Privacy Jurisprudence Review

Fall 2024

OSLER

Table of Contents

Editor's note

In the current digital age, where personal data circulates with unprecedented velocity and volume, the mandate of Chief Privacy Officers (CPOs), in-house counsel and compliance professionals, is both vital and challenging. This publication is designed to serve as an authoritative review of the latest developments in privacy law in Canada, providing critical insights into the judicial decisions and trends that are defining the contours of privacy rights and corporate responsibilities. By delving into significant case law, our objective is to arm CPOs with the foresight and knowledge necessary to maintain compliance and proactively manage the interplay between evolving legal standards, emerging technologies, and business imperatives, through expert commentary.

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*, as well as workshops and roundtables discussing emerging trends in AI and governance.

The authors wish to thank Andrea Korajlija, Tamara Kljakic, Josy-Ann Therrien, Brodie Noga and Marie-Laure 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

Option Consommateurs c. Home Depot of Canada Inc., 2024 QCCS 1305

Read the case details

Facts

Plaintiff sought the authorization to institute a class action against Home Depot alleging it breached its legal and statutory obligations by sharing with third parties, including Facebook, the personal information of class members without their consent, thereby violating their right to privacy. The sharing of such information was the subject of an investigation by the Office of the Privacy Commissioner of Canada (OPC), who concluded that the respondent had failed to obtain valid consent for the disclosure of personal information.

Decision

The Court partially authorized the class action against Home Depot, allowing the petitioner to seek recovery of $10,000,000 in punitive damages, but rejected the claims based on extracontractual liability and false representations. The Court also modified the description of the group, to restrict it to members who have a Facebook account.

According to the Court, the allegations deemed to be true suggested that Home Depot may have shared members' personal information without their implicit or explicit consent, thus violating articles 35 and 37 of the *Civil Code of Québec* (CCQ) as well as section 13 of the *Act respecting the protection of personal information in the private sector*, and sections 5 and 6.1 of the *Personal Information Protection and Electronic Documents Act*. There was therefore an arguable case that Home Depot may have committed a fault under article 1457 of the CCQ.

However, the Court found that the petitioner did not demonstrate the existence of a prejudice. The mere fact that personal information is in the unauthorized possession of third parties does not constitute a prejudice, and thus does not give rise to compensatory damages. For these reasons, the Court concluded that the petitioner had not demonstrated an arguable case based on extracontractual liability.

The Court also rejected the plaintiff's arguments based on false representations, since it found that the relevant sections of the *Consumer Protection Act*, were inapplicable.

With regard to punitive damages based on unlawful and intentional violation of the right to privacy, the Court found that the allegations allowed to draw the inference that the respondent must have known the consequences of the alleged wrongful conduct.

Key takeaway

The Court reiterates the importance of obtaining a consumer's express consent to the use of their personal information. The mere fact that personal information is in the unauthorized possession of third parties is not sufficient to constitute prejudice. This case serves as a reminder that a class action can be authorized solely on the basis of a claim for punitive damages.

Del Giudice v. Thompson, 2024 ONCA 70, leave to appeal to the SCC dismissed 2024 CanLII 88330

Read the case details

Facts

This appeal followed a decision dismissing a certification motion for a proposed class action based on a data breach of personal and confidential information collected from individuals applying for credit cards. The separate causes of action pleaded were categorized into two groups: (1) data misuse claims and (2) data breach claims. The motion judge found that the pleadings did not support any valid cause of action and "egregiously" contravened the rules of pleading. The appellants argued the motion judge erred in (1) determining that none of the causes of action pleaded were viable; (2) by relying on unsworn documents; and (3) striking out portions of the statement of claim without leave to amend.

Decision

The Ontario Court of Appeal dismissed the appeal, finding that the pleadings were defective as the claims advanced could not succeed. The Court also found that the motion judge was entitled to rely on unsworn documents to reach that determination on the basis of the settled principle that a pleading is deemed to include any document to which it refers. In this case, the documents in question (which included the defendant's privacy policy, the plaintiff's application for credit, and a credit card agreement) were all expressly referenced in the Statement of Claim. The Court therefore concluded that the motion judge was entitled to rely on these documents is dismissing the claim that the defendants had used the plaintiffs' information for unauthorized purposes. The Court also deferred to the motion judge's decision not to grant leave to amend, acknowledging that the appellants had been given multiple opportunities to amend their statement of claim but failed to do so.

Key takeaway

This case reaffirms that certification continues to be a powerful screening device to prevent meritless claims from moving forward, and also illustrates how defendants can challenge pleadings at an early stage. It is also a helpful reminder of the scope of pleadings, which are deemed to include any document(s) to which they refer.

Ari v. Insurance Corporation of British Columbia, 2024 BCSC 964

Read the case details

Facts

The Supreme Court of British Columbia assessed class-wide damages for a privacy breach by an employee of the Insurance Corporation of British Columbia (ICBC) who improperly accessed and sold the personal information of certain ICBC customers. Some of that information was used to carry out arson and shooting attacks on houses and vehicles belonging to some of these customers.

Decision

At an earlier stage of the proceedings, ICBC was held vicariously liable for its employee's breach of the *Privacy Act (BC Privacy Act)*. The class included all individuals residing at a home impacted by the privacy breach.

The Court awarded each class member nominal damages of $15,000, regardless of the actual harm individual class members had suffered. The Court found that this amount fell within the category of a modest or nominal award, based on the severity of the breach, the public purpose of the legislation, and the need for accountability. The Court rejected ICBC's proposed $500 damages award on the basis that it would trivialize the privacy interest that was violated, and render the cause of action under the *Privacy Act* effectively meaningless. Individual damages will be assessed at a later stage.

Key takeaway

Nominal damages for breaches of privacy legislation may be awarded, and the amount of such damages may — in appropriate circumstances — rise to a material amount in order ensure the protection of vulnerable information and clarify the consequences for any failure to do so. A defendant's motives in breaching an individual's privacy, including personal financial gain, and the fact that information was deliberately shared with criminals, increases the severity of the breach of privacy and the potential sanctions.

G.D. v. South Coast British Columbia Transportation Authority, 2024 BCCA 252

Read the case details

Facts

The Court of Appeal of British Columbia provided clarity on the liability of data custodians in the event of a data breach. This case involved a data breach by malicious third-party hackers who accessed employee's sensitive personal information, including social insurance numbers, banking information, birth dates, and addresses. The proposed class proceeding was filed on behalf of affected individuals against TransLink, the database custodian, alleging it had acted recklessly in failing to prevent the data breach.

Decision

The *BC Privacy Act* creates a cause of action for willful breaches of privacy. At certification, the chambers judge struck the plaintiff's *BC Privacy Act* claims on the basis that the defendant, even if reckless, did not willfully breach the class member's privacy by failing to prevent a third party from accessing their information without authorization. The B.C. Court of Appeal overturned this decision, holding that it is at least arguable that a data custodian who fails to adequately safeguard personal information, could be liable for a wilful violation of privacy.

The chambers judge also struck the plaintiff's claim in negligence on the basis that it was premised on a breach of the *Freedom of Information and Protection of Privacy Act* (BCFIPPA), as the BCFIPPA does not create a cause of action. The Court found that the negligence claim was not bound to fail, holding that the alleged breaches of BCFIPPA were relevant context and did not preclude TransLink from owing a common law duty of care to its employees and customers regarding the protection of their personal information.

The Court of Appeal remitted the question of whether to certify the proceedings to the chambers judge.

Key takeaway

Database custodians may be liable under privacy legislation for recklessly failing to prevent unauthorized access to sensitive personal information, even if there is no intentionality or involvement in the underlying breach. This arguably stands in contrast to the common law tort of intrusion upon seclusion, which Ontario courts have held does not apply to database custodians.

The case also clarifies that breaches of legislative or privacy regimes which do not themselves provide for a free-standing cause of action may nonetheless be relevant to whether a defendant's failure to prevent a data breach was "willful" conduct for the purposes of claims under the applicable privacy legislation.

Campbell v. Capital One Financial Corporation, 2024 BCCA 253

Read the case details

Facts

The British Columbia Court of Appeal recently provided guidance regarding breach of confidence and negligence claims in a class action arising from a data breach affecting individuals who had applied for or held credit cards issued by Capital One.

Decision

The decision addressed which causes of action were viable in the context of a data breach class action. The plaintiff appealed the certification judge's decision to strike his claims for breach of confidence and the common law tort of intrusion upon seclusion. The defendants cross-appealed the certification of the provincial statutory privacy torts, negligence, breach of contract, and breach of consumer protection claims.

The plaintiff had alleged that the hacker was liable for the tort of intrusion upon seclusion and provincial privacy legislation, and that Capital One was jointly liable for any moral damages caused by the hacker by virtue of British Columbia's *Negligence Act* (BC Negligence Act). The Court of Appeal disagreed, holding that the BC Negligence Act cannot be used to make a negligent party jointly liable for damages that they could never have been responsible for if they had acted alone. As the moral damages recoverable under the common law tort or under privacy legislation are different in kind from the damages that are recoverable in negligence, Capital One could not be held jointly liable for the moral damages caused by the hacker. The Court of Appeal declined to answer whether the tort of intrusion upon seclusion is recognized in British Columbia.

The Court of Appeal further struck the plaintiff's claim for breach of confidence on the basis that the defendant had wrongfully retained customer information. The tort of breach of confidence requires the plaintiff to establish a detriment resulting from the broken confidence. However, the plaintiff had only alleged harm resulting from the hacker's actions, not from any misuse of information by Capital One. This was not sufficient to maintain a claim for breach of confidence.

The Court of Appeal however upheld the remaining causes of action, including claims under provincial privacy legislation, negligence, breach of contract, and breach of consumer protection legislation.

Key takeaway

A plaintiff may not use the BC Negligence Act to recover moral damages that a hacker may be liable to pay under provincial privacy legislation or the tort of intrusion upon seclusion from a database defendant who negligently failed to prevent the same data breach.

A breach of confidence claim against a database defendant premised on the defendant having wrongfully retained information may be struck where there is a failure to plead a distinct detriment resulting from the alleged misuse.

The case also highlights the uncertainty that remains around the viability of statutory claims advanced against a database defendant in the context of a breach caused by a third-party intrusion. At the very least, such claims are likely to survive preliminary challenges.

Individuals' privacy interests

Canada (Privacy Commissioner) v. Facebook, Inc., 2024 FCA 140

Read the case details

Facts

The Privacy Commissioner of Canada (the Commissioner) filed a federal lawsuit against Facebook in 2020, after concluding in an investigation that Facebook had failed to safeguard user information or obtain valid consent for disclosing data to third-party apps hosted on its platform. The proceeding arose from the Commissioner's investigation into the scraping of Facebook user data by the app "thisisyourdigitallife". At first instance, the Federal Court dismissed the Commissioner's application, finding that the Commissioner had not shown that Facebook failed to obtain meaningful consent from users for disclosure of their data, nor that Facebook failed to adequately safeguard user data. The Court also held there was a lack of subjective evidence about Facebook users' expectations and understandings of privacy. This led to the Court finding "itself in an evidentiary vacuum."

Decision

The Federal Court of Appeal allowed the appeal, finding that the lower court erred in its analysis of meaningful consent and safeguarding under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Specifically, the Federal Court of

Appeal found that the Federal Court erred by premising its conclusion exclusively or in large part on the absence of expert and subjective evidence. Further, the Federal Court of Appeal found that the lower court failed to inquire into the existence or adequacy of the consent given by *friends* of users who downloaded third-party apps, separate from the installing users of those apps. The Federal Court of Appeal found that the friends were not given the opportunity to consider the third-party app's data policies on an app-by-app basis before disclosure and could not have understood the purposes for which their data would be used by the apps. Although Facebook's Data Policy — to which all users agreed — contained terms explaining how and when third-party apps could access their data, the Federal Court of Appeal found that the language was too broad to be effective as meaningful consent because a user reading the terms could not "sufficiently inform themself of the myriad ways that an app may use their data, and thus could not meaningfully consent to future disclosures to unknown third-party apps downloaded by their friends."

Key takeaway

This case includes an extensive analysis of the principles of meaningful consent and safeguarding under PIPEDA.

Parker v. Ontario Medical Association, 2024 FC 667

Read the case details

Facts

The applicants, three physicians, sought judicial review under section 14 of the PIPEDA concerning a study commissioned by the respondent Ontario Medical Association (OMA) regarding physicians' overhead costs. The study would involve the OMA disclosing physicians' first name, last name, date of birth, gender, primary address, and specialty to Statistics Canada. The applicants were members of the Ontario Specialists Association (OSA). The OSA filed a complaint with the Office of the Privacy Commissioner of Canada (OPC), alleging that the OMA's proposed study would contravene section 6.1 and Principle 4.3 of PIPEDA. The OPC dismissed the complaint on the basis that the study would not constitute "commercial activity" within the meaning of the PIPEDA and was therefore beyond the scope of the legislation. Additionally, the OPC found that it did not have jurisdiction to investigate the complaint. The physicians brought an application to the Federal Court seeking judicial review of the OPC's decision.

Decision

The Court dismissed the judicial review application, finding that the proposed study was not "commercial activity" within the meaning of PIPEDA. Consequently, PIPEDA did not apply. Justice Fothergill found that the information that the OMA wished to disclose to Statistics Canada constituted "personal information" under PIPEDA because the information was intended to permit the identification of the individuals. However, the Court held that the disclosure of physicians' personal information to Statistics Canada would not amount to "commercial activity" because it would not involve the "exchange, trade, buying and selling" of anything. The proposed study was intended to support negotiations with the government leading to a Physician Services Agreement (PSA), which sets billing rates for healthcare services across the province of Ontario. The OMA would derive no profit or financial benefit from the proposed study or the negotiation of the PSA. Additionally, the OMA does not act on behalf of the government in receiving or paying physicians' invoices, nor does it refer patients to physicians for treatment. The study's purpose was to provide insight into physicians' overhead costs and promote greater "income relativity" in the next PSA.

Key takeaway

This analysis sheds light on what will — and will not — amount to "commercial activity" within the meaning of PIPEDA. For example, the sharing of personal information may not amount to "commercial activity" if the disclosing organization does not derive a profit nor financial or other benefit from the disclosure.

Cyberattacks and data breach: reports

PIPEDA Findings No. 2024-002, Re, Office of the Privacy Commissioner of Canada

Read the case details

Facts

A customer of an alarm monitoring company, Brinks Home (Brinks), filed a complaint with the Office of the Privacy Commissioner of Canada (OPC) after inadvertently viewing the personal information of other customers on Brinks' online portal. Shortly thereafter, Brinks changed the online portal settings to prevent the information from being displayed. OPC investigated to determine whether Brinks had adequate security safeguards in place, and whether Brinks complied with breach notification requirements under PIPEDA.

Decision

OPC found that Brinks had failed to adequately protect customers' personal information from unauthorized access, but had subsequently implemented technical and procedural mechanisms to prevent similar incidents from occurring in the future. And, ultimately, Brinks sold all of its individual customer accounts. For these reasons, OPC found the

safeguarding aspect of the complaint was well-founded and resolved. In determining whether Brinks complied with its breach notification requirements, OPC found that the personal information revealed could be considered sensitive, but the probability of misuse was low. The OPC concluded that the breach did not present a real risk of significant harm, and therefore did not require Brinks to notify the affected individuals or report the breach to OPC.

Key takeaway

This case highlights the importance of properly safeguarding personal information and the importance of taking active measures to mitigate possible harm if breaches of such information do occur.

A Medical Imaging Clinic, Re, Ontario Information and Privacy Commissioner

Read the case details

Facts

A medical imaging clinic notified the Information and Privacy Commissioner of Ontario (IPC) that it was the victim of a ransomware attack. The clinic paid the ransom in exchange for an encryption key that allowed the clinic to recover all affected files. IPC investigated to determine whether the clinic took reasonable steps to protect personal health information, and whether a review was warranted under the *Personal Health Information Protection Act*.

Decision

IPC found that the clinic had taken sufficient efforts to determine the scope of the breach, which included patient and employee information as well as billing codes. IPC also found that the clinic had provided the appropriate notice, by posting a physical notice at the clinic's entrance and information desk, as well as providing a "pop up" notice on its website. Further, the clinic sent notification letters to over 14,000 referring physicians and to the clinic's employees and healthcare partners. The clinic also took action in order to minimize the risks of such a breach reoccurring in the future. Remedial measures taken by the clinic included revising their password policy, creating a policy for identification and removal of dormant user accounts, and changing their approach to backups to ensure one is always offline and would remain uncompromised in the event of another breach. Based on these findings, IPC determined that a review was not warranted.

Key takeaway

This case demonstrates that reviews by IPC may be avoided or minimized if victims of ransomware attacks provide proper notice and take sufficient remedial measures to minimize future risks.

Vankoughtnett, Re, Saskatchewan Information and Privacy Commissioner

Read the case details

Facts

Four dentists operated a general dentistry clinic as sole proprietors engaged in a cost-sharing agreement. One of the four dentists left the cost-sharing agreement and took copies of the clinic's entire patient database with him. The remaining dentists contacted the Saskatchewan Information and Privacy Commissioner (IPC) with concerns. The IPC found it had jurisdiction to investigate the matter, and considered whether privacy breaches occurred, and whether the remaining dentists had adequately responded to the privacy breaches.

Decision

The IPC concluded that the departing dentist's collection of the entire patient database was not authorized by, and constituted a privacy breach under, *The Health Information Protection Act* (HIPA). The IPC found that the root cause of the privacy breach was a lack of technical safeguards used to protect personal information, as the departing dentist should not have been able to access the remaining dentists' patient information in the first place. For these reasons, the IPC found that the remaining dentists had failed to fulfill their duty to protect patients' personal health information under HIPA. The IPC also found that the remaining dentists had taken reasonable steps to contain this breach by reporting the breach to IPC and ensuring the departing dentist could not further access the database, but they had failed to take steps to notify the affected individuals. The updated Privacy Policy used by the dentists remaining in the cost-sharing agreement was also held to be inadequate, as it conflated the requirements of the PIPEDA with the requirements of HIPA.

Key takeaway

This case highlights the extent to which regulators expect medical professionals to take care to ensure that they are adequately protecting patients' personal health information and preventing unauthorized access.

Privacy class actions: biometric data

Homsy c. Google, 2024 QCCS 1324

Read the case details

Facts

The petitioner, an individual whose personal data was collected, sought the authorization of the Court to institute a class action against the respondent, Google. The petitioner claimed that the respondent had been extracting, collecting, storing and using facial biometric data of Québec residents via the Google Photos application, without providing sufficient notice, without obtaining informed consent and without publishing biometric data retention policies.

The petitioner sought compensatory damages under the *Act respecting the protection of personal information in the private sector* (Private Sector Act) and the CCQ. The petitioner was also seeking punitive damages under section 272 of the *Consumer Protection Act* (CPA) and section 49 of the *Charter of Human Rights and Freedoms* (Québec Charter).

Decision

The Court authorized the class action against Google.

The Court found that facial biometric data qualified as personal information under section 2 of the Private Sector Act. Therefore, Google's practice of extracting, collecting, storing and using facial biometric data of Québec residents and sharing the data to third parties without consent could be argued to breach sections 8, 10, 13, 14 and 17 of the Private Sector Act, as well as articles 35 and 37 of the CCQ.

According to the Court, Google's practice may be argued to have constituted a civil fault under article 1457 of the CCQ. The Court also authorized the common issue of determining whether Google voluntarily violated section 5 of the Québec Charter, which provides for the right to privacy. The petitioner was therefore authorized to seek punitive damages pursuant to section 49 of the Québec Charter, in addition to compensatory damages.

Finally, Google's Terms of Services showed that there was no mention of the extraction, collection, storage and use of members' facial biometric data. By making this omission, the respondent may have overlooked an important fact in its representations to consumers.

Key takeaway

Given plaintiff's low burden at the authorization stage of a Québec class action, allegations of use without a person's consent of biometric information may be sufficient to allow class action authorization claiming a violation of the right to privacy. When such alleged breach is done willfully, it may give rise to punitive damages, in addition to compensatory damages.

Lam v. Flo Health Inc., 2024 BCSC 391

Read the case details

Facts

The British Columbia Supreme Court certified a class action lawsuit against Flo Health Inc. (Flo), a company that makes an app for tracking women's reproductive health. The plaintiff alleges that Flo violated the privacy of its users by disclosing sensitive personal information to third parties without consent. The proposed class included all users across Canada, excluding Québec.

Decision

The Court-certified common issues relating to breach of statutory privacy legislation, intrusion upon seclusion (except for class members residing in B.C. and Alberta), breach of confidence, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The Court, however, struck the claims of negligence, unjust enrichment, breach of provincial consumer protection legislation, conversion, and for B.C. and Alberta residents, intrusion upon seclusion.

The Court rejected Flo's arguments that the plaintiff's claims were barred by exclusion of liability and waiver of class actions clauses in its terms of use, because these provisions were unconscionable and contrary to public policy.

Key takeaway

The decision affirms that class action waiver clauses in consumer contracts will generally be unenforceable in British Columbia.

Breach of confidence uses a broad concept of detriment and does not require a plaintiff to plead an economic loss or a serious and prolonged psychological upset.

While a breach of PIPEDA does not in itself create a cause of action, such breaches may be relevant context for other causes of action.

Expectation of privacy

R. v. Bykovets, 2024 SCC 6

Read the case details

Facts

The appellant, Bykovets, was convicted of credit card fraud. During their investigation, law enforcement authorities obtained from Moneris, a third-party payment processing company, the IP addresses used for the appellant's transactions. This was done without prior judicial authorization.

The appellant alleged that the police's request to Moneris violated his right against unreasonable search and seizure under section 8 of the *Canadian Charter of Rights and Freedoms*, Part I of *The Constitution Act*, 1982, Schedule B to the *Canada Act 1982* (UK), 1982, c. 11 (Canadian Charter). The issue before the Supreme Court was whether an individual had a reasonable expectation of privacy of their IP address.

Decision

The majority of the Supreme Court allowed the appeal and ordered a new trial, holding that an individual's IP address is protected under section 8 of the Canadian Charter. Law enforcement authorities are therefore required to obtain judicial authorization before obtaining an IP address from a third party.

The Court interpreted section 8 of the Canadian Charter in a broad and purposive manner. Defining a "reasonable expectation of privacy" is an exercise of balance. In this case, the balance weighs in favour of extending a reasonable expectation of privacy to IP addresses. The highly private nature of the information an IP address may divulge, strongly suggests that the public's interest should prevail over the government's interest in advancing its goals in law enforcement.

The Internet has exponentially increased both the quality and quantity of information stored about Internet users. It has allowed private corporations to track users, and to build profiles containing information the users do not know they are revealing. By concentrating this mass of information with private third parties, the Internet has altered the topography of privacy under the Canadian Charter. It has added a third party to the constitutional ecosystem, making the horizontal relationship between the individual and the state tripartite.

While the third parties are not subject to section 8 of the Canadian Charter, they mediate a relationship which is directly governed by it — that between defendant and police. Judicial oversight is therefore appropriate to remove from private corporations the decision of whether to reveal information and, if so, how much to reveal.

The dissenting judges would have denied the appeal since they concluded that the appellant did not have a reasonable expectation of privacy of his IP addresses. Accordingly, the police would not have needed judicial authorization.

Key takeaway

A reasonable expectation of privacy includes protections to an individual's IP address, and is therefore protected under section 8 of the Canadian Charter. Prior judicial authorization is therefore required to obtain an IP address from a third party.

Access to information

Excavation National inc. c. Autorité des marchés publics, 2024 QCCS 2159

Read the case details

Facts

The plaintiff, Excavation National, is a construction company operating in Québec. The defendant, the Autorité des marchés publics (AMP), is a public body overseeing public procurement and the application of regulations governing public contracts in Québec.

On November 16, 2023, the AMP issued a decision refusing to authorize a contract between Excavation National with a public body, and registering it as ineligible for public contracts in Québec.

The plaintiff sought judicial review of the AMP's decision, and broad disclosure of AMP's file. It argued that the full file was necessary for the Court to decide on the legality of AMP's decision. The plaintiff concurrently filed an access to information request with AMP. The AMP refused to transmit the requested documents and deferred the decision regarding the access request.

Decision

The Court rejected the plaintiff's requests, concluding that the disclosure of the AMP's complete file constituted a fishing expedition. In particular, an assessment of the legality of the decision did not require the Court to have the AMP's complete file, particularly in light of the detailed reasons provided to Excavation National.

Key takeaway

In the context of the judicial review of an administrative decision made by a public body, fishing expeditions in the form of an access to information request to obtain the complete file of the decision-maker will not be granted. The Court will only order the disclosure of additional documents or evidence when it is necessary to assess the reasonableness of the administrative decision.

Gravel c. Agence du revenu du Québec, 2024 QCCQ 1589

Read the case details

Facts

The appellant, Gravel, was investigated by the provincial tax authority, Agence du revenu du Québec (ARQ). The appellant filed an access to information request with the ARQ, seeking various documents and information, including a list of ARQ employees who had access to the appellant's tax file. The ARQ refused to deliver said documents. The Commission d'accès à l'information (Commission) partially granted the appellant's application for review of the ARQ's decision. The ARQ destroyed some data related to Gravel's request in the period between the ARQ's refusal to deliver the documents and the Commission's decision. The destruction of the data made it impossible to generate the requested list of employees.

The Commission concluded that the destruction of the data did not constitute a breach of section 52.1 of the *Act respecting Access to documents held by public bodies and the Protection of personal information* (Access Act) since what was destroyed was not a document, but data that made it possible to generate the requested document. Gravel appealed the Commission's decision to the Court of Québec.

Decision

The Court allowed the appeal and quashed the Commission's decision.

The Court concluded that the Commission erred in law and failed to follow established case law when it concluded that the computer data that corresponded to the access request held by the ARQ was not a document.

The Court interpreted section 1 of the Access Act and determined that just because a query must be entered into ARQ's system to generate a document does not mean that the document does not exist. The only exception to this rule is when calculations or comparisons are necessary such that a new document is generated.

Therefore, the court determined that the ARQ had possession of the requested document within the meaning of section 1 of the Access Act at the time the request for access was made by Gravel. The ARQ had an obligation to keep the document pending any recourse in accordance with sections 52.1 and 102.1 of the Access Act. By destroying the data, the ARQ failed to comply with its document retention obligations under sections 52.1 and 102.1 of the Access Act.

Key takeaway

Computer data might constitute a document in the context of responding to an access to information request. The only exception is when calculations or comparisons are to be made such that a new document is generated. Computer data must be maintained where it is the subject of an access to information request and subsequent appeal.

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

Read the case details

Facts

In this case, the Supreme Court of Canada considered the scope of cabinet confidentiality in the context of an access to information request under Ontario's *Freedom of Information and Protection of Privacy Act* (OFIPPA).

A journalist had made an access to information request for 23 "mandate letters" from the Premier of Ontario to his ministers shortly after forming government in 2018. The Cabinet Office declined the request claiming the mandate letters were documents that would reveal the substance of cabinet deliberations and were thus exempt from disclosure under subsection 12(1) of OFIPPA. The Ontario Information and Privacy Commissioner (OIPC) found the letters were not exempt and ordered their disclosure. The Ontario Divisional Court overturned the decision on judicial review, holding that the letters were exempt. The Ontario Court of Appeal upheld the Divisional Court's decision.

Decision

The Supreme Court unanimously held that the mandate letters were exempt from disclosure. Justice Karakatsanis wrote the majority opinion, while Justice Côté wrote a concurring opinion that agreed in result with the majority but disagreed with their approach to the standard of review of the OIPC's decision.

The majority held that the OIPC had failed to appropriately grapple with the broader legal and factual context of subsection 12(1) OFIPPA. In particular, the OIPC failed to appreciate the constitutional conventions and traditions governing Cabinet confidentiality and Cabinet's deliberative process. In a constitutional democracy, the confidentiality of Cabinet deliberations is a precondition to responsible government. It is necessary so ministers do not censor themselves in policy debates and can then later stand together in public, and be held responsible as a whole, once a policy decision has been made and announced.

The failure to account for this context led the OIPC to take an unreasonable narrow interpretation of subsection 12(1) such that it did not protect "outcomes" of cabinet deliberations and caused him to mischaracterize the mandate letters themselves as the end product of cabinet deliberations. The majority held that cabinet confidentiality includes the prerogative to determine when and how to announce Cabinet decisions. The mandate letters included unannounced policy priorities, which being not yet public, could be subject to further debate and thus change through cabinet deliberations. The mandate letters were thus subject to Cabinet confidentiality and exempt from disclosure under subsection 12(1) of OFIPPA.

The majority reviewed the OIPC's decision on a reasonableness standard, as that was the standard argued by the parties. Justice Côté wrote that the decision must be reviewed on a correctness standard because Cabinet privilege is a question of central importance to the legal system as a whole.

Key takeaway

Disclosure exemptions under access to information legislation must be interpreted in their broader legal and factual context, including relevant constitutional norms and conventions.

Cabinet privilege is a foundational constitutional principle, and access to information exemptions intended to protect Cabinet privilege should be interpreted broadly.

Cabinet privilege includes the government's right to choose when and how to announce Cabinet decisions. Unannounced Cabinet decisions may thus be exempt from disclosure under access to information legislation.

Miville de Chêne c. Québec (City of), 2024 QCCAI 127

Read the case details

Facts

The petitioner submitted an access request to the City of Québec, the respondent, seeking access to documents related to a 2011 management agreement and a commercial lease (the Agreements) relating to the operation of the Centre Vidéotron. Numerous third parties were involved in the Agreements.

In particular, the petitioner requested access to financial statements from 2015 onward. The City of Québec refused to disclose these documents, claiming it did not have legal possession of them, as the documents belonged to the third parties and were not physically or legally held by the City.

Decision

The Commission concluded that the financial statements were not in the legal possession of the City. Although City of Québec employees had access to these statements during biannual visits, the records were produced by third parties for their own use, not for the City's purposes. In reaching its decision, the Commission considered that the statements were provided to the City for verification purposes only and that it did not have control over the documents or the ability to request them at any time. Additionally, the Commission confirmed that City of Québec was not attempting to evade responsibility by not physically holding the documents.

Key takeaway

Organizations do not have legal possession of documents simply because they have access to them for verification purposes, if they do not have control over the documents.

Privacy and employment

York Region District School Board v. Elementary Teachers' Federation of Ontario, 2024 SCC 22

Read the case details

Facts

The appellant, the York Region District School Board, represents an Ontario public school. The respondent, the Elementary Teachers' Federation of Ontario, represents two teachers employed by an Ontario public school.

Two teachers recorded their private communications regarding workplace concerns on a shared personal, password-protected log stored in a cloud. The school principal entered the classroom of one of the teachers and, in her absence, scrolled through the document and took screenshots with his cellphone. These communications then formed the basis for the school board to issue written reprimands. The teachers' union grieved the discipline, claiming that the search violated the teachers' right to privacy at work. An arbitrator concluded that there was no breach of the teachers' reasonable expectation of privacy when balanced against the school board's interest in managing the workplace.

The issue of whether employees have a right against unreasonable search and seizure in a workplace environment pursuant to section 8 of the *Canadian Charter of Rights and*

Freedoms, Part I of *The Constitution Act, 1982*, Schedule B to the *Canada Act 1982* (UK), 1982, c. 11 (Canadian Charter) was brought before the Ontario Court of Appeal. The Court of Appeal held that the search was unreasonable under section 8 of the Canadian Charter. The appellant appealed this decision, mainly on the basis that the Canadian Charter does not apply to Ontario's public school boards.

Decision

The Supreme Court dismissed the appeal.

According to the majority of the Supreme Court, Ontario teachers are protected by section 8 of the Canadian Charter and thus have a right against unreasonable search and seizure in their workplace.

Section 32 of the Canadian Charter sets out the scope of its application. The Canadian Charter applies to the government but can also be extended to other entities. It is the case when an entity either by its very nature, or, in virtue of the degree of governmental control exercised over it, can be characterized as "government" within the meaning of section 32 of the Canadian Charter.

The majority of the Supreme Court concluded that the Canadian Charter applies to Ontario public school boards because they are considered as inherently governmental for the purpose of section 32. This is so because public education, by its very nature, is a governmental function and Ontario public school boards are manifestations of government. It follows that all actions carried out by Ontario public school boards are subject to the Canadian Charter.

The concurring judges agreed with the applicability of the Canadian Charter to public school boards.

Key takeaway

The Supreme Court confirmed that the Canadian Charter applies to Ontario's public school boards. However, it left open the question of the applicability of the Canadian Charter to public schools in other provinces.

Pelletier c. Transvrac Montréal Laval inc., 2024 QCCAI 102

Read the case details

Facts

Pelletier, the petitioner, submitted an access request to her former employer, Transvrac Montréal Laval Inc., seeking access to her personal emails and contacts stored in her professional email account. Prior to her departure, an automatic transfer rule had been set up that forwarded her personal emails to her professional email account.

This led to a mixture of personal and professional emails in her work inbox. After her employment ended, Transvrac migrated her professional email account to the general manager's Outlook account.

Transvrac raised concerns about the burden of processing the request, requiring the review of over 5,000 emails. The company also raised that the contact list contained third-party information that should be protected under the *Act respecting the protection of personal information in the private sector.*

Transvrac asked the Commission to dismiss the petitioner's access request on the grounds that it was abusive.

Decision

The Commission concluded that Transvrac was indeed required to review all emails in the petitioner's former professional email account, which had been transferred to the general manager's account.

However, the Commission ultimately granted Transvrac's request to be exempted from processing the access request. It found that, while made in good faith, the petitioner's request was abusive due to the extensive volume of documents involved, and the effort required to separate personal from professional communications. The Commission considered the company's limited resources, noting that requiring the general manager to manually review over 5,000 emails and 2,000 contacts was unreasonable given the company's small size and workforce.

Key takeaway

When employees use their professional email accounts for personal communications, it can complicate a company's obligations when responding to access to information requests. In deciding the company's obligations in that regard, the court might consider the volume of documents involved, the effort necessary to separate personal and professional emails and the company's resources.

Martineau c. Telus, 2024 QCCAI 200

Read the case details

Facts

Martineau, the petitioner, requested access to several documents from her former employer, including her payroll records, time sheets, and the final report from a psychological harassment investigation. The investigation had been conducted under the *Canada Labour Code* and the *Work Place Harassment and Violence Prevention Regulations* (the Regulations). Of particular importance was subsection 30(2) of the Regulations, which require that the investigator's report must not reveal, directly or indirectly, the identity of persons who are involved in an investigation or the resulting resolution process.

Telus provided some documents but withheld others. In particular, it redacted portions of the final harassment investigation report on the basis of section 40 of the *Act respecting the protection of personal information in the private sector* (Private Sector Act), arguing that the redacted information contained personal data about third parties, and its disclosure could cause significant harm to those individuals.

Decision

The Commission d'accès à l'information (Commission) clarified that its jurisdiction did not extend to enforcing section 30 of the Regulations.

On the basis of section 40 of the Private Sector Act, the Commission ruled that Telus was justified in withholding portions of the report that contained personal information about third parties, as disclosing such information could lead to serious harm, including reputational damage and workplace retaliation. However, the Commission ordered Telus to release the parts of the report that contained Martineau's own personal information, as these did not fall under the protection of section 40.

Key takeaway

Organizations can be justified to redact personal information regarding third parties under the exception of section 40 of the Private Sector Act when there is a risk of significant harm, including reputational damage and workplace retaliation.

Jurisdiction of privacy authorities

Forest c. Bell, 2024 QCCAI 202

Read the case details

Facts

In November 2021, Forest, the petitioner, subscribed to various services from Bell, the respondent, including residential phone services. At that time, he was informed that only his first initial and last name, "Forest, S.," would be listed in the directory alongside his phone number. The transaction summary confirmed this under the "Directory listing" section.

On March 28, 2023, Forest discovered that his full name, address, and phone number were publicly displayed on the website Canada411.ca. He contacted Bell's customer service, expressing his lack of consent for this disclosure and requesting that his personal information stop being shared with third parties, such as the Yellow Pages. Forest also highlighted a security concern related to his profession, stressing that the public dissemination of his personal details posed a risk.

As he still had not received satisfaction regarding his requests, on April 28, 2023, Forest submitted a request for a review of the disagreement to the Commission d'accès à l'information (Commission). In addition to his proceedings before the Commission,

Forest also filed a claim before the Small Claims Division of the Court of Québec, seeking similar injunctive relief to that requested before the Commission, along with a monetary claim for damages.

Decision

The Commission ruled that it had exclusive jurisdiction to address Forest's request for a review of the disagreement, despite the parallel proceedings in the Court of Québec.

Citing section 134.2 of the *Act respecting Access to documents held by public bodies and the Protection of personal information* (Access Act), the Commission emphasized that it alone had the authority to decide on matters related to disputes over personal information under the *Act respecting the protection of personal information in the private sector* (Private Sector Act).

The Commission dismissed Bell's argument of lis pendens, noting that it retained the authority to examine and resolve Forest's request, regardless of the ongoing court proceedings. The Commission proceeded to review Forest's complaint and concluded that Bell had complied with his original request by ensuring that only "Forest, S." and his phone number would appear in the directory.

Key takeaway

The Commission holds exclusive jurisdiction over disputes concerning personal information under the Private Sector Act, even if similar issues are being addressed in other courts. Claims of lis pendens do not prevent the Commission from ruling on matters that fall within its jurisdiction.

Privacy in injunction proceedings

Boisvert Marine inc. c. Dumas, 2024 QCCS 3240

Read the case details

Facts

The plaintiff, Boisvert Marine Inc. (BMI), operates a wholesale business in leisure and sporting goods, specializing in the sale and repair of boats. The defendant, Dumas, is the general manager of BMI, which enabled him to purchase replacement parts and pay suppliers directly on behalf of BMI, using its funds.

BMI became aware of suspicious transactions involving Dumas. BMI alleged that Dumas diverted more than $3 million for his personal benefit in part by modifying BMI's bank statements.

BMI sought Mareva and Norwich orders from the Court, as well as an order to have a USB key verified by a forensic investigator.

Decision

The Court granted the Mareva and Norwich orders, and the verification of the USB key by a computer expert.

The Norwich order compelled third-party financial institutions to disclose documents in their possession that would allow BMI to trace the funds that Dumas had diverted. The Court determined that BMI satisfied the criteria for a Norwich order: (1) a bona fide claim against the unknown alleged wrongdoer; (2) the person from whom discovery is sought must be involved in the matter under dispute, he must be more than an innocent bystander; (3) the person from whom discovery is sought must be the only source of information available to the applicants; (4) the person from whom discovery is sought must be reasonably compensated for expenses arising out of compliance with the order, plus legal costs; and (5) the public interest in favour of disclosure must outweigh legitimate privacy concerns.

Regarding the last criterion, the right to privacy is provided for in articles 3, 35, 36 and 37 of the CCQ, and section 5 of the Charter of human rights and freedoms. The Court determined that, while a person's legitimate expectation of privacy deserves special consideration, it will not act as a bar to a Norwich order.

Key takeaway

The right to privacy does not constitute a bar to the issuance of a Norwich order.

De Trinidad c. Chambre de la sécurité financière, 2024 QCCAI 195

Read the case details

Facts

The petitioner, de Trinidad, a financial security advisor and registered member of Québec's Chamber of Financial Security (CSF), was the subject of a disciplinary investigation in 2016. On May 25, 2018, he was interviewed at the CSF's offices, and the interview was recorded. The recordings were stored in the CSF's IT system, and a DVD copy was provided to him.

In 2019, de Trinidad reviewed the DVD in preparation for his disciplinary hearing and claimed that certain parts of the recording — where the investigators allegedly threatened him — were missing. He requested access to the original recordings, but the CSF informed him that the storage unit containing the original files had been damaged during a power outage in 2018, resulting in the permanent loss of the original files. De Trinidad believed these original recordings were crucial to proving that the CSF had falsified evidence and therefore submitted an access request seeking documents related to the CSF's technological infrastructure and the power outage incident.

The CSF denied the request on the basis of sections 14 and 29 of the *Act respecting Access to documents held by public bodies and the Protection of personal information* (Access Act). The CSF argued that the requested documents contained sensitive information about its technological infrastructure, including system configurations and vulnerabilities, and disclosing them could compromise the security of its systems.

Decision

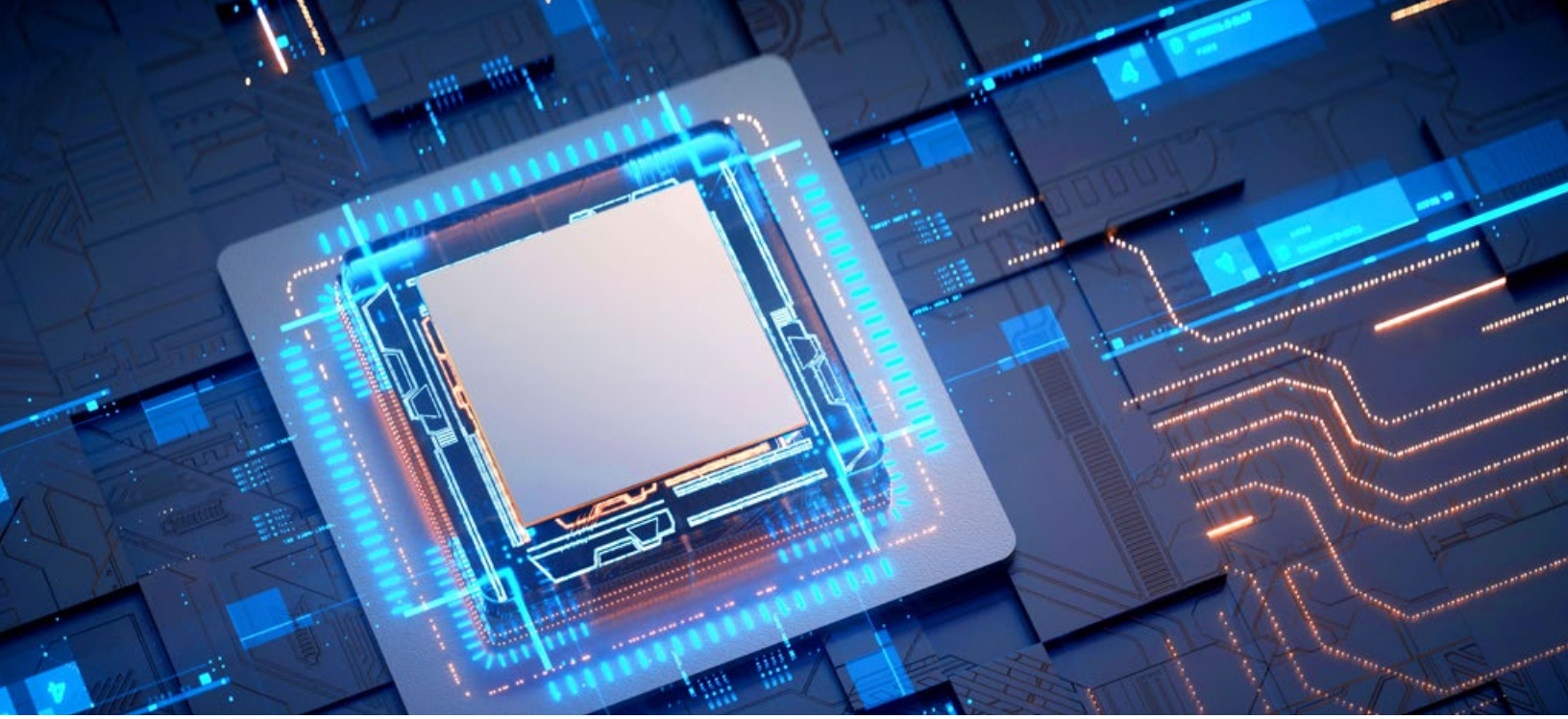
The Commission d'accès à l'information (Commission) ruled in favor of the CSF, upholding its decision to withhold the requested documents under sections 14 and 29 of the Access Act.

The Commission agreed that the requested documents contained information that could expose the CSF's systems to potential risks, such as cyber threats or unauthorized access, and thus that the security of CSF's systems could be compromised by disclosing the information.

The Commission highlighted that the risk posed by revealing such information outweighed any investigative purpose de Trinidad had for accessing it.

Key takeaway

Organizations may lawfully refuse to disclose information related to their technological infrastructure if such disclosure poses a security risk, even when such information is requested for investigative or legal purposes.



AI and privacy

McMaster University (Re), 2024 CanLII 17583 (ON IPC)

Read the case details

Facts

The case concerns McMaster University's use of Respondus Monitor, an AI-enabled software for online exam proctoring, and Respondus LockDown Browser, a software which limits what students can access on their computers during an examination. McMaster adopted this technology during the COVID-19 pandemic to maintain academic integrity in a remote learning environment.

The Information and Privacy Commissioner of Ontario (IPC) investigated the university's compliance with the *Freedom of Information and Protection of Privacy Act* (the Act), particularly regarding the collection, use, and disclosure of students' personal information by Respondus Monitor.

Decision

The IPC found that Respondus LockDown Browser collected little personal information, and only collected and used what it needed to function. On the other hand, the IPC found that Respondus Monitor collected more sensitive personal information, including biometric information, and used artificial intelligence (AI) technology, which carried heightened concerns.

While the collection was authorized under subsection 38(2) of the Act, the IPC found that the university did not provide adequate notice for its collection of personal information as required by subsection 39(2) of the Act, and also found that the use of students' personal information through Respondus Monitor was not in compliance with subsection 41(1).

Moreover, the IPC concluded that the contractual arrangement between the university and Respondus was contrary to subsection 41(1) of the Act as it did not adequately protect all personal information collected, and because it allowed Respondus to use personal information for system improvement purposes without the consent of students.

The IPC made several recommendations for the university to bring itself into compliance with the Act and recommended that the university adopt additional guardrails around its use of Respondus Monitor and incorporate stronger protections into its ongoing use of the software and any future agreement with Respondus.

Key takeaway

Institutions using software such as Respondus Monitor must ensure that adequate notice is provided to data subjects when their information is being collected. They must also ensure that contracts with third-party service providers adequately protect the personal information collected, and prohibit any uses of the personal information by the service provider absent the consent of the data subjects.

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