*, C.Q.L.R. c. C-12 (Québec Charter), is not a frivolous one. The Court held that this question deserved to be analyzed on its merits and authorized the class action.

The Court highlighted that the scope of the right to control the use of one's image has not yet been examined by the courts in such circumstances. It concluded that it is not far-fetched to raise the issue of whether the use of an image to, among others, create a facial imprint may violate the class members' right to control over the use of their image.

Key takeaway

This decision highlights the growing legal concerns surrounding the use of biometric data and facial recognition technology. As the case proceeds to the merits stage, it will be closely watched for its potential to shape the legal landscape in this rapidly evolving area, notably with regard to human rights and the right to one's image.

Imprimeries Transcontinental inc., Re, Commission d'accès à l'information du Québec, 1024350-S

Facts

In October 2020, the Québec privacy commissioner, the Commission d'accès à l'information (CAI), received from Imprimeries Transcontinental inc. (the Company) a declaration informing it of the creation of a database of biometric characteristics or measurements (the Declaration).

The original purpose of the Declaration was to justify the implementation, in the context of the COVID-19 pandemic, of an authentication system (the System) with two functionalities to control access to the Company's premises, i.e., a facial recognition functionality and a body temperature measurement functionality. At the time of its Declaration, the Company's objective with regard to the System was to ensure the safety of its employees and of its premises.

Considering that the temperature-taking functionality of the System had not been used since October 2022 and that the data generated by it had been destroyed, the CAI's decision only concerns the facial recognition functionality of the System.

Decision

The CAI ordered the Company to cease collecting biometric information allowing facial recognition, to cease using a facial recognition system using biometric measurements to control access to its premises, and to destroy the templates created and hash codes obtained by converting the facial photos collected.

After concluding that the Company is subject to 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 CAI held that a photograph of a person's face and its codification into a mathematical representation — both being part of the System's process — are sensitive personal information.

The *Québec Private Sector Act* provides that personal information may only be collected if there is a serious and legitimate interest. In addition, only personal information that is necessary for the purposes identified prior to the collection may be collected. In order to justify the need to collect such data, a company must demonstrate the legitimate, important and real objective pursued by this collection, as well as the proportionality of the invasion of privacy in relation to the objectives pursued. A company may not depart from these requirements, even with the consent of the person concerned.

First, the CAI considered that the Company had a legitimate interest in ensuring the security of its facilities and to take measures to control access to its premises. However, the CAI concluded that the Company had not demonstrated any particular security issues justifying such collection of personal information.

The CAI held that the Company did not demonstrate the importance of the objective pursued. Controlling access to a company's premises is a usual and common objective. A company's activities or a particular situation might justify a higher level of security that biometric data can provide, but there was nothing to indicate that this was the case here.

Second, the CAI concluded that the collection carried out by the Company was not proportional to the underlying objective considering the biometric and sensitive nature of the personal information in question. Indeed, the invasion of privacy resulting from the collection of the personal information was not minimized. The Company also did not establish how the collection of personal information required for the operation of the System provided benefits that outweighed the harm caused by such collection.

Key takeaway

This decision highlights the rigorous standards that apply to the collection and use of biometric data under Québec's privacy laws. Organizations must demonstrate a serious and legitimate interest and can only collect personal information that is necessary for the purposes identified prior to the collection. They cannot rely on consent alone to justify their practices.

This case reinforces the importance of prioritizing less privacy-intrusive alternatives wherever possible.

Granger v. Ontario, 2024 ONSC 6503

Read the case details

Facts

Micky Granger, a migrant farm worker, was subjected to DNA collection by the Ontario Provincial Police (OPP) in 2013 during an investigation of a violent sexual assault. Granger and 95 other workers provided DNA samples under what they believed was informed consent. However, the police did not provide copies of the consent forms, and the Centre of Forensic Sciences (CFS) retained the DNA profiles despite the *Criminal Code*'s requirement to permanently remove such data if the samples did not match any crime scene DNA. Granger alleged that this retention of his DNA violated his rights under section 8 of the *Canadian Charter of Rights and Freedoms* (Canadian Charter) and gave rise to a tort claim for intrusion upon seclusion.

Decision

The Court found that the CFS had failed to comply with the statutory requirement to permanently remove the electronic results of DNA analyses once it was established that the samples did not match. This failure constituted a breach of the plaintiffs' reasonable expectation of privacy, as they had consented to the collection of their DNA under the belief that their profiles would be destroyed if they were excluded as matches. The Court ordered aggregate damages of $1,000 per class member, totalling approximately $7,267,000, to be awarded for the breaches of the Canadian Charter rights. The Court emphasized that the breaches were serious and warranted damages for vindication and deterrence, despite the absence of evidence showing actual harm from the retention of the DNA profiles. However, the Court declined to award punitive damages, concluding that the CFS acted in good faith and did not engage in conduct that was malicious or reckless.

Key takeaway

This decision underscores the importance of strict compliance with statutory obligations when handling sensitive personal information, such as DNA. The CFS' failure to delete the electronic results as required by law was a key factor in the Court's decision. This highlights the legal risks organizations face when failing to adhere to statutory privacy safeguards, even in the absence of evidence showing actual harm.

Clearview AI Inc. v. Alberta (Information and Privacy Commissioner), 2025 ABKB 287

Read the case details

Facts

Clearview AI Inc (Clearview), a U.S.-based company, scraped billions of images from the Internet, including social media, to build a facial recognition database marketed to law enforcement. This decision arose following a joint investigation by Canadian privacy regulators (Alberta, British Columbia, Québec, and federal) into Clearview's facial recognition practices. It was released after the British Columbia Supreme Court's related decision in *Clearview AI Inc. v. Information and Privacy Commissioner for British Columbia*, 2024 BCSC 2311, and is largely consistent with it where there are common issues.

On February 2, 2021, the regulators issued a Joint Report finding that Clearview had violated privacy laws by scraping billions of images without consent, creating biometric profiles, and marketing its services to Canadian law enforcement. It recommended that Clearview cease offering its facial recognition tool in Canada, stop collection and use of Canadians' data, and delete any data in its possession.

On December 7, 2021, after Clearview refused to accept the recommendations, Alberta and its Information and Privacy Commissioner (the Commissioner) issued a binding order (the Order) requiring Clearview to adopt them. Clearview sought judicial review, challenging (i) Alberta's jurisdiction over it as a foreign corporation; (ii) the interpretation of "publicly available" information under the *Personal Information Protection Act*, S.A. 2003, c. P-6.5 (PIPA) — which exempts consent for such data; and (iii) the constitutionality of the Order under subsection 2(b) of the *Canadian Charter of Rights and Freedoms* (Canadian Charter), which guarantees the right to freedom of expression.

Clearview argued that: (i) its scraping of publicly accessible images was lawful and comparable to the practices of search engines like Google; (ii) PIPA's consent requirement was overly broad, chilling legitimate uses of public data (e.g., search engines); and (iii) the Order was unenforceable because it could not distinguish Albertans' data within its database.

The Commissioner: (i) maintained that Clearview violated Albertans' privacy rights under PIPA; (ii) defended its interpretation of the term "publicly available" information to exclude social media; and (iii) argued that any infringement of Canadian Charter rights was justified under section 1, given the low value of Clearview's commercial expression as compared to the significant privacy harms.

Decision

The Court declared that sections 12, 17, and 20 of PIPA, and subsection 7(e) of the *Personal Information Protection Act Regulation*, Alta. Reg. 366/2003 (PIPA Regulation), unjustifiably infringed subsection 2(b) of the Canadian Charter (freedom of expression). As a remedy, the Court struck the words "including, but not limited to, a magazine, book or newspaper" from subsection 7(e) of the PIPA Regulation, thereby vastly broadening the meaning of the term "publication" to include personal information and images posted to the internet (without privacy settings), and therefore the use of that information is not subject to a consent requirement.

This constitutional ruling did not invalidate the Order because the determination that Clearview's purpose for collecting and using personal information was unreasonable remained valid.

Applicability of PIPA to Clearview (jurisdiction)
The Court held that Alberta had jurisdiction over Clearview under the "real and substantial connection" test. Clearview had marketed its services to Alberta law enforcement and scraped images from servers located in Alberta, thereby establishing sufficient ties to the province. Its withdrawal from Canada during the investigation did not negate jurisdiction, as the Order addressed both past conduct and prospective compliance.

Interpretation of "publicly available"
The Court held that it was reasonable to interpret the "publicly available" exception contained in the PIPA and the PIPA Regulation to exclude social media. The Court accepted that privacy legislation warrants narrow exceptions to consent requirements. More generally, in considering the Canadian Charter arguments, the Court commented on an important principle of statutory interpretation of the PIPA: that the section 3 purpose statement indicates that the legislature sought to achieve balance, and not create a regime where privacy rights prevailed over all others. The result of this is that the purpose does not create an expansive or restrictive approach to interpretation.

Charter subsection 2(b) infringement
However, the Court ruled that PIPA's consent requirement unjustifiably limited freedom of expression, based on three main considerations:

- **Expressive activity:** The Court found that Clearview's scraping facilitated expression (e.g., search results), thereby engaging Canadian Charter protection. It specifically rejected Alberta's argument that the expression was not protected because it is commercial or motivated by profit.
- **Overbreadth:** The Court determined that the law's blanket consent rule captured benign activities (e.g., search engines indexing public data), disproportionately restricting lawful expression.
- **Minimal impairment:** While protecting privacy was recognized as a pressing and substantial objective, the Court held that the law's means were not minimally impairing. To address this, the Court tailored the remedy by broadening the "publicly available" exception to include public internet postings with no inherent privacy protections.

Reasonableness of Clearview's purpose
The Commissioner's finding that Clearview's use of the images it collected lacked a "reasonable purpose" under PIPA was upheld. The Court agreed that indiscriminate scraping, biometric profiling, and the commercial resale of data did not meet PIPA's reasonableness test. Clearview's argument that its practices aligned with the Canadian Charter values was rejected as untimely.

Enforceability of the Order
The Order was enforceable despite Clearview's claim that it could not identify Alberta-specific data. The Court dismissed this argument as a "scrambled egg defense," noting that Clearview could comply by adopting measures similar to its Illinois settlement. The Commissioner's iterative compliance process was also found to be lawful.

Key takeaway

The Court struck a balance between privacy and freedom of expression: while PIPA's overly broad consent requirement on the collection and use of publicly available information was deemed unconstitutional, Clearview's specific practices were found to be unreasonable under PIPA. The decision clarifies that privacy laws must not stifle legitimate internet searches and indexing but can appropriately target unreasonable uses of personal data, such as using that information to create a facial recognition database.

Privacy litigation: key importance of consent

Hogue c. Société canadienne des postes, 2025 QCCS 49

Read the case details

Facts

The plaintiff sought the authorization to institute a class action on behalf of customers of the defendant, Société canadienne des postes (Canada Post), alleging that their personal information had been collected and sold without their consent. The plainitiff alleged that Canada Post had created postal marketing mailing lists that it then sold to private corporations. The plaintiff was seeking an award of compensatory and punitive damages on behalf of the proposed class.

Decision

The Court authorized the class action in part and concluded that the allegations appeared sufficient to conclude that Canada Post collected information that goes beyond what is necessary to accomplish its purpose, that it resold this information to third parties for profit, and that it had not obtained the consent of its customers to do so. Therefore, it authorized the claims based on the violation of the *Privacy Act*, R.S.C. 1985, c. P-21, and of the *Civil Code of Québec*, C.Q.L.R. c. CCQ-1991.

The Court also authorized the claim based on the right to privacy under the *Charter of Human Rights and Freedoms*, C.Q.L.R. c. C-12 (the Québec Charter). It rejected Canada Post's argument that the Québec Charter does not apply to Canada Post on the grounds that it is a federal Crown corporation.

However, the Court did not authorize the misrepresentation claim based on the *Consumer Protection Act*, C.Q.L.R. c. P-40.1, because the plaintiff did not allege that he was aware of Canada Post's policy on the protection of personal information nor that he relied on Canada Post's representations contained therein.

With regards to compensatory damages, the Court notably stated that the use of personal information for commercial purposes without consent or compensation may cause harm. It thus concluded that the plaintiff's allegations could not be considered frivolous, including that his personal information is valuable and that he is entitled to claim payment of an amount equal to the value of the personal information collected by Canada Post.

As for punitive damages, the Court concluded that Canada Post's actions could be characterized as intentional within the meaning of section 49 of the Québec Charter.

Key takeaway

This decision reiterates the importance of obtaining consent to collect or use personal information, and highlights the legal risks associated with the unauthorized collection and resale of personal information. It also reflects the increasing recognition of personal information as a valuable asset for corporations.

E.G. v. Scotiabank (Bank of Nova Scotia), 2024 QCCS 3979

Read the case details

Facts

The plaintiff (E.G.), represented by his daughter, sought damages for the alleged violation of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (PIPEDA) by the defendant. E.G. alleged that Scotiabank wrongfully disclosed his bank statements to the Public Curator for Québec (the public curator) following a letter in which the public curator requested from Scotiabank disclosure of E.G.'s bank statements to protect his assets. Scotiabank applied to dismiss E.G.'s originating application.

Decision

The Court granted the application to dismiss.

The Court stated that subsection 7(3)(i) of the PIPEDA provides for an exception to the confidentiality of bank statements where the law requires disclosure.

The Court concluded that the law required disclosure of E.G.'s bank statements. Indeed, the public curator's letter, and the request for disclosure contained therein, was sent as part of inquiry powers under section 27 of the *Public Curator Act*, C.Q.L.R. c. C-81. Within the context of such inquiry, the public curator exercises its powers with the immunity conferred on commissioners under the *Act respecting public inquiry commissions*, C.Q.L.R. c. C-37, allowing the public curator to compel disclosure of personal information.

Although this reasoning was enough to grant Scotiabank's application to dismiss, the Court pointed out the lack of allegations regarding the nature of the prejudice suffered by E.G. as another basis for justifying the preliminary dismissal of the claim. The case law does not allow the award of compensatory damages solely because an unauthorized party had access to personal information.

Key takeaway

This decision reinforces the principle that privacy rights under PIPEDA are not absolute and may be overridden by statutory obligations to disclose personal information. It also highlights the importance of demonstrating actual harm in privacy-related claims.

For organizations, this case serves as a reminder to carefully assess whether a statutory exception applies before disclosing personal information.

Privacy interests and torts

Clearview AI Inc. v. Information and Privacy Commissioner for British Columbia, 2024 BCSC 2311

Read the case details

Facts

This judicial review application concerned the application of British Columbia's *Personal Information Protection Act* (PIPA) to Clearview AI Inc., a U.S.-based company providing facial recognition services. Clearview's technology collects ("scrapes") images of individuals from the internet, including those of British Columbians, and creates biometric identifiers for use by third-party clients, such as law enforcement agencies.

Following a joint investigation by Canadian privacy regulators, the Information and Privacy Commissioner for British Columbia (the Commissioner) found that Clearview had collected, used, and disclosed personal information of individuals in British Columbia without consent, in contravention of PIPA. The Commissioner issued an order prohibiting Clearview from offering its services in British Columbia, requiring it to cease collection, use, and disclosure of such information, and to make best efforts to delete personal information collected from individuals in the province without their consent.

Clearview sought judicial review, arguing that PIPA did not apply to its activities as a U.S.-based company, that the Commissioner's interpretation of "publicly available" information and "reasonable purpose" was unreasonable, and that the order was unnecessary, unenforceable, or overbroad.

Decision

The Supreme Court of British Columbia dismissed the petition, upholding the Commissioner's decision and order, making the following key findings:

- **Jurisdiction and extraterritorial application of PIPA:** Clearview's collection of personal information from individuals in British Columbia and its provision of services to entities in the province established a sufficient connection for jurisdiction. The fact that Clearview had no physical presence (offices, employees, or servers) in British Columbia was not determinative, given the nature of internet-based data collection and the business model at issue.
- **Interpretation of "publicly available" information:** The Commissioner reasonably interpreted "publicly available" information under PIPA and its regulations as excluding information available on social media or general internet sources. The Commissioner's conclusion that social media sites are not "publicly available" sources for the purposes of PIPA was supported by the statutory text, context, and purpose, as well as prior decisions and the sensitive nature of biometric information.
- **Consent and reasonable purpose:** The Court agreed that Clearview had not obtained the requisite consent for collection, use, or disclosure of personal information. The analysis considered (i) the sensitivity of the biometric data Clearview had scraped; (ii) the lack of connection between the purposes for which images were posted and Clearview's use of them; and (iii) the risks of harm, including misidentification and data breaches.
- **Necessity, enforceability, and breadth of the order:** The Court found the order necessary, given Clearview's refusal to commit to permanent withdrawal from the British Columbia market and its ongoing collection of personal information. Nor was the order overbroad, as PIPA regulates organizations' activities in relation to personal information of individuals in British Columbia, regardless of residency status.

Key takeaway

Provincial privacy legislation can have extraterritorial reach in the context of internet-based data collection. Privacy regulators may issue binding orders against foreign entities whose activities have a real and substantial connection to the province. Organizations also cannot rely on the "publicly available" exception under the PIPA to justify scraping personal information from social media or the internet without consent. Exceptions to privacy protections will be interpreted narrowly, and that the risk of harm — including loss of control over personal information and potential for misidentification — will be central to the assessment of reasonable purpose under privacy statutes. This decision is under appeal.

Moon v. International Alliance of Theatrical Stage Employees (Local 891), 2024 BCSC 1560

Read the case details

Facts

Kelly Moon, a former Senior Steward of IATSE Local 891, filed a civil claim against the union and several individuals on its executive board, alleging damages due to the unauthorized distribution of a report detailing her credit card use, which contained disputed and serious allegations against her. The report's release coincided with her re-election campaign in 2019, leading to significant reputational harm and her eventual electoral defeat. Moon claimed that the Executive Board, including Gary Mitch Davies, conspired to publish the report to undermine her candidacy, and she alleged breaches of various laws, including the *BC Privacy Act* and *Personal Information Protection Act* (PIPA), and negligence. The defendants sought to strike her claims, arguing that she failed to exhaust internal remedies and that her claims lacked a reasonable cause of action.

Decision

The defendants' application to strike the claims was largely dismissed, except for the challenge to the Election Committee's decision, which was administrative in nature. Most relevant was the Court's analysis of the tort of public disclosure of private facts, a tort that has been recognized in Alberta and Ontario. On reviewing recent B.C. Court of Appeal decisions in respect of intrusion upon seclusion (*Tucci v. Peoples Trust Company*, 2020 BCCA 246) and common law privacy torts more generally (*Insurance Corporation of British Columbia v. Ari*, 2023 BCCA 331), the Court found that it remained open to B.C. courts to recognize privacy torts, including public disclosure of private facts, and declined to strike the novel claim. The Court also declined to strike Moon's related claims under PIPA and the *BC Privacy Act*, as the Privacy Commissioner had found IATSE Local 891 in breach of PIPA, and in negligence.

Key takeaway

The Court declined to strike a claim for the tort of public disclosure of private facts, declining to close the door to privacy torts in B.C. and paving the way for the possible recognition of that specific tort.

The Hospital for Sick Children v. Information and Privacy Commissioner of Ontario, 2025 ONSC 385

Read the case details

Facts

The Hospital for Sick Children (SickKids) sought a sealing order to redact specific information from the record of proceedings following a ransomware cyberattack on December 18, 2022. This attack disrupted the hospital's clinical and corporate systems, leading to delays in prescriptions and lab results. By December 29, 2022, about 50% of the hospital's priority systems were restored. Following the incident, SickKids reported to the Information and Privacy Commissioner of Ontario (IPCO), which initiated an investigation under the *Personal Health Information Protection Act* (PHIPA) to determine if there was unauthorized disclosure or loss of personal health information. SickKids cooperated with IPCO, providing information about its cybersecurity measures, which the IPCO agreed to keep confidential to protect the hospital from future attacks.

Decision

SickKids demonstrated that the publication of the requested redacted information would increase its vulnerability to future cyberattacks, thereby jeopardizing the safety and security of its information technology systems and the critical medical care it provides. The Court found that the redactions sought were minimal and necessary to protect against further cyber threats, which serves an important public interest in safeguarding patient care. The Court granted the motion, finding that the redactions were necessary to protect the hospital's operations and public interest. Additionally, the Court ruled that SickKids was entitled to costs for the motion, as IPCO had initially opposed it but failed to file a proper factum, instead submitting a letter that did not assist the Court appropriately.

Key takeaway

The Court recognized the critical need to balance transparency with the protection of sensitive information, particularly in the context of cybersecurity. Organizations may be able to rely on this case to argue for limited redactions when they can demonstrate a credible risk of cyber threats.

Lamarche v. British Columbia (Securities Commission), 2025 BCCA 146

Read the case details

Facts

During an investigation, the British Columbia Securities Commission (the Commission) seized the appellant's email records — including communications he claimed were subject to solicitor-client privilege. The appellant commenced a civil action alleging breaches of the *Canadian Charter of Rights and Freedoms* and the *BC Privacy Act*, seeking declaratory and monetary relief. The Commission applied to stay or strike the claims on the basis that there was an ongoing administrative process and/or on the grounds that the claims disclosed no reasonable cause of action.

The chambers judge stayed the constitutional claims pending completion of the Commission's process and struck the *BC Privacy Act* claims. The appellant appealed, arguing that the Court should not defer to the administrative process and that his *BC Privacy Act* claims were improperly struck.

Decision

The Court of Appeal allowed the appeal in part. The Court affirmed the stay of the constitutional claims, holding that absent exceptional circumstances, litigants must exhaust administrative remedies before seeking judicial intervention.

However, the Court set aside the order striking the *BC Privacy Act* claims. While the Commission had a statutory immunity for acts done in good faith, a sufficient degree of recklessness can ground an inference of bad faith. The appellant's pleadings, which alleged the Commission had acted recklessly in failing to implement adequate protocols, were sufficient to ground a potential finding of bad faith or lack of good faith. The Court also rejected the chambers judge's conclusion that the *BC Privacy Act* could not be used to pursue claims that might also ground a Canadian Charter breach, clarifying that privacy and Canadian Charter claims are not mutually exclusive.

The Court ordered that the *BC Privacy Act* claims, including claims for punitive damages, be stayed (rather than struck) until the Commission's administrative process is complete, to avoid duplication and fragmentation of proceedings.

Key takeaway

BC Privacy Act claims may survive a motion to strike, even where statutory immunity for good faith conduct is pleaded, as a sufficient degree of recklessness can ground an inference of bad faith. The decision also confirms that privacy torts and Canadian Charter claims may proceed in parallel, subject to procedural deferral to avoid duplicative litigation.

Insurance Corporation of British Columbia v. Ari, 2025 BCCA 131

Read the case details

Facts

The underlying class action stemmed from the actions a former employee of the appellant who had accessed the private information of 78 customers for improper purposes and sold some of that information to criminals. Thirteen individuals were subsequently targeted in arson and shooting attacks. The class was defined to include all individuals whose information was accessed, as well as residents at their addresses. The summary trial judge awarded the aggregate damages award of $15,000 per class member for breach of privacy under section 1 of the *BC Privacy Act*. These damages were awarded regardless of whether any individual class member had actually suffered harm. Individual harms would be addressed at a later stage of the proceeding.

Decision

The Court of Appeal upheld the damages award, affirming that the *BC Privacy Act* creates a tort for breach of privacy without proof of damage. General damages may be awarded to compensate, vindicate, and deter injuries to the privacy interest itself, reflecting the quasi-constitutional nature of the right to privacy.

The Court rejected the argument that, absent proof of harm, only nominal damages are available, emphasizing that the law presumes some damage flows from the mere invasion of privacy. The seriousness and deliberate nature of the breach, including the distribution of information to criminals and the resulting risks to class members, justified an award above a merely symbolic amount. The limiting damages to a trivial sum would undermine the legislative intent of the *BC Privacy Act* and render the statutory right to privacy protection ineffective.

Key takeaway

The decision confirms that under the *BC Privacy Act*, general damages for breach of privacy may be awarded without proof of consequential harm. While the decision only concerned the *BC Privacy Act*, other provinces have similar legislation such that the Court of Appeal's reasoning may be applicable to parallel privacy statutes. The case also underscores that potentially significant aggregate damages awards may be granted for data breaches, even in the absence of evidence of individual harm.

Access to information

Centre d'acquisitions gouvernementales c. Teva Canada limitée, 2025 QCCQ 892

Read the case details

Facts

The appellant, the Centre d'acquisitions gouvernementales (the CAG), a Québec public body, appealed a decision rendered by the Commission d'accès à l'information (the CAI), which ordered the CAG to transmit to the respondent, Teva Canada Limited (Teva), copies of two access to information requests it received as part of the application 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 Public Sector Act*). Teva had sent a request to the CAG to obtain a copy of these two requests which aimed, in particular, to obtain a copy of a contract entered into with multiple suppliers, including Teva.

The CAI concluded that these access to information requests were held by the CAG in the exercise of its duties. The CAI also determined that the documents requested did not contain personal information, as the access to information requests were made for and on behalf of legal entities.

Decision

The Court dismissed the appeal.

The Court concluded that the CAI did not commit a reviewable error in finding that access to information requests are documents held in the exercise of the duties of a public body, which must be interpreted liberally within the meaning of the *Québec Public Sector Act*. The Court highlighted that the fact that the constitutive Act of a public body does not specifically provide for its obligation to hold certain documents does not in itself lead to the conclusion that these documents are not held in the exercise of its duties.

Duties of a public body extend to all its main duties, ancillary duties arising from these main duties, duties assumed voluntarily, and activities incumbent upon it by virtue of its constitutive Act or by virtue of a statute of general application, such as the *Québec Public Sector Act*. Therefore, the Court concluded that the documents requested by Teva in its access to information request were held by the CAG in the exercise of its duties.

Moreover, the Court held that the identity of access to information requesters was not confidential personal information. The Court recalled that the name of a person acting as a representative of a company is not considered confidential personal information if it is not associated with any other significant personal information. Thus, the documents requested by Teva did not contain any confidential personal information within the meaning of the *Québec Public Sector Act*.

If the legislator wished to establish a fundamental principle aimed at protecting the identity of access to information requesters and the confidentiality of access to information requests themselves, it would have been specified explicitly. The Court reiterated the CAI's view that it is not its role to create a new exception to the right of access nor to rewrite the *Québec Public Sector Act*.

Since the Court concluded that no exception to the right of access was applicable in this case, nothing prohibited the CAG from communicating the documents requested to Teva.

Key takeaway

This decision clarifies the scope of the *Québec Public Sector Act* by affirming that access to information requests are documents held in the exercise of a public body's duties and that the right of access must be interpreted liberally, unless an exception is expressly provided for in the *Québec Public Sector Act*.

In addition, the identity of access to information requesters is not confidential personal information within the meaning of this statute if it is not associated with any other significant personal information.

Office of the Information and Privacy Commissioner for British Columbia v. Airbnb Ireland UC, 2024 BCCA 333

Read the case details

Facts

This appeal concerned the disclosure of information about short-term rental (STR) licensees in the City of Vancouver, collected by the City pursuant to its agreement with Airbnb. In 2018, the City amended its bylaws to require STR operators to obtain licenses, which are issued in the operator's name and list their home address. Under a Memorandum of Understanding, Airbnb provided the City with hosts' names, license numbers, home addresses, and email addresses, all deemed "personal information" under the *Freedom of Information and Protection of Privacy Act* (FIPPA).

A requester sought disclosure of STR hosts' names, license numbers, and addresses. The City denied the request, citing several FIPPA exceptions, including those related to safety, property security, third-party business interests, and personal privacy. The requester sought review by the Office of the Information and Privacy Commissioner (IPC).

The IPC adjudicator ordered disclosure of certain information, finding that most of the City's and Airbnb's concerns about harm were not substantiated, except in one case involving a stalking victim. The adjudicator also determined that STR addresses were "contact information" rather than "personal information," as they were used for business purposes, and thus not protected from disclosure under section 22 of FIPPA.

Airbnb sought judicial review, arguing that the adjudicator's interpretation of FIPPA was unreasonable and that hosts should have been given notice and an opportunity to participate in the review. The Supreme Court of British Columbia set aside the IPC's decision, remitted the matter for reconsideration, and ordered that notice be given to all licensees before reconsideration.

Decision

The British Columbia Court of Appeal allowed the IPC's appeal in part, on the sole issue of whether individuals whose information might be disclosed should have notice of the IPC's consideration of the disclosure. It held that the decision of whether and to whom notice should be given falls within the IPC's discretion under section 54 of FIPPA.

The Court affirmed the lower court's decision, emphasizing that the adjudicator's analysis was overly formalistic and failed to properly consider the legislative context and purpose, and the practical privacy implications of disclosing home addresses used for business purposes.

Key takeaway

The case underscores the need for a contextual and purposive approach to the interpretation of "personal information" under FIPPA, particularly where home addresses are used for both personal and business purposes.

Jurisdiction of privacy authorities

Société québécoise d'information juridique c. Commission d'accès à l'information, 2025 QCCQ 859

Read the case details

Facts

An individual filed an application for review with the Québec privacy commissioner (CAI) after the Société québécoise d'information juridique (SOQUIJ) declined her request that her personal information be anonymized on SOQUIJ's website. SOQUIJ manages a database of judgments notably issued by the Tribunal administratif du logement (TAL) and the Tribunal administratif du travail (TAT).

SOQUIJ filed an application to dismiss, raising that the CAI lacked jurisdiction to rule on the application for review. It pointed out that the CAI already had in hand, at that time, all the relevant elements enabling it to grant, prior to a hearing on the merits, its application to dismiss. The CAI rejected the jurisdictional challenge and SOQUIJ appealed the decision.

Decision

The Court considered that the individual requiring anonymization from SOQUIJ had not, at any time, asked the TAL or TAT for any form of anonymization, *in camera* proceedings or measures to ensure the confidentiality of her identity. The Court held that the CAI could not impose the remedy sought, as it does not sit in appeal or review of these tribunals' decisions. A hearing on the merits was neither necessary nor desirable to reach such a conclusion.

Thus, the issue before the CAI was to determine the identity of the body with jurisdiction to grant the remedy sought by the individual seeking anonymity. Only the TAT and the TAL could "rectify", modify or anonymize the decisions they had rendered.

The personal information to which the rectification request relates is public information, as the individual seeking same did not ask the TAL or TAT to anonymize their decisions. In these circumstances, the remedy provided for in section 89 of the *Québec Public Sector Act* cannot be applied to rectify decisions rendered by jurisdictional bodies such as the TAT and TAL.

By refusing to grant the application to dismiss, and thereby refusing to decline jurisdiction, the CAI arrogated to itself a jurisdiction that falls more specifically on the TAT and TAL. Moreover, it erred when it concluded that personal information obtained in the exercise of a jurisdictional function, not covered by a non-disclosure, non-publication or non-dissemination order, remains covered by Chapter III of the *Québec Public Sector Act*, which includes section 89.

The CAI dismissed the application to dismiss on the grounds that it has general jurisdiction over SOQUIJ by virtue of its status as a public body under the *Québec Public Sector Act*. On appeal, the Court found that the CAI erred as it must have jurisdiction over the essence of the dispute, which was not the case here. SOQUIJ's appeal was granted in part, along with its jurisdictional challenge.

Key takeaway

This decision provides important insights into the jurisdictional limits of the CAI. It also reinforces the principle that confidentiality orders can only be issued by the tribunal or court hearing the claim. The CAI cannot retroactively impose such orders on decisions rendered by these tribunals or courts.

AI and privacy

Svoboda v. Modiface Inc., 2024 ONSC 6249

Read the case details

Facts

The Ontario Superior Court addressed an application to enforce Letters Rogatory issued by a U.S. court in a class action, where the applicants, representing a class, alleged violations of the Illinois *Biometric Information Privacy Act*. The U.S. court sought to compel ModiFace Inc., a Canadian company that developed augmented reality (AR) technology, to produce its source code and provide deposition testimony. ModiFace resisted the request, arguing that the scope was overly broad and that disclosing its source code could severely and irreparably harm its business.

Decision

The Court found that the applicants failed to demonstrate the relevance and necessity of the un-obfuscated source code under Ontario law, determining that the request was contrary to public policy due to the potential risk to ModiFace's proprietary technology. However, the Court ordered ModiFace to provide its compiled and obfuscated code and to submit to a deposition, emphasizing that the production of un-obfuscated code was not warranted. The Court also noted that the burden of compliance should not fall on ModiFace, a non-party to the U.S. action, and that less intrusive methods of obtaining the necessary information were available.

Key takeaway

This decision highlighted the importance of balancing international judicial assistance with the protection of Canadian businesses' confidential information. Disclosing un-obfuscated source code to a competitor would unnecessarily and severely harm the Canadian company's business interests.

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