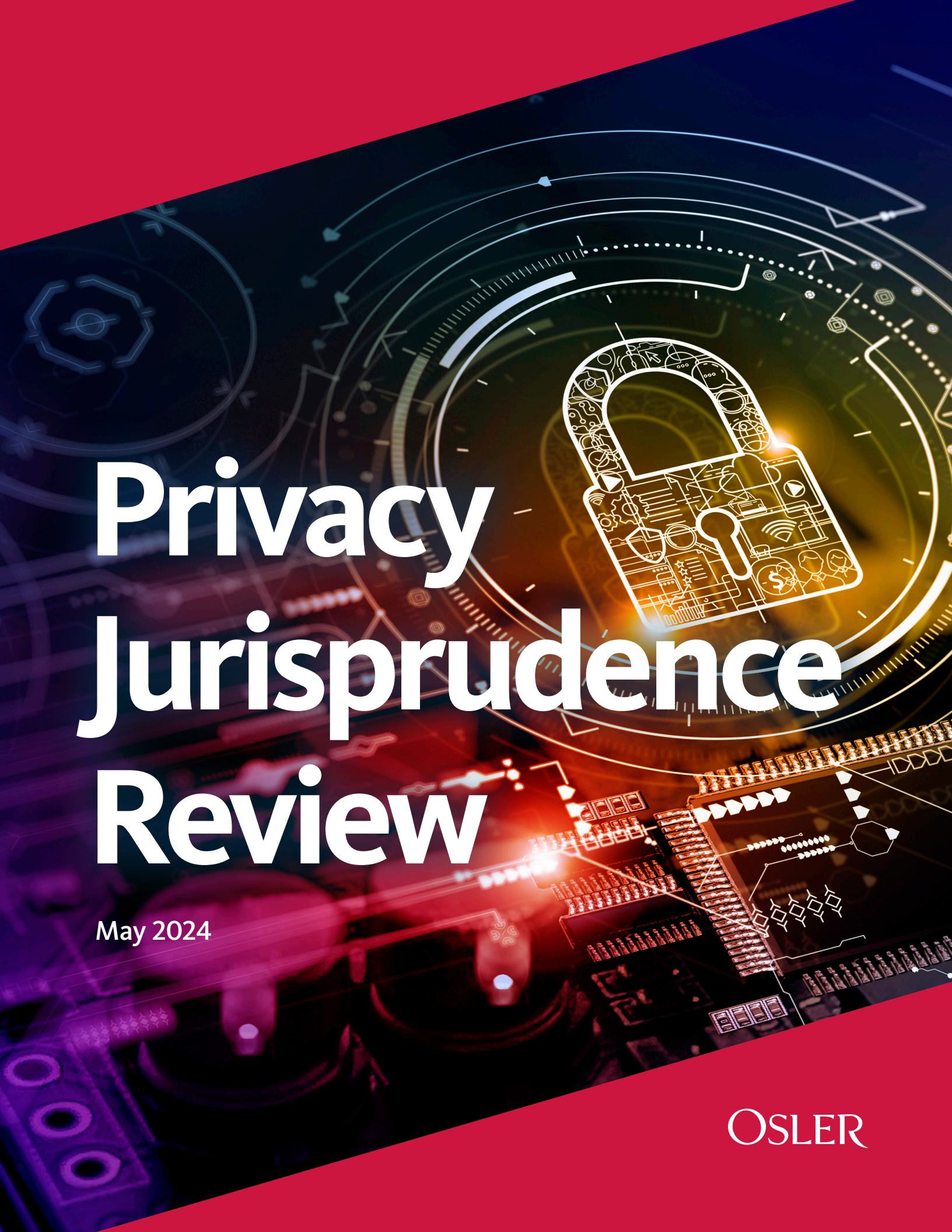


# Privacy Jurisprudence Review

May 2024

OSLER

# Table of contents

# Editor's note

The semi-annual *Privacy Jurisprudence Review* is intended to help busy in-house counsel, Chief Privacy Officers and compliance professionals navigate recent Canadian court decisions, gain a broad understanding of how privacy law is evolving in Canada and prepare for what lies ahead for their organization.

Osler's specialized Privacy Litigation 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.*

Comprising case summaries accompanied by expert commentary, the *Privacy Jurisprudence Review* will help readers identify and understand emerging trends while also gaining insight into the potential practical implications of those trends for their organizations within a broader policy context of evolving privacy law.

Recognizing how difficult it can be at times to keep up with developments, the *Privacy Jurisprudence Review* is intended to serve as a readily accessible, efficient and practical resource to help readers stay in the know, while saving time.

The authors wish to thank Andrea Korajlija, Tamara Tljakic, Josy-Ann Therrien and Marie-Luare Saliah-Linteau for their valuable contribution to this publication.

## Commentary contributors

**Kristian Brabander**
Partner, Litigation
**kbrabander@osler.com**
514.904.8107

**Robert Carson**
Partner, Litigation
**rcarson@osler.com**
416.862.4235

**Tommy Gelbman**
Partner, Litigation
**tgelbman@osler.com**
403.260.7073
604.692.2794

**Jessica Harding**
Partner, Litigation
**jharding@osler.com**
514.904.8128

**Craig Lockwood**
Partner, Litigation
**clockwood@osler.com**
416.862.5988

**Julien Morissette**
Partner, Litigation
and Insolvency &
Restructuring
**jmorissette@osler.com**
514.904.5818

# Privacy class actions: data breaches

## Highland Cannabis Inc. v. Alcohol and Gaming Commission of Ontario, 2024 ONSC 423

Read the case details

### Facts

The defendant High Tide Inc. and the plaintiff Highland Cannabis Inc. are in the retail cannabis industry. Highland Cannabis commenced an action against High Tide and the Alcohol and Gaming Commission of Ontario (AGCO), in relation to a data breach at the AGCO. Specific data regarding sales figures at retail cannabis stores for the months of July and December 2021 was either leaked or misappropriated. Highland Cannabis claimed that High Tide accessed this data and used it to the detriment of Highland Cannabis. High Tide brought a motion to dismiss the action on the basis that it was frivolous, vexatious and an abuse of the court's process.

### Decision

The court granted High Tide's motion and dismissed the action as against it. The court found that the statement of claim was frivolous and vexatious, and that it was plain and obvious that the plaintiff could not succeed in its claims. The court held that there

was no cause of action for intrusion upon seclusion, as High Tide did not intentionally intrude on the plaintiff's private affairs or concerns, and a reasonable person would not regard the invasion (accessing the sales data) as highly offensive causing distress, humiliation or anguish. The court further held that there was no cause of action for conversion, as the tort does not apply in the case of a data breach, and High Tide did not interfere with the plaintiff's right or title to the data. The court held that the mere viewing by passive recipients, in the context of this breach, cannot amount to an unlawful act.

## Key takeaway

This case illustrates the limitations of the torts of seclusion and conversion in the context of data breaches. The court noted that the tort of intrusion upon seclusion requires intentional or reckless conduct, and that High Tide was also a victim of the data breach. The court found that the tort of conversion does not apply to information, intellectual or intangible property, and that High Tide did not interfere with Highland Cannabis' right or title to the data.

# Carter v. LifeLabs Inc., 2023 ONSC 6104

Read the case details

## Facts

The plaintiffs, who are current or former customers of LifeLabs, a medical laboratory testing company, sued LifeLabs for a data breach that potentially affected the personal information of 8.6 million customers. The plaintiffs alleged various causes of action, including negligence, breach of contract, consumer protection remedies, statutory privacy violations and unjust enrichment, and sought damages and disgorgement of profits. After four years of litigation, the parties agreed to settle the action subject to court approval. The settlement agreement provided for a payment of $4.9 million in guaranteed settlement funds and $4.9 million in contingent settlement funds by LifeLabs to the class members, depending on the number of claims filed. The settlement agreement also stipulated that class counsel would request a 25% contingency fee of the settlement funds, and that each representative plaintiff would receive an honorarium of $2,500, if approved by the court.

## Decision

The settlement agreement and the counsel fee were approved, but the request for honorarium was denied. The representative plaintiffs' contribution was typical of the good work done by representative plaintiffs, and the court held that this was not an exceptional case that would justify an honorarium.

### Key takeaway

The court will scrutinize the fairness and reasonableness of a settlement agreement and counsel fees in a class action, and will consider various factors, such as the likelihood of recovery, the amount and nature of the settlement, the recommendation and experience of counsel, the future expense and duration of the litigation, the number and nature of objections and the presence of good faith bargaining.

# Option Consommateurs c. Home Depot of Canada Inc., 2023 QCCS 3493

Read the case details

## Facts

The defendant Home Depot allegedly breached its legal and statutory obligations by sharing with Meta Platforms Inc. and Facebook the personal information of class members without their consent, thereby violating their fundamental right to privacy. The Office of the Privacy Commissioner of Canada (OPC) investigated the sharing of personal information and concluded that the defendant had failed to obtain valid consent for the disclosure of such information.

The defendant was seeking permission to submit relevant evidence at the authorization stage under section 574 of the *Code of Civil Procedure* (CCP). At the outset, the court reiterated that it may allow relevant evidence at this stage if such evidence would enable the court to have a better understanding of the facts in its assessment of the criteria of section 575 of the CCP, while acting with caution to avoid turning the screening mechanism into a "pre-trial."

## Decision

The court granted the defendant permission to file Home Depot's Privacy and Security Statement in evidence, but denied permission relating to Facebook's Privacy Policy and Tools pertaining to Off-Facebook Activity.

The court decided that Home Depot's Privacy and Security Statement is a relevant and essential piece of evidence in the factual framework on which the request to authorize a class action is based. According to the court, this evidence would allow the defendant to contest allegations contained in the application in connection with the conditions of use or sharing of personal information. The court further found that this evidence would enable the defendant to present arguments highlighting the difference between in-store purchases and those made on the defendant's website, which were not the subject of the OPC's investigation, and would therefore be useful for the composition of the class and the formulation of questions of fact.

With respect to Facebook's documents, the court ruled that the defendant had not met its burden of proof. While the defendant argued that these documents, referred to in the OPC's report, are necessary to demonstrate the tools available to Facebook users to control their personal information, the court pointed out that it is not sufficient to wish to complete an exhibit if the relevance of the evidence is not demonstrated.

## Key takeaway

Confidentiality and security statements may be filed as relevant evidence under section 574 of the CCP where such statements allow a defendant to contest allegations contained in the application in connection with the conditions of use or sharing of personal information, and to present arguments in relation to the composition of the class and the formulation of questions of fact.

However, it is not sufficient to argue that the evidence being sought to be filed complete an exhibit if the relevance of the evidence is not demonstrated.

# Insurance Corporation of British Columbia v. Ari, 2023 BCCA 331

Read the case details

## Facts

The Insurance Corporation of British Columbia (ICBC) is appealing a decision in which it was found liable for its employee breaching the privacy of ICBC customers by selling private information linking the customers' licence plates to their home addresses. Several of these customers were then targeted with arson and shooting attacks. On appeal, ICBC maintained that the judge erred in concluding that the information was private, in imposing vicarious liability and in finding that general damages could be determined on a class basis.

## Decision

The Court of Appeal for British Columbia dismissed the appeal, stating that the trial judge had not erred in his conclusions on all arguments raised by the appellant. Namely, the Court stated that no mistakes were made in concluding that the sold information was private within the meaning of the *Privacy Act*; ICBC customers had a reasonable expectation that the information they provided the appellant would only be used for legitimate ICBC business purposes. They otherwise had the right to control the use of their personal information. Moreover, the Court stated that the judge did not err in imposing vicarious liability as policy reasons support the imposition of liability.

## Key takeaway

The employee's conduct in selling some of the information to third parties for a criminal purpose tainted all of her actions in accessing the customers' files without a legitimate business purpose.

The decision also confirms that the *Privacy Act* does not require proof of actual damage. General damages can be awarded on a class basis, without requiring individualized proof.

# G.D. v. South Coast British Columbia Transportation Authority, 2023 BCSC 958

Read the case details

## Facts

The plaintiffs are former employees of the defendant South Coast British Columbia Transportation Authority, and they seek certification of their proposed class proceeding under the *Class Proceedings Act* on their own behalf and on behalf of all other persons whose personal information was compromised by or as a result of a data security breach in 2020 that affected the computer networks and systems of the defendant.

In December 2020, TransLink's IT team discovered ransomware on their network, confirming that part of its IT infrastructure had been the target of a ransomware attack. Despite their cybersecurity program, cybercriminals gained access to TransLink's network security and inserted the ransomware after a successful phishing attempt on one of TransLink's operating subsidiaries' employees. The defendant took many steps to respond to the threat. The plaintiffs asserted the following causes of action: violation of statutory obligations to safeguard privacy, negligence, civil tort of conversion and unjust enrichment. Mainly, the plaintiffs pleaded that the defendant caused or enabled the data breach as it violated its own privacy policy standards.

## Decision

The court held that the claims are bound to fail and therefore dismissed the plaintiffs' application for certification.

### Key takeaway

The court stated that the target of statutory tort in a database breach context can only be the hacker, and not the database defendant.

# Broutzas v. Rouge Valley Health System, 2023 ONSC 540

Read the case details

## Facts

The plaintiffs are women who gave birth at either a hospital within the Rouge Valley Health System or at the Scarborough and Rouge Hospital between 2009 and 2014, and whose personal information was accessed and disclosed by rogue employees of the hospitals to salespeople of Registered Educational Savings Plans (RESPs) without their consent. They brought two proposed class actions against the hospitals, the rogue employees, the RESP salespeople and the RESP companies, alleging the tort of intrusion upon seclusion and seeking damages. The motions judge dismissed their certification motions, finding that they did not satisfy the criteria under section 5 of the *Class Proceedings Act, 1992*. The plaintiffs appealed from the dismissal, focusing on the tort claim against the individual defendants and the corresponding vicarious liability claims against the hospitals and the RESP companies.

## Decision

The Divisional Court agreed with the motions judge that the rogue employees did not access or disclose confidential medical information about the plaintiffs, but only contact information that was personal and not private, in the context of this case. The Court also agreed that a reasonable person would not regard the intrusion as highly offensive, causing distress, humiliation or anguish, as required by the third element of the tort. The Court found that the motions judge did not err in concluding that there was no cause of action against the RESP salespeople, who did not intrude upon the plaintiffs' seclusion, and that the scope of the tort did not need to be extended to them. The Court also found that the motions judge did not err in finding that the RESP companies could not be vicariously liable for the actions of the RESP salespeople.

### Key takeaway

The key takeaway from this decision is that the tort of intrusion upon seclusion is limited to deliberate and significant invasions of personal privacy that a reasonable person would find highly offensive.

# Privacy class action: biometric data

## Doan c. Clearview AI Inc., 2024 QCCS 213

Read the case details

### Facts

The petitioner sought authorization to institute a class action in compensatory and punitive damages against the respondent Clearview AI Inc. The respondent's activities involve the practice of "scraping," which uses multiple data collection programs — or "web crawlers" — to scan the Internet and collect images of individuals. The petitioner alleges that the respondent collected and extracted, on a massive scale, class members' photographs and other personal information, without their consent, for commercial purposes. According to the petitioner, the respondent's actions, including the collection, storage and use of their images and information, as well as the extraction of their biometric information, constituted a violation of their right to privacy, which is protected under Article 5 of the Québec *Charter of Human Rights and Freedoms*.

The respondent filed an application for leave to submit relevant evidence under article 574 of the *Code of Civil Procedure*, namely factual clarifications about its operations, extracts of evidence given by the petitioner in its proceedings before the Federal Court and the petitioner's statement of claim before the Federal Court.

## Decision

The court allowed only the filing of the petitioner's statement of claim before the Federal Court. According to the court, this evidence will allow the respondent to demonstrate that the Federal Court class action involved the same proposed representative plaintiff, similar facts and similar allegations. The court highlighted the fact that the Federal Court had previously found that none of the criteria for certification were met in this case, and that decision was not appealed. The court reasoned that allowing the introduction of other evidence would lead to an adversarial debate contrary to the purpose of the authorization process, which is to weed out frivolous and meritless claims.

The court further concluded that its jurisdiction over the proposed class action should be addressed on the merits. The constitutional issue should be considered only if necessary, in light of the facts of the case and the statutory background. In the court's view, the authorization stage is not the appropriate time for such a debate. Therefore, for the purpose of deciding the authorization issues, the court considered that Article 3148(3) C.C.Q. benefits from a presumption of validity.

### Key takeaway

When faced with an application to adduce relevant evidence by defendants under article 574 of the *Code of Civil Procedure*, the court must ensure that the introduction of the evidence will not lead to an adversarial debate contrary to the purpose of the authorization process.

The Court's jurisdiction over a proposed class action should be addressed on the merits and the constitutional issue should be considered only if necessary. The authorization stage is not the appropriate time for such debate.

# Situmorang v. Google, LLC, 2024 BCCA 9

Read the case details

## Facts

The appellant appealed from an order dismissing his application to certify a class proceeding, and dismissing the action itself, on the basis that the notice of civil claim did not disclose a cause of action.

This proposed class action involves allegations against Google LLC for using facial recognition technology to extract, collect, store and use the facial biometric data of thousands of Canadians without their knowledge or consent. The appellant argued that this conduct violated their privacy rights and pleaded causes of action under the *British Columbia Privacy Act* (B.C. Privacy Act) and the common law tort of intrusion upon seclusion. The appellant also seeks remedies under provincial consumer protection legislation, claiming that Google engaged in deceptive and unconscionable practices.

## Decision

The first judge dismissed the appellant's application to certify the action as a class proceeding, and ultimately dismissed his action, stating that the notice of civil claim did not disclose a cause of action pursuant to section 4(1)(a) of the *Class Proceedings Act* and that it was not in the interests of justice to allow the appellant to amend the claim.

The Court of Appeal found that the first judge erred in mischaracterizing the nature of the appellant's claims, and in her approach to assessing the viability of the pleaded claims. According to the Court of Appeal, this affected her analysis of the causes of action, leading to errors in assessing the elements of the claim. The Court of Appeal pointed out that, assuming the facts pleaded to be true, the notice of civil claim does disclose a cause of action for breach of privacy under the B.C. Privacy Act. The Court of Appeal further determined that, while there are deficiencies in the pleaded claims for remedies under provincial consumer protection legislation, the appellant should have an opportunity to address the deficiencies through amendments. The elements of the common law tort of intrusion upon seclusion are sufficiently pleaded. The issue of whether a common law privacy tort exists in British Columbia should be raised, as necessary, with the court below on the remittal.

### Key takeaway

When determining whether a claim discloses a cause of action, the court should assume the pleaded facts as true, read the claim generously and avoid addressing the merits of the claims. It is essential for judges to accurately characterize the nature of the claims and refrain from weighing evidence at this stage.

# Doan v. Clearview AI Inc., 2023 FC 1612

Read the case details

## Facts

The plaintiff sought to certify a class action against Clearview AI Inc., a corporation that provides facial recognition and identification services, alleging copyright infringements and violations of the moral rights of the class members.

The plaintiff claimed that Clearview's conduct involved the collection, possession, reproduction, use, distribution, rental, sale and offering for rent and sale of photographs without the consent of the rights holders. She argued that Clearview's actions amounted to copyright infringements and other violations of the *Copyright Act*.

## Decision

The only issue was whether the court should certify the action as a class action. The court dismissed the plaintiff's motion for certification, finding that people could not determine whether they are members of the class and the plaintiff had not established that Clearview possesses or can analyze the relevant metadata necessary to identify the class members. The plaintiff had not established an identifiable class of two or more persons, which is a certification requirement under the Federal Courts Rules.

### Key takeaway

In privacy class actions, it will often be challenging for plaintiffs to identify an appropriate class definition. This is an example where the plaintiff's inability to do so was fatal to the certification motion.

# Individuals' privacy interests

## Google LLC v. Canada (Privacy Commissioner), 2023 FCA 200

Read the case details

### Facts

In a reference, the Privacy Commissioner of Canada asked the Federal Court whether the operation by Google LLC of its search engine is excluded from the scope of Part I of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) through the "journalistic purpose" exception in section 4(2)(c) of PIPEDA when the search engine collects, uses and discloses journalistic articles published by a newspaper. The Federal Court found that PIPEDA applies.

Google appealed. Google's first argument was that the Federal Court should have refused to answer the question as it could not have properly answered it without considering the *Canadian Charter of Rights and Freedoms* (i.e., whether subjecting Google's search engine to Part I of PIPEDA would infringe on the *Charter's* guarantee of freedom of speech and whether the Commissioner has jurisdiction to decide *Charter* issues). Google's second argument was that the reference judge interpreted the exception found in s. 4(2)(c) of PIPEDA too restrictively.

## Decision

The Federal Court of Appeal dismissed Google's appeal. All three judges agreed that the Federal Court made no errors in relation to the *Charter* issues. However, the panel reached different conclusions regarding the journalistic purpose exception. The two-judge majority of the Federal Court of Appeal (Justices Laskin and Gleason) dismissed Google's appeal, finding that the Federal Court was correct in concluding that the journalistic purpose exception does not apply. The third judge (Justice Webb) wrote dissenting reasons, finding that PIPEDA does not apply to the Google search engine when it collects, uses and discloses journalistic articles published by a newspaper.

### Key takeaway

There continues to be uncertainty about the scope of the journalistic exception under s. 4(2)(c) of PIPEDA.

# Gagnon c. Ministère des Transports et de la Mobilité durable, 2023 QCCAI 394

Read the case details

## Facts

In May 2022, the plaintiff submitted two access requests to the *Ministère des Transports et de la Mobilité durable* (the Minister). Although the Minister partially responded to the access requests, the plaintiff was not satisfied with the response and subsequently filed a request for review with the Commission d'accès à l'information (the Commission). During the preparatory conference, the Minister notably argued that the Commission should refuse to hear the plaintiff's case on the grounds that the plaintiff is acting on behalf of two companies of which he is the president, and that the plaintiff cannot act in his personal capacity.

## Decision

The Commission concluded that, pursuant to Section 9 of the *Act respecting access to documents held by public bodies and the protection of personal information*, the plaintiff was entitled to participate in the proceedings in his individual capacity. The Commission highlighted the fact that the legislator, in recognizing the right of any person to access documents held by public bodies, deliberately excluded any requirement relating to the applicant's interest in obtaining a document. Thus, an applicant is not required to provide the reasons for the request or to disclose the purpose for which they intend to use the document. Consequently, an organization cannot require that the applicant justify their interest or intentions or establish their status or qualifications. The accessibility of a document should not be assessed on the basis of the person exercising this right, but rather on the basis of the document itself.

The Commission also reiterated its position by confirming that legal entities, including public bodies, associations, companies and unions, must be represented by a lawyer in accordance with the *Act respecting the Barreau du Québec* when such representation involves legal pleadings. However, this obligation does not limit the right of a legal entity to be represented by one of its officers if the representation is aimed at clarifying factual issues without involving legal pleadings, which falls exclusively within the competence of a lawyer.

## Key takeaway

The legislator, in recognizing the right of any person to access documents held by public bodies, deliberately excluded any requirement relating to the applicant's interest in obtaining a document. As such, an individual can act in their personal capacity in an access request. While legal entities must be represented by a lawyer, this obligation does not limit the right of a legal entity to be represented by one of its officers if the representation is aimed at clarifying factual issues without involving legal pleadings.

# Access to information

## Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner), 2024 SCC 4

Read the case details

### Facts

A journalist from the Canadian Broadcasting Corporation requested access to 23 mandate letters delivered by the Premier of Ontario to his ministers in 2018. These letters set out the Premier's views on policy priorities. The Cabinet Office declined the request, claiming that the letters were exempt from disclosure under the Cabinet records exemption in section 12(1) of Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA), which protects the confidentiality of records that reveal the substance of the Cabinet's or its committees' deliberations.

The Information and Privacy Commissioner of Ontario (IPC) found that the letters were not exempt and ordered their disclosure. The IPC's decision was upheld by the majority of the Court of Appeal for Ontario, which found the IPC's decision reasonable.

## Decision

The appeal to the Supreme Court of Canada was allowed, and the IPC's order was set aside. The mandate letters are protected from disclosure under s. 12(1) of FIPPA.

The majority of the Supreme Court explained that, in addressing assertions of Cabinet confidentiality, administrative decision makers and reviewing courts must be mindful not only of the paramount importance of public access to government-held information, but also of the fundamental purpose of Cabinet secrecy to enable effective and responsible government, as well as the considerations of efficiency, candour and solidarity that underlie it. All freedom of information legislation across Canada balances these two essential objectives through a general right of public access to government-held information subject to exemptions or exclusions. Courts and decision makers must also be mindful of the dynamic nature of executive decision making (which goes beyond formal meetings of Cabinet and its committees, and includes priorities communicated by the Premier at the outset of his term), the function of Cabinet itself and its members, the role of the Premier, and Cabinet's prerogative to choose when and how to announce its decisions.

The majority found that, in this case, the narrow zone of protection for Cabinet deliberations created by the IPC's interpretation and application of s. 12(1) of FIPPA was not justified, even on a more deferential standard of reasonableness. The majority found that the IPC failed to give meaningful weight to the legal and factual context, including traditions and constitutional conventions concerning Cabinet confidentiality, the role of the Premier and the fluid, dynamic nature of the Cabinet decision-making process. As a result, the majority found that the IPC's narrow interpretation of the "substance of deliberations" was unreasonable, as was the IPC's application of the provision to the mandate letters.

### Key takeaway

Freedom of information legislation strikes a balance between the public's need to know and the confidentiality that the executive requires to govern effectively. All such legislation across Canada balances these two essential goals through a general right of public access to government-held information subject to exemptions or exclusions — including those for Cabinet records or confidences. The interpretation and application of s. 12(1) of FIPPA must not be limited in a manner that would provide an unreasonably narrow zone of protection.

# Fonderie Horne c. Ministère de l'Environnement et de la Lutte contre les changements climatiques, 2023 QCCQ 10259

Read the case details

## Facts

The appellant Fonderie Horne, who operates a major industrial facility in Rouyn-Noranda, appealed from the decision rendered by the Commission d'accès à l'information (the Commission) which denied its application for review of a decision to disclose a document.

The Ministère de l'Environnement et de la Lutte contre les changements climatiques (the Minister) agreed to disclose tables showing all measurements taken of various air emissions from the Horne smelter in Rouyn-Noranda for 2019 following an access request made by an interested party. Fonderie Horne referred the matter to the Commission, requesting a review of the Minister's decision to disclose the document.

Fonderie Horne claimed that the Commission committed a decisive error of law in its interpretation of the exception to the right of access provided for in section 28 of the *Act respecting access to documents held by public bodies and the protection of personal information* (the Access Act), by adopting a criterion of application that is not in accordance with the law. Further, the appellant argued that the Commission committed a decisive error of law in its interpretation of paragraph 4 of section 118.4 of the *Environment Quality Act* (EQA), which led it to erroneously conclude that it applied in this case.

## Decision

The court concluded that s. 28 of the *Access Act*, which aims to avoid prejudicing investigations or potential investigations, is not a substitute or alternative for sections 23 and 24 of the *Access Act*, which deal with the protection of industrial or commercial secrets. The court pointed out that the document in dispute must be produced and transmitted to the Minister annually by the appellant under its ministerial authorization. According to the court, if the appellant's argument were to be accepted, the document in dispute could never be transmitted to an access requestor, even though it is clear that there is not and never could be any criminal prosecution against the appellant in relation to the contents of this document.

The court also interpreted s. 118.4(4) of the EQA, which grants any person the right to obtain the described information and documents, unless the exception provided in s. 28 of the EQA applies. The court highlighted that the *Access Act* does not override the provisions of other statutes that provide a more generous right of access. In the court's view, the legislator has clearly indicated that the EQA regime is more generous and is

part of the complete framework, which promotes citizen participation in maintaining and improving environmental quality. The court found that there is no error of law in the Commission's decision that would justify overturning it.

For all these reasons, the court dismissed the appeal.

## Key takeaway

Section 28 of the Access Act, which aims to avoid prejudicing investigations or potential investigations, is not a substitute or alternative for ss. 23 and 24, which notably deal with the protection of industrial or commercial secrets.

Moreover, the *Access Act* does not override the provisions of other statutes that provide a more generous right of access. The EQA provides a more generous right of access, which is part of its legislative framework to promote citizen participation in maintaining and improving environmental conditions.

# American Iron & Metal Company Inc. v. Saint John Port Authority, 2023 FC 1267

Read the case details

## Facts

The applicant American Iron and Metal Company Inc. sought a review under subsection 44(1) of the *Access to Information Act* (ATIA) of the decision by the Saint John Port Authority to disclose portions of a 2011 lease agreement and a 2017 lease renewal and amending agreement entered into between American Iron and the Port Authority. The decision was made further to a request by the Canadian Broadcasting Corporation under section 6 of the ATIA. The Port Authority determined that certain information was exempt from disclosure under the ATIA, but concluded that the remainder of the two documents should be disclosed to the CBC. American Iron disagreed and sought to exempt large portions of the documents from disclosure under paragraphs 20(1)(b), (c) and/or (d) of the ATIA.

## Decision

The court found that the information was not exempt under paragraph 20(1)(b) because it was not "supplied" by American Iron to the Port Authority, but rather constituted terms and conditions that were negotiated between the parties. The court also found that American Iron failed to establish a reasonable expectation of probable harm arising from the disclosure of the information as required under paragraphs 20(1)(c) and (d). The court held that American Iron's evidence was insufficient, speculative and based on generalities, bald assertions and hypothetical risks. The court also rejected American Iron's reliance on anticipated negative media coverage as a basis for exemption.

## Key takeaway

The decision demonstrates that a third party objecting to the disclosure of information should give careful consideration to the nature and extent of evidence needed — in the particular context of the case — to demonstrate why disclosure should not be made.

# Newfoundland and Labrador (Information and Privacy Commissioner) v. Newfoundland and Labrador (Justice and Public Safety), 2023 NLCA 27

Read the case details

## Facts

An applicant made an access to information request to the Minister of Justice and Public Safety (the Minister) regarding a complaint about environmental violations. The Minister disclosed all relevant documents except those withheld under specific provisions of the *Access to Information and Protection of Privacy Act, 2015* (ATIPPA 2015). The applicant filed a complaint with the Information and Privacy Commissioner, challenging the Minister's refusal to disclose the withheld records. The Commissioner requested that the Minister provide a complete copy of the records and justify the claimed exceptions to disclosure. The Minister argued that the records were protected by solicitor-client privilege.

## Decision

The first judge made two key findings. First, the Commissioner did not have the authority to compel the disclosure of solicitor-client records, such that the Minister was not required to comply with the Commissioner's recommendation for disclosure. Second, even if the Commissioner had the authority, the Minister had met the burden of proving that the applicant had no right to access the solicitor-client privileged records.

The Court of Appeal examined the Supreme Court's decision in *Alberta (Information and Privacy Commissioner) v. University of Calgary*, 2016 SCC 53, to perform its analysis. The Court agreed with the first judge that the relevant provisions of ATIPPA 2015 do not explicitly grant the Commissioner the power to compel the production of records subject to solicitor-client privilege. The Court also considered the purpose and intent of the legislation, as well as the importance of solicitor-client privilege in the legal profession, in analyzing the burden of proof placed on the Minister to establish that the applicant had no right to access the privileged records.

The Court emphasized that the conclusion that the Commissioner cannot compel the production of solicitor-client records does not leave an applicant without recourse. In such cases, an applicant can appeal the refusal directly to the Supreme Court of Newfoundland and Labrador under section 52 of ATIPPA 2015. The courts would then address the issues associated with the claim of solicitor-client privilege, as is traditionally done.

## Key takeaway

This decision highlights the importance of solicitor-client privilege and the limits of an Information and Privacy Commissioner's powers in accessing privileged information.

# Savard c. Université de Montréal, 2023 QCCAI 237

Read the case details

## Facts

The petitioner applied to the Commission d'accès à l'information after the respondent only partially complied with his access request. Université de Montréal refused access to certain documents by invoking the protection of tests intended for comparative appraisal (section 40 of the *Act respecting Access to documents held by public bodies and the Protection of personal information* (the Act)) as well as the protection of information of a technical nature (section 22 of the Act).

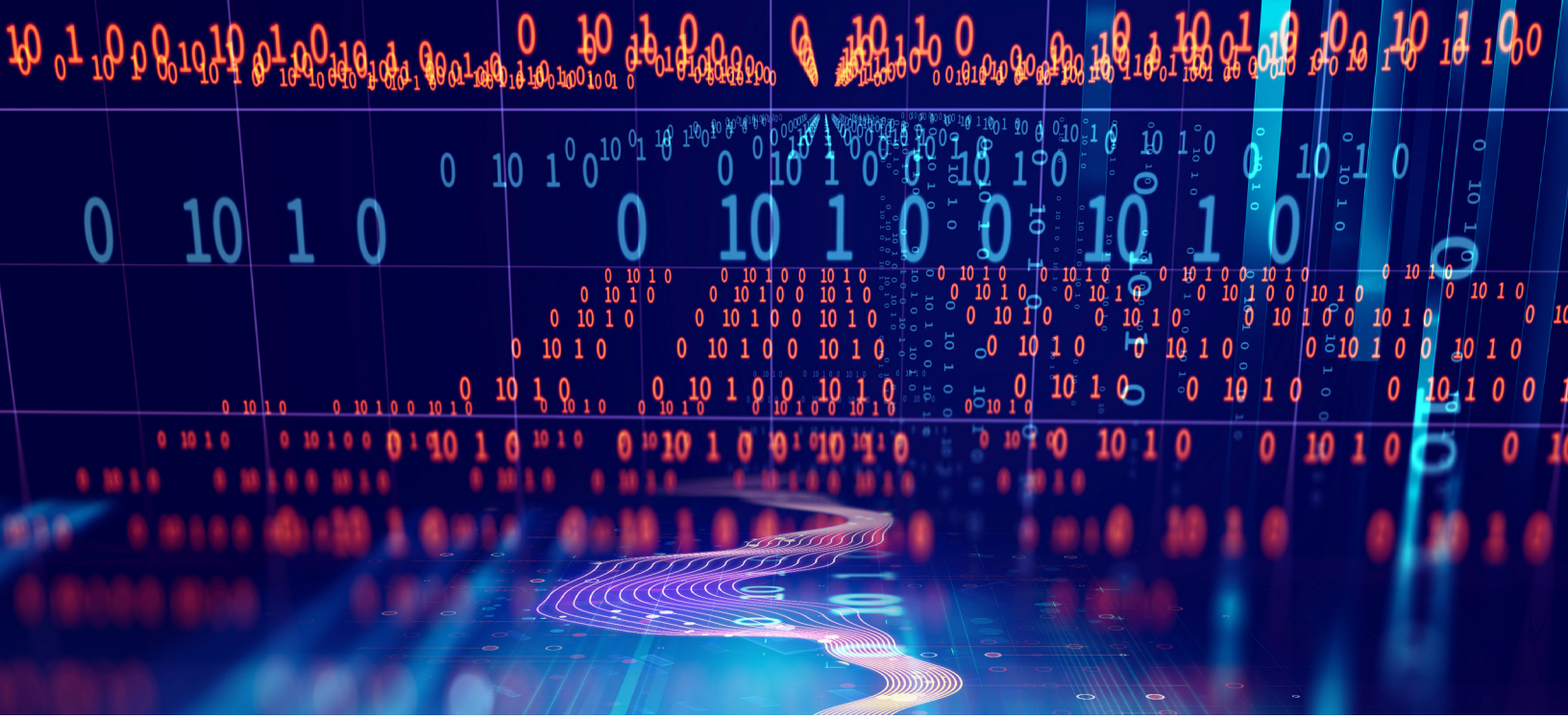
Only the latter remains in dispute, which regards certain documents provided to students for identified courses. With respect to this matter, Université de Montréal maintained that in addition to certain documents containing both test and training elements, the disclosure of other requested documents (i.e., content of lectures, PowerPoint presentations, recorded courses) would likely cause financial loss to Université de Montréal or to provide an advantage to third parties.

## Decision

The Commission ordered Université de Montréal to submit to the plaintiff all requested documents for which the defendant invoked s. 22 of the Act, stating that the loss of prestige is not an economic impact within the meaning of s. 22 of the Act; rather, the competition that exists between educational institutions is to attract the best candidates. Université de Montréal presented no evidence of any economic impact resulting from the fact that the candidates selected would no longer be the best in its opinion due to the disclosure of the teaching material that was the subject of the access request.

### Key takeaway

The loss of prestige is not an economic impact within the meaning of s. 22 of the Act.



# Cyberattacks and data breach: reports

## Complaint HR22-00036 (Re), PHIPA DECISION 210 (ON IPC)

Read the case details

### Facts

A public hospital was the victim of a cyberattack during which the threat actor accessed numerous hospital systems. The IPC opened a file relating to this breach, and subsequently received four complaints from affected individuals.

During the data breach, the hospital took immediate steps to disable the affected accounts and fix the firewall issue that had allowed the access to occur. It severed its servers from the Internet and third-party networks, and isolated any systems showing signs of compromise. The hospital disabled all compromised accounts, including the one used by the threat actor, and forced password resets for all accounts in the hospital's active directory. The hospital was not able to contain the data that the threat actor had already transferred out before the hospital found out about the breach. However, it did make efforts to limit any further spread of this data by monitoring the dark web for signs of any data that may have been obtained from this breach.

The hospital notified the public of the breach by posting a Personal Information Public Notice on the hospital's website, and it also self-reported the breach to the IPC by notifying of a breach under the *Personal Health Information Protection Act* (the Act).

The hospital provided the IPC with numerous guidelines in place addressing information security, all of which were revised following the cyberattack. These included guidance on the strength of passwords, limitations on privileges granted to accounts and firewall protections. The hospital also provided the IPC with a breach protocol specific to cybersecurity incidents, which was put in place following the incident.

## Decision

In light of the numerous steps taken by the hospital to remediate the situation, including the guidance now in place, the Commissioner concluded that it was not necessary to pursue a review of the matter under Part VI of the Act.

### Key takeaway

Taking immediate steps to adequately respond to a data breach and implementing remediation steps to resolve harm will factor into the IPC's discretionary decision to review a matter under Part VI of the Act, which can lead to offences, prosecutions and fines.

## About Osler, Hoskin & Harcourt LLP

Osler is a leading law firm with a singular focus – your business. From Toronto, Montréal, Calgary, Ottawa, Vancouver 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 500 lawyers to provide responsive, proactive and practical legal solutions driven by your business needs. For over 150 years, we've built a reputation for solving problems, removing obstacles, and providing the answers you need, when you need them.

**It's law that works.**

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



OSLER