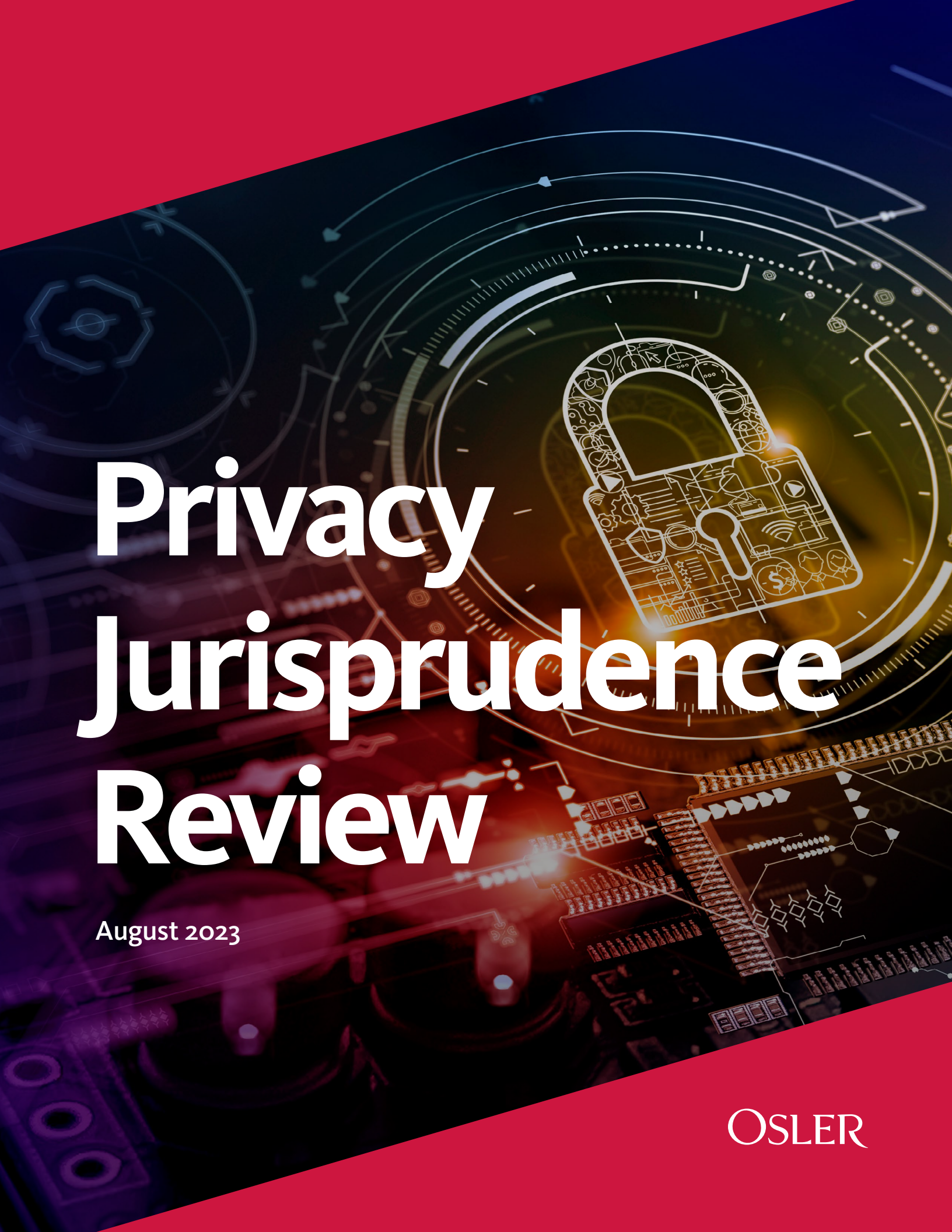

Privacy Jurisprudence Review

August 2023

OSLER

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.

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.

Special thanks to all the Osler associates involved in authoring these case summaries for their valuable contribution.

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

Table of Contents

PRIVACY AND EMPLOYMENT

PRIVACY IN THE DISPUTE RESOLUTION PROCESS

INDIVIDUALS' PRIVACY INTERESTS

Privacy class actions: Data breaches

In a trilogy of privacy class action certification appeals, the Ontario Court of Appeal (ONCA) refused to certify three class actions based on the tort of intrusion upon seclusion first recognized in *Jones v. Tsige*. In June 2022, the Court heard the three appeals consecutively, and released its decisions together in November 2022. The Court held that defendants who collect and store personal information of individuals (the Database Defendants) cannot be held liable under the intentional tort of intrusion upon seclusion in the context of a data breach by a third-party hacker.

In each of these cases, the plaintiffs sought to certify class proceedings against Database Defendants who had experienced a data breach where threat actors hacked the defendants' computer networks and compromised their data, including the personal information of proposed class members. In addition to claims of negligence and breach of contract, the plaintiffs alleged the Database Defendants were also liable for intruding on the plaintiffs' privacy.

On the claims pleaded, the ONCA found the Database Defendants did not do anything that could constitute an act of intrusion or invasion into the privacy of the plaintiffs. The alleged intrusions were committed by unknown third-party hackers, acting independently from, and to the detriment of, the interests of the Database Defendants. None of the facts pleaded could, in law, provide a basis upon which the actions of the hackers could be attributed to the Database Defendants. Further, none of the material facts pleaded indicated that the Database Defendants acted in consort with, or were vicariously liable for, the hackers' conduct.

In recent years, claimants have attempted to expand the application of the intentional tort of intrusion upon seclusion to cybersecurity and have sought to have class actions certified on that basis. This privacy trilogy from the ONCA is a clarification of the scope of the tort and makes clear that liability can only attach to a party who is an active participant in the wrongful access of private information of another. While the Court of Appeal has effectively narrowed the scope for future privacy class actions against database defendants, reckless protection of information or wilful blindness to inadequate cybersecurity measures could impose liability onto corporations for other torts, such as negligence.

Owsianik v. Equifax Canada Co., 2022 ONCA 813

Read the case details

Facts

Owsianik was the first of the three cases to be heard by the lower courts. The representative plaintiff pleaded that Equifax's "reckless" data management practices constituted an intrusion that would be highly offensive to a reasonable person. A data breach by hackers provided unauthorized access to the personal information stored by Equifax, including individuals' social insurance numbers, names, dates of birth, addresses, driver's licence numbers, credit card numbers, email addresses and passwords.

Decision

At first instance, the court certified the claim for intrusion upon seclusion finding that it was not plain and obvious that the tort could not succeed at trial. That decision was reversed, however, by a majority of the Divisional Court who found that there was no possibility of establishing the tort where the Database Defendants were not alleged to have committed the wrongful intrusion themselves.

Key Takeaway

In dismissing the appeal, the ONCA reviewed the three elements of the tort of intrusion upon seclusion: (1) conduct; (2) state of mind; and (3) consequence. The ONCA held that the plaintiffs' claim failed at the "conduct" stage of the analysis. The ONCA found that the defendants had not committed any conduct that amounted to an invasion of or intrusion on the plaintiffs' privacy. The defendants' wrongdoing, if any, rested in their failure to prevent hackers from carrying out an invasion of privacy. The Court reasoned that liability would properly be pursued under the tort of negligence, or under a breach of contract or other statutory duty. Since neither Equifax nor anyone acting on Equifax's behalf, or in consort with them, unlawfully accessed any information, to impose liability on Equifax for the tortious conduct of the unknown hackers would create a new and potentially very broad basis for a finding of liability for intentional torts.

Obodo v. Trans Union of Canada, Inc., 2022 ONCA 814

Read the case details

Facts

Like Equifax, Trans Union accumulated and stored its customers' personal information in its database for purposes of providing credit-related services. As in *Owsianik*, the database was breached by unknown third-party hackers. At first instance, the motion judge certified the proposed class proceeding in relation to the claims in negligence, as well as certain statutory claims, but declined certification of the intrusion upon seclusion claims on the basis of the Divisional Court's reasoning in Owsianik.

Decision

The plaintiff appealed directly to the Court of Appeal in relation to this latter aspect of the ruling. The ONCA ultimately upheld the dismissal of the proposed certification of the intrusion upon seclusion claims on the basis that the tort had "nothing to do" with a Database Defendant (with cross-reference to the reasons delivered in the *Owsianik* appeal). In the *Obodo* reasons, the ONCA also addressed the plaintiff's additional arguments in relation to vicarious liability, concluding that Trans Union was not vicariously liable for the hackers' conduct because such liability rests primarily on policy considerations which are, in turn, predicated on the existence of an employer-employee relationship and a connection in some sense between that relationship and the employee's tortious misconduct.

Key Takeaway

This relationship is a precondition to the imposition of vicarious liability and without it, the claim fails.

Winder v. Marriott International, Inc., 2022 ONCA 815

Read the case details

Facts

In *Winder*, third-party hackers accessed Marriot's reservation database which contained customers' personal information, such as passport numbers and payment information. Unlike the claims in *Owsianik* and *Obodo*, this claim alleged that Marriott invaded its customers' privacy when it collected and stored their personal information in a manner that (i) did not reflect the representations Marriott had made to them and (ii) did not meet Marriott's legal obligations in respect of maintaining the security of the information. The claimants alleged that these legal obligations included contractual and statutory obligations, as well as obligations imposed by industry standards and practices. The claimants attempted to argue that obtaining the customers' personal information deceptively by false premises made it a "reckless" intruder, regardless of whether any third party ever actually gained access to the customers' information stored in the database.

Decision

The ONCA found that there was no allegation that Marriott accumulated, stored or used the personal information provided by its customers for any purpose other than the purposes reasonably contemplated by the customers. Marriott's misconduct was not that it breached its customers' privacy rights, but that it failed to safeguard those privacy rights from intrusion by others. The only interference with the customers' ability to control access to and use of their personal information occurred when unknown third-party hackers breached Marriott's database. Until the hackers acted, there was no breach of the customers' privacy rights and no intrusion.

Key Takeaway

The plaintiffs in all three of these cases sought leave to appeal to the Supreme Court of Canada. Those applications were dismissed in July 2023.

Danny Lamoureux c. Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM), 2023 CanLII 24495 (CSC)

Read the case details

Facts

The appellant's class action was based on the loss of a laptop computer mistakenly left on a train by an IIROC inspector. The computer was never found. The information on the computer was password protected, but, despite internal policies put in place by the respondent to ensure greater protection, it was not encrypted. The computer contained the personal information of thousands of Canadian investors. The members composing the class alleged that the respondent's lack of security measures in place to protect their personal information caused a violation of their right to privacy, protected under article 5 of the Québec *Charter of Human Rights and Freedoms*.

Decision

The Supreme Court of Canada dismissed the application for leave to appeal from a judgment of the Court of Appeal of Québec which in turn dismissed an appeal from a Superior Court judgment. The lower court dismissed the class action after a full trial on the merits. No reasons were given for the Supreme Court's dismissal of the leave application. However, the Superior Court and Court of Appeal decisions were upheld.

The lower Courts had held that the fear and inconvenience experienced by members as a result of the loss of their personal information did not constitute compensable harm. Rather, they are akin to the normal inconveniences that any person living in society encounters and should be required to accept. The evidence did not support a finding that the computer or the class members' information was in the hands of a malicious person, nor was there a convincing link between the loss of the computer and the illicit uses alleged by the members. The defendant-respondent had reacted diligently, according to the standards expected in similar circumstances.

Key Takeaway

In the absence of demonstrated compensable harm, a corporation may successfully defend itself against claims following a data incident by reacting diligently to the incident.

Sciscente c. Audi Canada inc., 2022 QCCS 2911

Read the case details

Facts

The plaintiff sought authorization to bring a Canada-wide class action on behalf of those individuals in Canada whose personal information held by the defendants Audi Canada Inc. and Volkswagen Group Canada Inc. was compromised in a March 2021 data breach. The data breach compromised the personal information of 3.3 million customers throughout North America.

Decision

The Superior Court authorized the class action against Audi only, and only for Québec residents. None of the alleged facts could support a finding that the breach affected VW's customers in Canada, as the evidence provided related solely to customers located in the United States. The Court held that a sufficient demonstration of possible wrongdoing had been made out as against Audi, based in part on the amount of time that went by before the breach was noticed, and the subsequent delay in notifying customers.

Key Takeaway

The Québec courts require some evidence that Québec/Canadian customers were affected by a data incident. The plaintiff cannot rely solely on evidence that U.S. customers were affected.

Privacy and misuse of personal information

Option Consommateurs c. Flo Health Inc., 2022 QCCS 4442

Read the case details

Facts

In 2016, the defendant launched an app called "Flo" that allows women to track their menstrual cycle and ovulation periods. An investigative report revealed that unencrypted and personally identifiable and intimate information was transmitted by the defendant to Facebook. Following the publication of this report, the defendant changed its privacy policy, indicating that it would not share any personal data with third parties. The plaintiff sought authorization to bring a class action against the defendant on behalf of individuals in Québec who used the Flo application between June 1, 2016 and February 23, 2019. The plaintiff alleged that the defendant breached its contractual and statutory obligations with respect to the preservation of class members' personal information. The plaintiff was seeking compensatory damages (for material injury, relating to the infringement of the right to one's image) and punitive damages (under the Québec *Charter of Human Rights and Freedoms and Consumer Protection Act).*

Decision

The Superior Court authorized the class action. The defendant had admitted to transferring certain information it collected, including a "unique device identifier." The Court therefore found that it was not hypothetical or speculative to say that personal and highly sensitive information had been transferred to third parties who had used or may use it for purposes other than the technical operation of the Flo application. The extent to which the combined effect of the disclosure of information along with the unique device identifier allows for the personal identification of the user was held to be an issue to be examined on the merits of the class action.

Key Takeaway

The courts may, in some circumstances, authorize a class action even where there is some uncertainty as to whether the information disclosed is personally identifiable.

Canada (Privacy Commissioner) v. Facebook, Inc., 2023 FC 533

Read the case details

Facts

The Privacy Commissioner of Canada (OPC) investigated a complaint that a third-party application obtained Facebook users' personal data through the Facebook platform and disclosed it to another third party, Cambridge Analytica. The OPC issued a report concluding that Facebook had breached the *Personal Information Protection and Electronic Documents Act* (PIPEDA) by sharing Facebook users' personal information with third-party apps without the users' consent and by failing to safeguard users' information. The OPC then brought an application in the Federal Court under paragraph 15(a) of PIPEDA alleging that Facebook breached the Act and seeking a remedy against Facebook.

Decision

The Court dismissed the application, finding that the OPC did not discharge its burden to establish that Facebook had breached PIPEDA by failing to obtain meaningful consent. The OPC did not adduce any expert evidence of what Facebook could feasibly have done differently, nor was there any subjective evidence from Facebook users about their expectations of privacy or their appreciation of the privacy issues at stake when using Facebook. The Court stated that, although such evidence may not be strictly necessary, "it would have certainly enabled the Court to better assess the reasonableness of meaningful consent in an area where the standard for reasonableness and user expectations may be especially context dependent and are ever-evolving." As a result, the Court was left to draw inferences that were not supported by the evidentiary record.

The Court also found that once information was disclosed to a third-party app, Facebook's safeguarding obligations under PIPEDA were at an end. Further, the Court stated that, even if the safeguarding obligations had applied to Facebook after information was disclosed to third-party applications, there was insufficient evidence to determine whether Facebook's contractual agreements and enforcement policies constitute adequate safeguards.

Key Takeaway

On a *de novo* hearing under section 15(a) of PIPEDA, a breach of the legislation cannot be found in an "evidentiary vacuum." The OPC bears the burden and is required to lead cogent evidence to establish a breach. Moreover, this decision supports the principle that, once an organization is authorized by a user to disclose information to a third-party app, the organization's safeguarding duties under PIPEDA are at an end.

Facebook, Inc. v. Canada (Privacy Commissioner), 2023 FC 534

Read the case details

Facts

The underlying facts are essentially the same as the facts in the previous summary: the OPC investigated a complaint that a third-party application obtained Facebook users' personal data through the Facebook platform and disclosed it to Cambridge Analytica. The OPC issued a report concluding that Facebook had breached PIPEDA by sharing Facebook users' personal information with third-party apps without the users' consent and by failing to safeguard users' information. However, this decision relates to an application filed by Facebook in the Federal Court, seeking judicial review of "the [OPC's] decisions to investigate and continue investigating, the investigation process, and the resulting Report of Findings."

Decision

The Court dismissed this application on the threshold ground that the application for judicial review was not brought in time, nor was an extension warranted. Nonetheless, the Court went on to address the substantive claims in the event that the decision on the threshold ground was wrong. The Court did not accept Facebook's submissions that the complainants lacked standing, that the OPC's investigation lacked a necessary real and substantial connection to Canada or that the investigation resulted in a breach of procedural fairness.

Privacy and biometrics/AI

Enquête concernant le Centre de services scolaire du Val-des-Cerfs (anciennement Commission scolaire du Val-des-Cerfs), 2022-11-09, 1020040-S

Read the case details

Facts

This decision emanates from the oversight division of the Commission d'accès à l'information (CAI). The CAI launched an investigation of the Val-des-Cerfs school board which had developed an algorithm, in partnership with a consulting firm, to target Grade 6 students who were at significant risk of dropping out. The school board had developed a machine learning methodology which would analyze more than 300 types of raw data taken from a database of the students' personal information and generate a set of predictive indicators of dropout risk (the Tool). The CAI's decision following the investigation ruled as to whether the organization had met its obligations under the *Act respecting Access to documents held by public bodies and the Protection of personal information* (the Access Act) in the collection and use of personal information in the development phase of the project.

Decision

First, the CAI determined that while the personal information was depersonalized to prevent the direct identification of the students and their parents, it was not anonymized as it was not irreversibly depersonalized, and therefore still allowed for identification of the students.

Second, the CAI found that, in the development of the Tool, the school board had used the personal information for a new purpose, contrary to section 65.1 of the Access Act. When the information was first collected, the students and their parents had not been informed and therefore had not consented to the use of the information to generate predictive indicators of dropout risk. However, the CAI determined that the purpose for which the information was used was compatible with the objectives of the school board to ensure academic success.

Third, the CAI concluded that the Tool constituted artificial intelligence, as it was "a system whose purpose was to augment human work, capable of predictive analysis by a technological system involving algorithms." Importantly, as a result of the analysis it performed, the Tool produced new personal information, namely, predictive indicators of the risk of dropping out, which the CAI determined amounts to a *collection* of personal information within the meaning of the Access Act.

In light of the determination that the school board had collected personal information in its development of the Tool, the CAI found that it had not abided by its obligations to inform the parents of the students about the ways in which the data was used. The CAI called on the school board to adopt security measures to ensure the protection of personal information collected, including procedures for its destruction, and to destroy the Tool's existing output. It also called on the school board to proceed with a privacy impact assessment prior to the deployment of the Tool.

Key Takeaway

This decision of the oversight division of the CAI is the first in Québec to provide guidance on the CAI's interpretation of several issues surrounding artificial intelligence. Specifically, the CAI definition of artificial intelligence and its determination that the production of predictive indicators constitutes a "collection" of personal information, are novel. This determination in particular could subject organizations that use artificial intelligence to generate insights to the privacy law provisions applicable to the collection (and not the use) of personal information, including notably obtaining consent of the concerned individuals. In certain circumstances, this decision may need to be taken into consideration in the interpretation of new section 65.2 of the Access Act, and its private sector equivalent, section 12.1 of the *Act respecting the protection of personal information* in the private sector, which will enter into force in September 2023 and set forth new transparency rules for automated decision-making.

Situmorang v. Google LLC, 2022 BCSC 2052

Read the case details

Facts

The plaintiff sought certification of a class action against Google LLC for Google's use of face grouping technology. The plaintiff alleged that Google did not obtain informed consent from the class members for use of the face grouping technology and used the facial biometric data of the class members for its own competitive advantage. The plaintiff advanced claims under both the B.C. *Privacy Act* (the Statutory Claim) and the common law tort of intrusion on seclusion (the Common Law Claim).

Decision

The Supreme Court of British Columbia refused to certify the action, finding that it was plain and obvious that both the Statutory Claim and Common Law Claim could not succeed.

The Court found that it was plain and obvious the Statutory Claim could not succeed because it could not be established that Google's conduct was a wilful violation of privacy or that Google lacked claim of right to engage in the face grouping conduct.

In assessing the Common Law Claim, the Court was required to consider whether Google had invaded the plaintiff's "private affairs or concerns." The Court held that it was an open question as to whether a retained collection of facial biometric data may be information capable of implicating one's "private affairs and concerns." Despite this, the Court held that it was plain and obvious the Common Law Claim would fail because the plaintiff could not establish that an intrusion arising from Google's use of face grouping would be considered highly offensive by a reasonable person.

Key Takeaway

The question of whether a retained collection of facial biometric data may be information capable of implicating one's "private affairs and concerns" remains open. There is therefore a risk that organizations that collect and retain facial biometric data may be vulnerable to claims of common law intrusion on seclusion.

Access to information

Dutremble c. Hydro-Québec, 2023 QCCAI 3

Read the case details

Facts

The applicant applied to Hydro-Québec for access to documents concerning the Chute-Bell dam. The agency argued that the information was still in dispute and its disclosure would have the effect of reducing the effectiveness of a program intended for the protection of property or persons – in this case, the 2019-2023 Safety Program, which is intended to protect its dams – as well as undermining the security of the state.

Decision

The request to overturn HQ's refusal to release the documents was dismissed. HQ relied upon section 29 of the *Act respecting Access to documents held by public bodies and the Protection of personal information*. Its evidence demonstrated the sensitive nature of the information at issue and showed that the disclosure of this information would have the effect of reducing the effectiveness of its security program. Further, the information is sufficiently specific that a person could exploit it. Disclosing it could allow malicious

persons to commit acts that could put the infrastructure at risk and have foreseeable consequences, including dam failure, that would have a direct effect on the safety of people as well as on road infrastructure, including the bridges on Highways 148 and 50.

Key Takeaway

The safety exception relied upon to deny access is rarely used, but may become more prevalent with growing concerns about the safety of critical infrastructure. In certain cases, the exception may apply to an access request relating to information for which there is a safety concern, although the extent is likely to depend on heavily factual determinations.

Ville de Laval c. Savard, 2022 QCCQ 8465

Read the case details

Facts

The CAI ordered the appellant City of Laval to provide the respondent Mr. Savard with excerpts of a legal opinion within the meaning of section 31 of an *Act respecting Access to documents held by public bodies and the Protection of personal information*. The legal opinion was written by a lawyer in the context of the admissibility of a complaint for psychological harassment filed by Mr. Savard against the City.

Decision

The City argued that once a document qualifies as a legal opinion within the meaning of section 31 of the Act, the legal opinion as a whole becomes indivisible as protected by solicitor-client privilege, and no excerpts can be communicated. The Court of Québec partially granted the appeal from the decision of the CAI. The Court first determined that excerpts of a document covered by solicitor-client privilege may be disclosed to a party making a request for access. The fact that a document is covered by solicitor-client privilege does not make it indivisible. That said, in this case, the excerpts of the legal opinion to which the CAI had granted access were mostly covered by solicitor-client privilege and the CAI erred in law by ordering the City of Laval to disclose them, except for one excerpt relating to a description of the parties.

Key Takeaway

While the CAI and Court of Québec are sensitive to privilege claims, there is no hard-and-fast rule that a document covered by solicitor-client privilege is indivisible. In certain cases, excerpts may be disclosed to a third party. The party objecting to disclosure will need to establish that the relevant information is so integral to privileged legal advice that it cannot be extracted without waiving privilege.

Saskatchewan (Ministry of Labour Relations and Workplace Safety), Re, 2023 Carswell Sask 99

Read the case details

Facts

The Ministry of Labour Relations and Workplace Safety (LRWS) received an access to information request under *The Freedom of Information and Protection of Privacy Act, SS 1990-91*, (FOIP) from the applicant, who was the employer of an injured worker. The request was regarding documents related to a workplace injury. LRWS released some documents, but not all. LRWS withheld documents under subsections 22(b), 22(c), 29(1), 15(1)(c), 15(1)(e), 19(1)(b) and 13(1)(a) of FOIP and subsection 27(1) of *The Health Information Protection Act, SS 1999* (HIPA). The Saskatchewan Information and Privacy Commissioner received a request for review from the applicant. After that request, LRWS issued a second revised decision altering its claim that subsections 13(1)(a) and 22(b) of FOIP applied.

Decision

The Commissioner considered each section individually. Regarding subsection 27(1) of HIPA, the Commissioner ruled that there was no consent to release these documents by the injured worker and therefore LRWS applied this section properly for the majority of documents. The Commissioner did rule that one document must be released, as it was information provided by the applicant and it would be an "absurd result" if the LRWS did not provide these documents. Regarding subsection 15(1)(c) of FOIP, the Commissioner again applied the "absurd rule," as the applicant was involved in the creation of the documents that were being withheld (for example, they were contracts the applicant had signed or emails they were copied on). Regarding subsection 29(1) of FOIP, the Commissioner ruled some documents were incorrectly withheld, as publicly available information and individuals' signatures applied in a work context are not personal information. The names of witnesses to the injury were also not considered personal information. The Commissioner found some documents, including addresses that would not have been known by the applicant, were protected under subsection 29(1) of FOIP.

Key Takeaway

Under the "absurd rule," if the result of the ruling of the Commission leads to an absurd result, such as the prevention of the disclosure of information to an applicant which the same applicant has access to, then that result should be avoided.

Brightwater Senior Living, Re, 2022 CarswellSask 535

Read the case details

Facts

On October 5, 2021, the applicant submitted an access to information request to Brightwater Senior Living for their deceased mother's medical records. Brightwater responded to the applicant's request on December 14, 2021. The applicant was dissatisfied with the time Brightwater took to respond to the request. On February 3, 2022, the Office of the Saskatchewan Information and Privacy Commissioner informed the applicant and Brightwater that it would be undertaking a review.

Decision

The Commissioner found that Brightwater had not responded to the applicant's request within the timelines legislated under s. 36(1)(a) of the *Health Information Protection Act*. Brightwater submitted that it initially did not respond to the request because the applicant was not listed as power of attorney or any point of contact for the resident. The Commissioner held that Brightwater was required to respond to the request setting out its reasons for refusing access within the legislated timelines.

Key Takeaway

Where a trustee believes a person requesting access to information does not have the right to access the requested information, it must respond to the request setting out its reasons for refusing access within the legislated timelines.

Cain v. Canada (Health), 2023 FC 55

Read the case details

Facts

The Federal Court considered an application under the *Access to Information Act* for the disclosure of postal codes and cities for licensees entitled to grow medical marijuana. Health Canada agreed to release only the first digit of the postal codes – even though the applicant sought access to the first three characters (the Forward Sortation Area) – because of the "serious possibility" that the second and third characters of the postal codes could be linked with other information to identify specific individuals.

Decision

The Federal Court dismissed the application. The Court reasoned that for some regions, a relatively small number of people live within a single Forward Sortation Area, and there was a risk that the first three characters could be combined with other information that is publicly available to identify a particular licensee. The Court found that privacy rights must prevail. The evidence demonstrated a serious possibility that disclosing the requested data would risk exposing very sensitive information about individuals. This justified Health Canada's refusal to disclose the second and third characters of the postal codes. The Federal Court also found that Health Canada was not required to undertake further "de-identification techniques" to disclose more of the information.

Key Takeaway

The Federal Court relied on jurisprudence from the Supreme Court of Canada, and the intention of Parliament, to find that privacy must prevail in a clash between access to information and individuals' privacy rights. On the facts of this case, the Federal Court was persuaded that the risks to privacy "are simply too great."

Privacy and employment

Hébert c. Syndicat de professionnelles et professionnels du Gouvernement du Québec, 2022 QCCAI 300

Read the case details

Facts

The applicant, an employee of the Ministère de l'Agriculture, des Pêcheries et de l'Alimentation (MAPAQ), claimed to have been the victim of psychological harassment from her managers and colleagues. She filed a complaint for psychological harassment and a grievance against her employer. The Syndicat de professionnelles et professionels du gouvernement du Québec (SPPGQ) represented the applicant in her grievance. An investigator was appointed to investigate the complaint and prepare a report. The applicant applied to the SPPGQ to obtain access to this report as well as to any other reports or documents related to her grievance. Access was denied to 10 documents. The applicant also sought to have her identity anonymized in this decision, given the sensitive nature of the information contained therein.

Decision

The CAI overturned the MAPAQ's decision in part. Section 13 of the *Act respecting the protection of personal information in the private sector* states that personal information may be disclosed to third parties only to the extent that the individual consents to its disclosure. Some documents filed as part of the analysis of the applicant's grievance contained communications between various MAPAQ employees. The name of the plaintiff did not appear in any of these communications and the plaintiff was not copied on the mailings. The documents contained facts, opinions or perceptions of third parties with respect to certain events or matters in the course of their work, which the CAI found constitute personal information about third parties. In the absence of the concerned third parties' consent, the personal information could not be disclosed.

Key Takeaway

Opinions expressed by one person about another regarding his or her skills, opinions, choices or work practices constitute personal information both to the person expressing them and to the person who is the subject of the opinions. Such information may therefore not be disclosed, except with the consent of the concerned third party. For organizations holding this type of information, it may be advisable to identify subjective assessments as such and separate them from factual compilations or strictly objective records of personal information.

Advanced Upstream Ltd., Re, 2023 CarswellAlta 630

Read the case details

Facts

The complainant was a former employee of Advanced Upstream Ltd. Their employment agreement included a non-solicitation clause that survived for 12 months after the employment ended. Advanced Upstream heard that the complainant had been providing services to a competitor and sent a letter through lawyers to the competitor. The letter informed the competitor of the possibility that the complainant may be in breach of their restrictive covenants. After receiving the letter, the competitor informed Advanced Upstream that it had engaged in discussions with the complainant, but had decided not to hire the complainant. The complainant found out that the letter had been sent, and filed a complaint alleging that Advanced Upstream had disclosed his personal information. Advanced Upstream later reported an unauthorized breach of PIPA, but continued to dispute that the disclosure violated their privacy rights.

Decision

The Commission first found that the letter did contain personal information in the form of the complainant's name, the fact that he was employed by Advanced Upstream in a particular position, his address, his signature and a disclosure letter which listed his non-profit and charitable activities, other business activities, ownership interests in other entities and his marital status along with his partner's first name. The Commission then found that the complainant had consented to the disclosure of his personal information through an article in his employment agreement which granted consent for the disclosure of employee's personal information for the ongoing operations of the corporation. The Commission lastly considered whether the disclosure was reasonable as required by Section 19 of PIPA and found that the purpose of disclosure was reasonable in the corporation seeking to avoid a breach of an employment agreement, but the scope of disclosure was not, specifically with respect to disclosing the complainant's address, marital status, name of his spouse, signature and conflicts of interest.

Key Takeaway

Organizations handling personal information can reach out to competitors to protect their non-solicit and non-compete interests, but in doing so, they should ensure that personal information included in materials that aren't necessary to protect these interests are redacted or otherwise not disclosed.

Direct Energy Regulated Services, Re, 2023 CarswellAlta 629

Read the case details

Facts

Under a Premise Vacancy Agreement (PVA), the owner of a property (the complainant) was required to provide contact information to an energy services company (the organization). Sixteen years after the property was sold, the organization contacted the complainant. The complainant complained that the organization did not comply with section 35 of PIPA (retention and destruction of information).

Decision

The organization complied with PIPA because the information was exempt pursuant to section 4(3)(d) of the Act. Given that section 4(3)(d) exempts the collection, use and disclosure of personal information, it must, at least to some extent, exempt the retention of that information. In the broader sense of obtaining energy services from

the organization, the complainant's business responsibilities relative to the organization ended when the property was sold, however the requirement that the complainant contact the organization in order to terminate the PVA endured.

Key Takeaway

Section 4(3)(d) of PIPA exempts the retention of business contact information, so long as that information is retained for the purposes stated in that section: to enable an individual to be contacted in relation to the individual's business responsibilities, and for no other purpose.

Saskatchewan Health Authority, Re, 2023 CarswellSask 44

Read the case details

Facts

An employee filed a grievance after their employer, the Saskatchewan Health Authority, posted a notice on a whiteboard stating that the employee was on medical leave. The employee argued that this disclosure of their personal health information violated their privacy rights.

Decision

The Office of the Saskatchewan Information and Privacy Commissioner agreed with the employee and found that the employer had breached its duty to protect the employee's personal health information. It found that privacy breaches occurred when the manager shared the employee's personal health information with office administrative staff, when the office administrative staff recorded the employee's personal health information on the attendance white board and when staff viewed the employee's personal health information on the white board.

Key Takeaway

This case emphasizes the importance of maintaining confidentiality in medical information, as well as the need for employers to have clear policies and procedures in place to ensure the protection of such information. It also highlights the significance of privacy rights and the importance of employers taking adequate steps to safeguard personal health information in the workplace.

Livingston v Saskatchewan Human Rights Commission, 2022 SKCA 127

Read the case details

Facts

The appellant appealed a chambers decision striking his action on the grounds of lack of jurisdiction and abuse of process. The original statement of claim concerned breach of privacy in an employment human rights issue. The appellant and his union submitted that the workplace, the Saskatchewan Human Rights Commission, breached his privacy and their duty of procedural fairness when they inquired about and disclosed his employment issue with his co-workers.

Decision

The Court of Appeal dismissed the appeal and held that the chambers judge did not err in finding that the essential issue related to employment and was thus the jurisdiction of an arbitrator as stipulated in the workplace collective agreement. Specifically, the essential nature of the appellant's claim for breach of privacy arose from employment. The Court stated that such human rights issues are contemplated and incorporated in collective bargaining agreements. The Court also cited the Supreme Court of Canada's judgments in *Weber v. Ontario Hydro* and *Northern Regional Health Authority v. Horrocks* which held that courts of inherent jurisdiction cannot entertain issues that relate to a collective agreement, subject to residual discretionary jurisdiction.

Key Takeaway

Privacy issues that arise from employment concerns are subject to limitations in jurisdiction dictated by collective bargaining agreements.

Privacy in the dispute resolution process

Rousseau c. Conseil de l'industrie forestière du Québec, 2022 QCCAI 332

Read the case details

Facts

A company terminated the plaintiff's employment which led him to file a complaint with the Commission des normes, de l'équité, de la santé et de la sécurité au travail (CNESST). The plaintiff then asked the company to provide him with a copy of his employee file, including his employment contract and letter of employment, as well as all policies regarding email usage and vacation time. However, some of the documents which were relevant to his termination were not sent to him. Thus, the plaintiff filed an application to the CAI. Two days later, the plaintiff signed a termination agreement, which did not explicitly mention proceedings before the CNESST. The company claimed that the complaint ought to be rejected.

Decision

The CAI upheld the refusal of the company to provide documents. A company may refuse, under section 39(2) of the *Act respecting the protection for personal information in the private sector* (the Act) to disclose personal information when it may have an impact on legal proceedings. Further, this determination should be made in accordance with the proceedings as they stand as of the date of the termination. Even if the proceedings later conclude, the decision will stand if the exception applied at the relevant time. Here, there was a direct link between the documents sought by the plaintiff and the legal proceedings; at the time the company sent its response to the plaintiff's access request, the complaints to the CNESST were pending.

Key Takeaway

The CAI has broadly interpreted the right to refuse the communication of personal information to the person it concerns where disclosure of the information would be likely to affect judicial proceedings in which either party has an interest. Also noteworthy, the CAI held that general release language in a settlement agreement will not effect a release of a complaint filed with the CAI.

Centre universitaire de santé McGill c. Lemay, 2022 QCCA 1394

Read the case details

Facts

In September 2012, Québec's anti-corruption agency, the Unité permanente anticorruption (UPAC) executed a search warrant at the appellant McGill University Health Centre's offices following allegations of collusion and corruption in the awarding of contracts for construction work. The appellant then retained counsel for advice as to the remedies and actions to be taken in light of these allegations. The lawyer retained a forensic accounting firm, which produced a preliminary report. That report was then disclosed voluntarily to UPAC. The primary issue in the appeal was whether the voluntary disclosure of the privileged report to UPAC, in the context of a criminal investigation, resulted in the loss of privilege and confidentiality of the document with respect to other third parties.

Decision

The Court of Appeal held that the CAI and the Court of Québec were correct in determining that privilege and confidentiality with respect to third parties were not lost where the information was disclosed to police forces. The CAI and the Court of

Québec had correctly relied on prior jurisprudence establishing that the act of disclosing privileged information to the police is a moral obligation, which does not demonstrate a clear and unequivocal intent to waive solicitor-client privilege.

Key Takeaway

The disclosure to law enforcement authorities of privileged information for the purpose of assisting in a criminal investigation does not automatically result in the loss of privilege or confidentiality of the document with respect to other third parties.

Nintendo du Canada ltée c. Tilmant-Rousseau, 2022 QCCQ 5610

Read the case details

Facts

This judgment is an appeal from a decision of the CAI which had overturned a decision of the Office québécois de la langue française (OQLF). In September 2007, the appellant, the Entertainment Software Association of Canada (ESAC), entered into a memorandum of understanding (MOU) with the OQLF, on the conditions related to the distribution of video games in Québec and dealing with various aspects of their marketing. In 2017, the OQLF refused to provide the respondent Laurence Tilmant-Rousseau with a copy of the MOU, citing the confidential nature of the document. This decision was challenged before the CAI. The ESAC and Nintendo Canada Ltd. intervened in opposition to the application for review, on the basis that the MOU was protected by settlement privilege. In August 2019, the CAI ordered the OQLF to disclose the MOU to the respondent.

Decision

The Court of Québec concluded that the CAI erred in refusing to apply settlement privilege in the context of an access to information request. The CAI had based its decision on the quasi-constitutional nature of the *Act respecting Access to documents held by public bodies and the Protection of personal information* which protects citizens' right to information. The Court of Québec found that when settlement privilege applies, it carries with it a *prima facie* presumption of inaccessibility of third parties to the communications made for the purpose of settling the dispute, including the settlement agreement. It applies to any dispute that may be brought before the courts, administrative tribunals, arbitrators and mediators, even in the absence of statutory or contractual confidentiality provisions. It is not merely a rule of evidence, but rather is a substantive rule. In this case, the court found that the MOU was protected by settlement privilege.

Key Takeaway

In line with recent jurisprudence, the Court of Québec reiterated that settlement privilege is a generic principle that takes precedence over the general rule of access to records of public bodies. This is a relatively broad interpretation of settlement privilege, which goes beyond the rights of the parties to the settlement and does not set a time limit for its application.

Acuren Group Inc., Re, 2023 CarswellAlta 217

Read the case details

Facts

The applicant was an employee of the respondent, Acuren Group Inc. The applicant alleged that his employment was terminated without cause and that a complaint made about him by another employee played a role in his termination. Pursuant to the *Personal Information Protection Act* (PIPA), the applicant made a request to the respondent seeking the disclosure of information pertaining to complaints made against him, his personnel file and all communications and records surrounding the release of his employment. The respondent noted that much of the information requested was not the applicant's personal information, and as a result, the respondent withheld some of the information pursuant to sections 24(3)(b) and 24(3)(c) of the PIPA. The remaining records were also withheld under section 24(2)(a) of the PIPA as subject to litigation privilege or solicitor-client privilege.

Decision

The court held that the respondent properly withheld information under sections 24(3)(b) and 24(3)(c) of the PIPA because the disclosure of such information would result in revealing opinions that were made to the respondent in confidence, as well as personal information about another individual. In addressing the information withheld subject to litigation privilege, the court held that there was no litigation privilege because the

applicant executed a general release in favour of the respondent and as such, there was no reasonable apprehension of litigation. Further, the court held that although some of the information contained legal advice, there was no solicitor-client privilege because the information was not confidential as it was shared outside of the solicitor-client relationship.

Key Takeaway

An organization can deny access to an employee's personal information if such access would reveal the personal information of another individual or opinions that were made in confidence. Similarly, for solicitor-client privilege to be effective, the information must be a communication between the solicitor and client, must contain legal advice and must remain confidential.

Individuals' privacy interests

Charest c. Procureur général du Québec, 2023 QCCS 1050

Read the case details

Facts

In April 2017, a newspaper company published documents relating to the plaintiff, Jean Charest, former Premier of Québec, obtained or created by Québec's anti-corruption agency, the Unité permanente anticorruption (UPAC). The documents were leaked to the press in the context of an investigation into sectoral financing by the Québec Liberal Party when it was the ruling party. This was – and still is – a high-profile case.

Decision

The Superior Court of Québec ruled in favour of the plaintiff, awarding $35,000 in compensatory damages and $350,000 in punitive damages. The Court found that UPAC had failed to protect Mr. Charest's personal information, contrary to the provisions of the *Act respecting Access to documents held by public bodies and the Protection of personal information*. Under the Act, disclosure of personal information to the media without the knowledge of the individual concerned is not permitted. The Attorney General argued that the plaintiff could not have had a significant expectation of privacy as a politician. The Court rejected this argument.

Key Takeaway

Although this case centres on a public body that leaked personal information to the press, the Court's ruling shows that the protection of personal information is taken very seriously, even in the case of public figures who are also entitled to the protection of their personal information and retain an expectation of privacy despite their public appearances.

Bellevue West Building Management Ltd., Re, 2022 BCIPC 74

Read the case details

Facts

The complainant owns an apartment in a building where all the owners incorporated Bellevue West Building Management Ltd. to coordinate the use and enjoyment of the building. Bellevue is run by a management committee that installed a video surveillance system to combat break-in attempts and minor property damage. The complainant complained to the Information and Privacy Commissioner for British Columbia that Bellevue had collected and used her personal information consisting of the images captured by the surveillance.

Decision

The Commission first considered whether the complainant had consented to the collection of her personal information and found that, while the signs that had been put up did constitute sufficient notice, the complainant's use of the public spaces under surveillance did not constitute her consent as Bellevue argued – inherent in consent is an element of choice, and the complainant had to use the laundry room and lobby to access her suite. Bellevue relied on sections 12(1)(c), 12(1)(h) and 12(1)(j)(i) to justify why it didn't require the complainant's consent, but the Commission found that none of these sections applied. Because Bellevue was not authorized to collect the personal information to begin with, the Commission also found that it was not authorized to use it under ss. 6(1) and 6(2).

Key Takeaway

For consent to be given for the use or collection of personal information, one must have a legitimate opportunity to decline.

Métis Addictions Council of Saskatchewan Inc., Re, 2023 CarswellSask 124

Read the case details

Facts

Sensitive personal information of patients of the Métis Addictions Council of Saskatchewan Inc. (MACSI) was found in a recycling bin by a member of the public, who then provided it to the media. The files contained confidential information about clients' addictions and mental health issues, and had not been properly disposed of by MACSI. A member of the media advised the Office of the Saskatchewan Information and Privacy Commissioner of the files.

Decision

An investigation by the Office of the Saskatchewan Information and Privacy Commissioner found that the files contained sensitive personal information, including details of clients' addictions and mental health issues, and had not been properly disposed of. MACSI was found to be in breach of the *Health Information Protection Act*; it was determined that MACSI did not take all the steps it could have to contain the breach nor did it make enough effort to provide notification to the affected individuals. MACSI was ordered to pay a fine and take steps to prevent similar breaches in the future.

Key Takeaway

The case highlights the importance of proper handling and disposal of sensitive personal information, particularly in the context of healthcare and other industries that deal with such information. It also serves as a reminder to organizations of their obligations under privacy legislation and the potential consequences for failing to comply with these obligations.

James v. Amazon.com.ca, Inc., 2023 FC 166

Read the case details

Facts

The applicant, Tamara James, claimed that she created an account with Amazon.com.ca, Inc., but forgot her password. She sought access to customer account information, including account receipts and audio recordings of her dealings with Amazon customer service. Amazon tried to assist James in resetting the password, but James declined to accept that assistance.

James filed a complaint to the Privacy Commissioner and corresponded with the Amazon Privacy Officer, Amazon Executive Customer Relations employees and Amazon counsel to try to resolve the issue. Amazon concluded that it could not authenticate James as the requestor because (i) James was unwilling to follow the steps provided to reset her password; and (ii) the information James provided did not correspond with the information on Amazon's server.

The Commissioner's Report found that "Amazon provided [James] with a fair and reasonable response to [her] access request when it could not verify [her] identity." James then brought the dispute before the Federal Court pursuant to section 14 of PIPEDA.

Decision

The Court dismissed the application. James did not discharge her burden of establishing any violation of PIPEDA. Amazon was under an obligation to protect the account information (PIPEDA, Principle 7); in the Court's words: "that is the very purpose of the PIPEDA." Accordingly, the Court found, Amazon "was justified in refusing to give access to personal information without being able to authenticate the identity of the requester in the circumstances of this case."

The Court dismissed several other issues raised by James, including arguments that Amazon violated Principle 6 (on the basis that allegedly inaccurate information in Amazon's possession prevented authentication of the requestor's identity) and that Amazon violated the timeliness requirement under section 8 of PIPEDA.

Key Takeaway

Organizations can validly deny access to personal information if the requestor's identity cannot be appropriately authenticated. Here, Amazon offered reasonable assistance seeking to authenticate James's identity. As the Court found: "Assistance was available. The Applicant chose to not use it."

Barrett v Royal Bank of Canada, 2022 FC 1534

Read the case details

Facts

Maureen Barrett resigned from her job at RBC Life Insurance Company and assumed a new role as a financial adviser with Sun Life Financial. At the time of her resignation from RBC Life, the company was investigating Barrett for alleged fraudulent conduct involving her personal bank account. Sun Life also undertook its own independent investigation into Barrett's conduct as an employee of Sun Life. After Sun Life terminated Barrett's employment, Barrett alleged it was because RBC had disclosed her personal banking information to Sun Life without her consent, in contravention of PIPEDA. Barrett brought an application pursuant to s. 14 of PIPEDA. She sought a declaration that RBC's disclosure of her personal information to Sun Life contravened PIPEDA, damages and costs.

Decision

The Court dismissed Barrett's application, finding that the disclosure of personal information was made in accordance with subsection 7(3)(d.1) of PIPEDA, which permits disclosure of personal information without knowledge or consent of the individual in order to further an investigation. The Court found that RBC reasonably disclosed Barrett's personal banking information in furtherance of Sun Life's investigation of Barrett's conduct. The Court stated that the information was relevant to Sun Life's investigation and it was reasonable for RBC not to inform Ms. Barrett or seek her consent prior to the disclosure, because this could have compromised the investigation.

The Court explained that it would not have found that the disclosure was authorized by RBC's own investigation, alone, because disclosing the personal information to Sun Life would have done nothing to further RBC's investigation or to prevent any fraud, since the alleged fraudulent activity with Barrett's bank account had already happened.

Finally, the Court stated that, even if Ms. Barrett could demonstrate a violation of PIPEDA, an award of damages would not be appropriate. Any breach by RBC would not have been egregious and her employment was not terminated because of the very limited disclosure of her personal information by RBC.

Key Takeaway

This decision clarifies the circumstances under which paragraphs 7(3)(d.1) and (d.2) of PIPEDA permit the disclosure of personal information without an individual's knowledge or consent in order to further an investigation and suppress or prevent fraud. In this particular case, the disclosure was reasonable in furtherance of an investigation, even if it would not have been reasonable to suppress or prevent fraud.

Al-Husseini v. Altaif Inc., 2022 FC 1497

Read the case details

Facts

The applicant, Sadeq Al-Husseini, brought an application under section 14 of PIPEDA against Altaif Inc. for disclosing financial information that allegedly exceeded the scope of a production order related to Al-Husseini's divorce proceedings in the Ontario Superior Court of Justice (the Production Order).

Decision

The Federal Court dismissed the application, finding that Altaif had not breached Al-Husseini's privacy rights because the foreign exchange transfers that Altaif disclosed were within the scope of the Production Order. The Court also accepted Altaif's submissions that Altaif reasonably believed that the information was required to be disclosed under the Production Order.

Given that finding, there was no need to address the issue of damages. However, the Court explained that even if the Court's interpretation of the scope of the Production Order was incorrect, Al-Husseini had not established that he suffered damages as a result of the disclosure. The Court further stated that, although PIPEDA gives the Federal Court discretion to grant remedies for privacy breaches, an award for privacy law damages should only be made in the "most egregious of circumstances."

Key Takeaway

This decision highlights some of the challenges in asking one court to interpret the scope of an order issued by another court for the purposes of assessing an alleged violation of PIPEDA. The Federal Court was ultimately able to make findings about the scope and purpose of the Production Order in this case, but the reasons reflect the limits of this exercise.

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