SPRING 2021

Privacy in the Courts: A quarterly review

ACCESSPRIVACY BY OSLER

Table of Contents

Introduction

This quarterly review of Canadian jurisprudence is intended to help busy in-house counsel, Chief Privacy Officers and compliance professionals navigate recent court decisions and gain a broad understanding of how privacy law is evolving in Canada. Through expert commentary, users can begin to see trends over time and gain insights into potential implications for their organizations. Recognizing how difficult it can be at times to keep up with developments, this review is intended to serve as a readily-accessible, efficient and practical resource to help readers stay in the know, while saving time.

Adam Kardash, National Lead of AccessPrivacy by Osler, would like to thank Professor Teresa Scassa of the University of Ottawa for her valuable contribution in authoring these case summaries. The accompanying expert commentary offers readers an enhanced understanding of the case by providing a rich scholarly analysis, discussing its practical implications for organizations and placing it within a broader policy context of evolving privacy law.

We hope users find this resource useful and we welcome feedback on how it might be improved over time. Please send comments to info@accessprivacy.com.

Decision places limits on scope of tort of intrusion upon seclusion

Owsianik v. Equifax Canada Co., 2021 ONSC 4112

Facts

The defendants in a class action lawsuit appealed a decision to allow a claim of intrusion upon seclusion at the certification stage. The lawsuit was in relation to a massive data breach that occurred as a result of a malicious hack of the defendant Equifax's databases.

The tort of intrusion upon seclusion is an intentional tort that requires the defendant to have deliberately intruded upon the private affairs of the plaintiffs. The plaintiffs argued that Equifax had an obligation to maintain the security of the personal information it collected about Canadians, that it knew its security was inadequate, and that it did nothing to address the security defects. By not addressing known security defects, the plaintiffs argued that Equifax had intruded upon the seclusion of the plaintiffs. At the certification stage, a claim will not be dismissed unless it is 'plain and obvious' that the claim is doomed to fail. The judge at first instance found it was not plain and obvious that this claim was doomed to fail.

Decision

The majority of a divided Divisional Court overturned a judge's decision to allow the claim of intrusion upon seclusion.

Discussion

Justice Ramsay, for the majority, noted that the interpretation of intrusion upon seclusion advanced by the plaintiffs amounted to a novel claim. The tort had been first recognized only nine years ago by the Ontario Court of Appeal in *Jones v. Tsige*. He stated that the tort "has nothing to do with a database defendant [...] It has to do with humiliation and emotional harm suffered by a personal intrusion into private affairs, for which there is no other remedy because the loss cannot be readily quantified in monetary terms" (at para 54). Although he accepted that the Court of Appeal in *Jones* did not intend their decision to be the last word on the tort of intrusion upon seclusion, he was of the view

that applying the tort in the circumstances of this case would open the floodgates. Although he noted that courts in other class actions have shown an openness to the potential for the tort to evolve in the context of large data breaches, he was unwilling to extend the tort in this way on the facts before him.

One of the advantages of the tort of intrusion upon seclusion is that it does not require proof of damages in the same way other causes of action might. This makes it very useful in data breach class action lawsuits where damages are often very difficult to establish. This fact did not sway Justice Ramsay. He noted that "The essence of [the plaintiffs'] claim has to do with risk to economic interests caused by disclosure of their financial information. It is not too much to ask that they prove their damages" (at para 57).

Justice Sachs dissented. In her view, *Jones v. Tsige* dealt with different facts, and the Court of Appeal in *Jones* had acknowledged the threat posed to privacy by technological change. She noted that the tort of intrusion upon seclusion was "a new tort designed to protect privacy rights" (at para 7), and that such rights have been recognized by the Supreme Court of Canada as having 'quasi-constitutional' status. In her view, "in a world where the threats posed to those rights by technology are growing and changing, the limits of the tort should be allowed to develop" (at para 7).

Justice Sachs emphasized that Justice Sharpe in *Jones v. Tsige* did not set rigid boundaries to the tort. She noted that "he was clear in his reasons that he was seeking to establish a cause of action that would encompass the facts before the court in that case" (at para 42). This did not mean that the application of the tort could not be considered in other factual contexts. Further, she noted that Justice Sharpe was clearly concerned about the privacy risks posed by the "routine collection and aggregation of highly personal information that is readily accessible in electronic form" (at para 42). She noted that "[t]here is nothing in his reasons to indicate that the concern was limited to the third parties who actually hack the information" (at para 42).

Justice Sachs also observed that in recognizing the new tort in *Jones*, Justice Sharpe had emphasized that the facts before him "cried out for a remedy" (at para 43). In her view, the same applied in this case. She stated: "Equifax knew that their systems were

vulnerable to being hacked and chose to do nothing about it, which in turn led to precisely the hack that they had been warned about. These actions facilitated an intrusion that a reasonable person could find to be highly offensive" (at para 43). She noted as well that if the claim for intrusion upon seclusion is not certified, the difficulty in proving damages (common to all data breaches) could leave the plaintiffs without a remedy. She dismissed the floodgates argument, noting that the tort is limited to "deliberate and significant invasions of personal privacy" (at para 44). In her view, this is enough to limit its application.

This is an interesting and important decision. There are a growing number of class action lawsuits relating to large-scale data breaches. As was recently noted in *Karasik v. Yahoo! Inc.*, it is often very difficult for plaintiffs to prove actual monetary damages. This is because, absent identity theft, financial harm may be impossible to quantify. Even if identity theft is established, it may be difficult to show a causal link between the identity theft and the particular data breach at issue. A tort that is compensable without proof of actual damages can be a useful mechanism for holding an organization to account in circumstances where the burden faced by plaintiffs to show harm is overwhelming.

Professor Teresa Scassa, Canada Research Chair in Information Law and Policy, University of Ottawa

This case, together with *Del Giudice v. Thompson*, 2021 ONSC 5379, signals that the Ontario courts will not find a defendant in breach of a privacy tort for the conduct of a third-party hacker. The decision also stands for a broader proposition with good common-sense appeal: a defendant will only have "intruded" on an individual's privacy if the defendant themselves has intruded. Moreover, that intrusion by the defendant must be "highly offensive". This is a high bar that would seem to preclude, for instance, a breach founded on the disclosure of otherwise public information. It remains to be seen whether courts across the country will follow the Ontario approach: while defendants have raised this argument before BC courts, there have been no reported decisions on point. In any case, the best defence will remain a strong, proactive IT security practice.

Emily MacKinnon, Associate, Litigation, Osler, Hoskin and Harcourt LLP

Settlement agreement approved in privacy class action

Del Giudice v. Thompson, 2021 ONSC 4024

Facts

The settlement agreement reached in this class action related to only one of multiple defendants. The data breach involved Capital One, which stored its customer data on Amazon Web Services Inc., a cloud services provider. An employee of Amazon hacked the Capital One database and allegedly misappropriated customer personal data. She also allegedly posted unencrypted data on GitHub's site. GitHub, with whom this settlement agreement was reached, had been added as a defendant in the class action against Capital One, Amazon and the employee.

Decision

Justice Perell approved the settlement agreement.

Discussion

This settlement agreement is essentially a discontinuance of the action against GitHub. In an earlier attempt to settle the action, the plaintiffs and the defendant GitHub had, by consent, asked the court to rule that it had no jurisdiction in the matter. Justice Perell had declined to do so, noting that the court's jurisdiction is not a matter for the parties to determine by agreement. He also noted that the issue of jurisdiction would have to be heard on its merits. He adjourned the matter. The parties later returned to the court with a modified agreement.

The revised settlement amounted to a discontinuance of the action against the particular defendant GitHub. One of the reasons for the discontinuance was a concern that "there is a real chance of GitHub prevailing on the issue [of jurisdiction] and exposing the Representative Plaintiffs to an adverse costs award" (at para 7). The claims against the other defendants would not be adversely affected by the settlement. Justice Perell approved the settlement agreement, finding it to be "fair and reasonable and in the best interests of the Class Members" (at para 10).

Breach of duty of utmost good faith not saved by PIPA exceptions

Barata v. Intact Insurance Co., 2021 ABQB 419

Facts

The plaintiff was driving with her partner when their vehicle struck and injured a man. The couple stop and spoke to the companions of the injured man, then returned to their car and left the scene before police and an ambulance arrived. The man subsequently died of his injuries. Later the same day, the police arrested the plaintiff's partner, on the assumption that he had been the one driving the car. He was charged with a number of offences including impaired driving causing death.

The plaintiff reported the accident to her insurance company and an investigator (named as a defendant in the case) began his investigation. The plaintiff told the investigator that she had been the one driving the car at the time of the accident. The investigator shared this information with the police, who later charged her with failing to stop, to provide her name and address or to provide assistance. Her partner was also charged with these offences. Both were tried and acquitted. The plaintiff then sued her insurance company, arguing that it breached its duty of confidentiality to her when it shared the information she had provided to the company with the police without her knowledge or consent. The insurance company argued that the disclosure was authorized under the province's *Personal Information Protection Act* (PIPA).

Decision

The court found that the insurance company had breached its duty of utmost good faith to its client, and that the disclosure at issue was not justified under PIPA. However, he also found that the plaintiff had suffered no damages as a result of the breach.

Discussion

Justice Dunlop ruled that a duty of confidentiality exists between insured and insurer, and that the relationship between them is "the reciprocal duty of utmost good faith" (at para 8). He did not go so far as to find that the insured's duty to provide all the

particulars of an incident was met with a reciprocal duty on the part of the insurance company to keep confidential any information it received. Nevertheless, the duty of good faith limits what an insurer can do with the information. Justice Dunlop observed that if insurance agents regularly provided client information to the police, they would be acting as agents of the police. Although there might be instances where it is in the interests of an insured to share information with the police, a "purely gratuitous disclosure to police, which does nothing to further the insurer's investigation, would not be reasonably justified, and therefore would be a breach of the insured's [sic] duty of utmost good faith to the insured" (at para 17). In this case, the disclosure to the police "served no purpose in the insurance investigation because it did not seek any information for Intact" (at para 22). As a result, it was a purely gratuitous disclosure that breached the duty of utmost good faith.

The next issue was whether PIPA authorized the disclosure of the information. The defendants argued that under s. 20(*f*) an organization may disclose personal information to a law enforcement agency without consent in order "to assist in an investigation". Under s. 20(*m*), a disclosure is permitted if it "is reasonable for the purposes of an investigation or legal proceeding". In either case, the disclosure must be for purposes that are reasonable, and it must also be limited to the extent that "is reasonable for meeting the purposes for which the information is disclosed" (PIPA, s. 19).

Justice Dunlop found that since a compelled statement from the plaintiff would be inadmissible in a criminal prosecution, it was not reasonable for the insurance agent to have shared the information with police. He noted that this kind of disclosure would undermine the relationship between insurer and insured. In this case, the insurance company had asked the plaintiff several times if they could share information with the police, and she had refused. He found that sharing the information with police was not reasonable in the circumstances. Even if PIPA authorized the disclosure, Justice Dunlop ruled that the insurance company would not be absolved of its duty of utmost good faith.

In spite of finding a breach of the duty of utmost good faith, Justice Dunlop found that the defendant's disclosure ultimately caused no harm to the plaintiff. Several months after the incident, her partner told police that she was driving; thus, the police had this information from another source. He declined to infer that the police had charged the plaintiff as a result of the disclosure by the defendants. He noted as well that after charges were laid against the plaintiff, the police obtained the investigator's notes through a production order. He concluded that the disclosure "did not cause or even contribute to, the charge and the prosecution" (at para 44). Justice Dunlop found no damages and declined to award any punitive damages.

Preliminary injunction granted over privacy of documentary film subjects

Côté v. Lachance, 2021 QCCS 1914

Facts

Two firefighters, the director of communications for their fire department, and a lieutenant-instructor with the service sought a preliminary injunction to prevent the showing of the plaintiff's documentary film, pending resolution of the privacy issues raised by the case. The film told a story of periods of idleness between calls for emergency response.

At the time he made his documentary, the respondent was a student in the last year of a media studies program at the Université du Québec à Montréal. The documentary was a program requirement, although he later also submitted it to film festivals, two of which accepted it. Prior to shooting the film, the respondent sought and received permission from the fire department's director of communications to film onsite at fire station 43. He also sought permission from the two firefighters to film them. The fourth applicant – a lieutenant-instructor – was captured on film in one sequence and had never consented to being part of the documentary. The two firefighters indicated that although they consented to being filmed, they believed that it was on the condition that they could review the film prior to its release and that they had the right to veto the use of the material at that point. They did not see the film prior to its release by the respondent.

The applicants objected to the film that was produced. In their view it created the false impression that firefighters did nothing but idle away their time in between calls to fires. They argued that the film breached their privacy rights and their rights to their images, and damaged their reputations. They made these arguments under both the *Civil Code of Quebec* and the Quebec *Charter of Human Rights and Freedoms*. The respondent countered that he had obtained explicit authorization to make the film from the director of communications and that he had obtained the express consent of the two firefighters. He also argued that, given the filming was open and evident, he had implied consent from all of the plaintiffs to the filming and by extension to the distribution of his film.

Decision

The court granted the interlocutory injunction.

Discussion

An applicant for a preliminary injunction must first establish that there is a serious legal issue to be tried. Justice Lucas found that the applicants asserted privacy rights under the Quebec *Charter of Human Rights and Freedoms* and the *Civil Code*, including the right to their images. Although the respondent argued that he had obtained consent, Justice Lucas noted that the director of communications could not consent to any invasion of privacy or use of the image of the firefighters. Each person appearing in the film would have had to sign an authorization on their own behalf. The respondent argued that, because he was present during the filming and did not object, the lieutenant-instructor had consented to the filming. Justice Lucas noted that consent to filming is not consent to particular uses of the film. She was not prepared to assume that he had consented to the distribution of his image on the internet and at film festivals. In the case of the two firefighters, although they had consented to the filming in the fire station, they argued that they had reserved the right to view and approve of the film before it was released. Although the evidence was not conclusive on this point, Justice Lucas found that there was some evidence that the defendant had undertaken to send them a copy of the final version – and that they might have understood this to mean that they had a right to object.

Justice Lucas also noted that the consent to being filmed was not necessarily a consent to being part of a film that only represented part of what took place between emergency calls. Justice Lucas found that, for the purposes of the interlocutory injunction, it could not be said that the firefighters were aware of the real intentions of the defendant with respect to the use of the footage and could not have implicitly consented to the film that had actually been made. She found that the use made of the images could be argued to go beyond any implied consent provided by the firefighters. She found that the issues of consent were serious ones and met the threshold for a preliminary injunction.

The second criterion that must be met is whether irreparable harm might flow if the injunction is not granted. In this case, Justice Lucas found that, if the film were released at film festivals and on the internet, it would be impossible to reverse any harm to the reputation and privacy of the applicants. She found that the harm to the applicants would be serious and irreparable.

The final criterion requires an assessment of the balance of convenience. Justice Lucas noted that the completion of the film allowed the respondent to graduate from his program. Although he had to withdraw it from the festivals that had accepted it, she found his assessment of the impact of these withdrawals on his career to be speculative. She noted that he was early in his career, with many other films in circulation, and with many other opportunities to advance his career. As for the applicants, Justice Lucas found that they would suffer permanent and irreparable harm if the film were distributed before the privacy and consent issues could be formally resolved. She granted the interlocutory injunction.

Court rules on motions in proceedings between the federal Privacy Commissioner and Facebook

Canada (Privacy Commissioner) v. Facebook Inc., 2021 FC 599

Facts

This decision involved applications by both the federal Privacy Commissioner and Facebook in two related proceedings subsequent to the Report of Findings that issued following the Office of the Privacy Commissioner's investigation of complaints relating to the misuse of Facebook data by Cambridge Analytica. In the first proceeding, the Privacy Commissioner brought an application under s. 15(*a*) of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), seeking an order against Facebook. The second proceeding is an application for judicial review brought by Facebook in relation to the Commissioner's decision to conduct and complete its investigation. Facebook alleges that the Commissioner lacked jurisdiction and that the investigation was unreasonable. It also raises procedural fairness issues.

Facebook brought a motion to have parts of the Privacy Commissioner's affidavit and some of its exhibits related to its s. 15(*a*) application struck. The Privacy Commissioner brought a motion to strike the judicial review application on two bases: 1) that Facebook, through the s. 15(*a*) application, has an alternative to judicial review; and 2) that the application for judicial review is out of time, having been filed almost a year after the Report of Findings was issued.

Decision

Facebook's motion was allowed in part. The Commissioner's motion was rejected.

Discussion

Facebook was partially successful with its application to strike parts of the lengthy affidavit submitted by the Office of the Privacy Commissioner of Canada in support of its s. 15(*a*) application. The Federal Court ruled that most of those paragraphs of the affidavit objected to by Facebook were admissible. However, it did agree that parts of the affidavit and its accompanying exhibits that related to academic articles should be struck

as impermissible hearsay. Justice Gagné noted that "expert opinion can be adduced through a properly qualified expert who can be cross-examined" (at para 36). Parts of the affidavit referring to news articles and the accompanying news articles were also struck on the basis that they appeared to be relied upon for the truth of their contents.

On the Privacy Commissioner's motion to strike Facebook's application for judicial review, Justice Gagné noted that notice of an application for judicial review should only be struck where it is "so clearly improper as to be bereft of any possibility of success" (at para 74). She considered the Commissioner's argument that s. 18.5 of the *Federal Courts Act* provided that judicial review was not available where an Act of Parliament expressly provides for an appeal to the Federal Court or for some other form of recourse that allows for the decision to be set aside. Justice Gagné, however, agreed with Facebook that s. 15(*a*) of PIPEDA was not an adequate alternative to judicial review in this case since s. 15(*a*) "grants recourse to the Commissioner and the complainant, but not to the organization under investigation" (at para 86). Although it is true that the application launched by the Commissioner would be a hearing *de novo* in which Facebook could participate, and that finding it to be an adequate alternative in this case would conserve judicial resources, she ruled that there was a debatable issue as to whether it was an adequate alternative. She noted that the procedural fairness arguments raised by Facebook in its application for judicial review were not ones normally addressed in a s. 15(*a*) application. She declined to grant the motion to strike.

As for the delay in bringing the application, Justice Gagné observed that, according to the case law, arguments about delay should be addressed at the hearing of the application for judicial review on its merits and not on a motion to strike. This is because "the interests of justice are the overarching consideration on a request for an extension of time" (at para 96), and this requires some consideration of the merits of the application. Although Justice Gagné observed that Facebook had made "minimalist" arguments in support of its application for an extension of the time limit and that she was not particularly persuaded by arguments relating to changing counsel, the need to balance interests required some consideration of the merits. Since she was unable to conclude that the application was entirely devoid of merit, she declined to strike the application for judicial review at this preliminary stage.

Dignity dimension of privacy may justify limits on open courts principle

Sherman Estate v. Donovan, 2021 SCC 25

Facts

The Trustee administering the estate of two extremely wealthy victims of a high profile and unsolved murder sought a sealing order on the probate proceedings. The order was sought on the basis that the intense curiosity about the case and the large sums of money involved would lead to significant intrusions on the privacy of beneficiaries and might even affect their personal safety. The Ontario Superior Court of Justice had issued a sealing order for a period of two years, with the possibility of renewal. The Court of Appeal had reversed this decision and lifted the sealing orders. This decision was appealed to the Supreme Court of Canada.

Decision

The unanimous court upheld the decision to lift the sealing orders.

Discussion

The open courts principle is a fundamental value in Canadian law. It is protected by the right to freedom of expression in the *Canadian Charter of Rights and Freedoms*, but it is also considered to be a principle "essential to the proper functioning of our democracy" (at para 30). By default, therefore, court proceedings and their records are open to the public.

Nevertheless, over time courts have recognized that there are some circumstances in which competing public interests require limits to be placed on the open courts principle. These limits could be in the form of anonymization, sealing orders or publication bans. Restructuring the test from *Sierra Club of Canada v. Canada (Minister of Finance)*, Justice Kasirer stated that in order to justify a limit on presumptive court openness, an applicant must demonstrate that:

(1) Court openness poses a serious risk to an important interest;

(2) The order sought is necessary to prevent this serious risk to the identified interest because reasonably alternative measures will not prevent this risk; and

(3) As a matter of proportionality, the benefits of the order outweigh its negative effects. (at para 37)

In earlier case law applying the *Sierra Club* test and involving privacy issues, the important public interest asserted was not privacy *per se*. For example, the protection of the privacy of a victim of sexual assault was linked to the important public interest in encouraging victims to come forward and report the crime. In *Sherman Estate*, however, privacy itself was asserted as the important public interest that justified a confidentiality order.

Justice Kasirer accepted that privacy could be a sufficiently important public interest. Although not all privacy interests will meet this threshold, "in some of its manifestations, privacy does have social importance beyond the person most immediately concerned" (at para 46). He noted that the courts have recognized a public interest in confidentiality which can overlap with some privacy concerns.

Justice Kasirer, for the unanimous court, began by noting that the Supreme Court of Canada has "consistently championed privacy as a fundamental consideration in a free society" (at para 5). However, in the context of open courts, case law has always recognized that a certain loss of privacy is "inherent in any court proceeding open to the public" (at para 31). He observed that "neither individual sensibilities nor mere personal discomfort associated with participating in judicial proceedings are likely to justify the exclusion of the public from court" (at para 31). Because of this, he rejected the idea that an "unbounded privacy interest" could qualify as an important public interest. Instead, he focused on those circumstances "where an aspect of a person's private life has a plain public interest dimension" (at para 32).

Justice Kasirer reviewed the Supreme Court of Canada's privacy jurisprudence. He observed that the court has considered privacy protection to be "a fundamental value in modern, democratic states" (at para 50). He stated "[t]he importance of privacy, its 'quasi-constitutional status' and its role in protecting moral autonomy continues to find expression in our recent jurisprudence" (at para 51). The importance of privacy is reflected in public and private sector data protection laws, and its protection has been recognized by the Court as a "pressing and substantial objective" (at para 52). He noted that the case law and academic literature demonstrate that privacy is more than a personal concern. However, he observed that this alone does not make it "an important public interest" for the purposes of limiting the open courts principle.

Privacy becomes a matter of significant public interest when it impacts on human dignity. Dignity "transcends the interests of the individual and, like other important public interests, is a matter that concerns the society at large" (at para 33). What is important is not the personal nature of the information; rather, it is the fact that the information's highly sensitive character would make its dissemination "an affront to [...] dignity that society as a whole has a stake in protecting" (at para 33). In other words, the interest must be one that "transcends the interests of the parties to the dispute" (at para 43).

In order to establish a privacy interest that amounts to a public interest, the individual would have to prove, with evidence, "that the information in the court file is sufficiently sensitive such that it can be said to strike at the biographical core of the individual and, in the broader circumstances, that there is a serious risk that, without an exceptional order, the affected individual will suffer an affront to their dignity" (at para 35). A core aspect of dignity is the "ability to present aspects of oneself to others in a selective manner" (at para 71). According to Justice Kasirer, dignity is undermined when individuals lose control over how they present themselves to the public.

However, beyond identifying the important public interest, an applicant for a confidentiality order or other limit on open courts must also demonstrate that there is a serious risk to this interest. This sets a high threshold. According to Justice Kasirer: "in order to preserve the integrity of the open court principle, an important public interest concerned with the protection of dignity should be understood to be seriously at risk only in limited cases" (at para 63). He cautioned that "Neither the sensibilities of individuals nor the fact that openness is disadvantageous, embarrassing or distressing to certain individuals will generally on their own warrant interference with court openness" (at para 63). Instead, in his view "[d]ignity gives concrete expression to this public order interest because all of society has a stake in its preservation, notwithstanding its personal connections to the individuals concerned" (at para 68).

Justice Kasirer provides additional guidance to determine when core biographical information is at serious risk. He notes that one consideration is the extent to which it would be disseminated absent an exception to the open courts principle. In other words, if allowing the publication of the information would lead to its broad dissemination, this suggests a serious risk. On this point, Justice Kasirer notes that technology has altered the impact of information shared in court proceedings. What might once have been heard by only a limited audience physically present in court or with access to paper court records, might today be much more easily and widely disseminated over the internet.

Other relevant considerations include the extent to which the information is already in the public domain, and the extent to which its sharing in court proceedings or records might amplify its availability.

The test requires demonstrating that the information at issue is highly sensitive or "core biographical" information, and that its disclosure via open courts would put the public interest in protecting this information at serious risk. Justice Kasirer stated:

> [...] the important public interest in privacy, as understood in the context of the limits on court openness, is aimed at allowing individuals to preserve control over their core identity in the public sphere to the extent necessary to preserve their dignity. The public has a stake in openness, to be sure, but it also has an interest in the preservation of dignity: the administration of justice requires that where dignity is threatened in this way, measures be taken to accommodate this privacy concern. Although measured by reference to the facts of each case, the risk to this interest will be serious only where the information that would be disseminated as a result of court openness is sufficiently sensitive such that openness can be shown to meaningfully strike at the individual's biographical core in a manner that threatens their integrity. (at para 85)

Having established the test, Justice Kasirer next applied it to the facts of the case before him. He found that the Trustees had failed to establish the necessary serious risk to the public interest in privacy. The information the Trustees sought to protect was not highly sensitive in nature and none of it went to the biographical core of the affected individuals. He acknowledged that the public dissemination of the information (which was very likely given the degree of media interest) would impact the beneficiaries' privacy, but it would not adversely impact their dignity. He stated: "none of this information provides significant insight into who they are as individuals, nor would it provoke a fundamental change in their ability to control how they are perceived by others" (at para 91). This was the case even though some of the beneficiaries were minors.

Justice Kasirer also found that there was no serious risk to physical safety. Although the estate at issue involved two victims of unsolved murders, and although the feared harms were grave, he found that these harms were purely speculative. He noted that the issue was not whether the individuals faced risks to their personal safety, but rather whether the disclosure of the information in open court would put their safety at risk. To limit the open courts principle, the risk of physical harm would have to be a serious one, "well grounded in the record or the circumstances of the particular case" (at para 102).

Finally, Justice Kasirer noted that the Trustees would also have had to demonstrate that the order sought was necessary to address the risks to the applicants and that its impact on the open courts principle is proportionate to that risk. In this case, he noted that the sealing order sought was an extreme limit on the open courts principle; a publication ban would be much less constraining. Although neither measure was found to be justified on the facts, it is clear that the proportionality step of the assessment is relevant to determining the extent of any limit on the open courts principle.

With the increasing ease and rapid dissemination of information over the internet, there has been growing pressure on courts to address the tension between privacy and the open courts principle. The courts have maintained the fundamental importance of the open courts principle, but have allowed some limits to openness where circumstances warrant. These circumstances must involve a serious risk to an important public interest, and the limitations must be necessary to mitigate this risk. Prior to this decision by the Supreme Court of Canada, privacy interests factored into court analyses indirectly. For example, the privacy interests of victims of sexual abuse or violence would be protected by courts, but the underlying important public interest was not privacy *per se*, it was the concern that without this protection, victims of such abuse would not come forward to seek justice.

In *Sherman v. Donovan*, the Supreme Court of Canada recognizes that privacy in its own right could be a public interest that justifies limiting the open courts principle. However, the court makes it clear that it is not just a general privacy interest that will suffice – it is acknowledged that litigants must accept a certain exposure of their private interests when they go before the courts. Rather, the privacy interest must be of such a significance that it undermines dignity. There is a strong public interest in protecting basic human dignity. The dignity interest is implicated where the personal information that would be disclosed is of a highly sensitive, core biographical nature.

This case is also interesting for the acknowledgement by the court of how technological change has impacted the privacy interests of litigants.

Professor Teresa Scassa, Canada Research Chair in Information Law and Policy, University of Ottawa

Anonymization and publication ban denied in defamation case

A.B. c. Robillard, 2021 QCCS 2550

Facts

The plaintiffs are A.B., a Quebec public figure, and his foundation. A.B.'s his name was mentioned in postings on a Quebec-based #metoo website called *Dis-son-nom*. The site allows people to post accounts of sexual abuse or misconduct at the hands of others. The plaintiff is suing for defamation, but is concerned that if his name is made public in the legal proceedings, it will amplify the impact of the allegations by drawing attention to them. He maintained that his continued employment depended entirely upon his good reputation and that publicity regarding the allegations would negatively affect his ability to continue working. A request for anonymization in a similar lawsuit against the website *Dis son nom* was recently rejected by a Quebec Court.

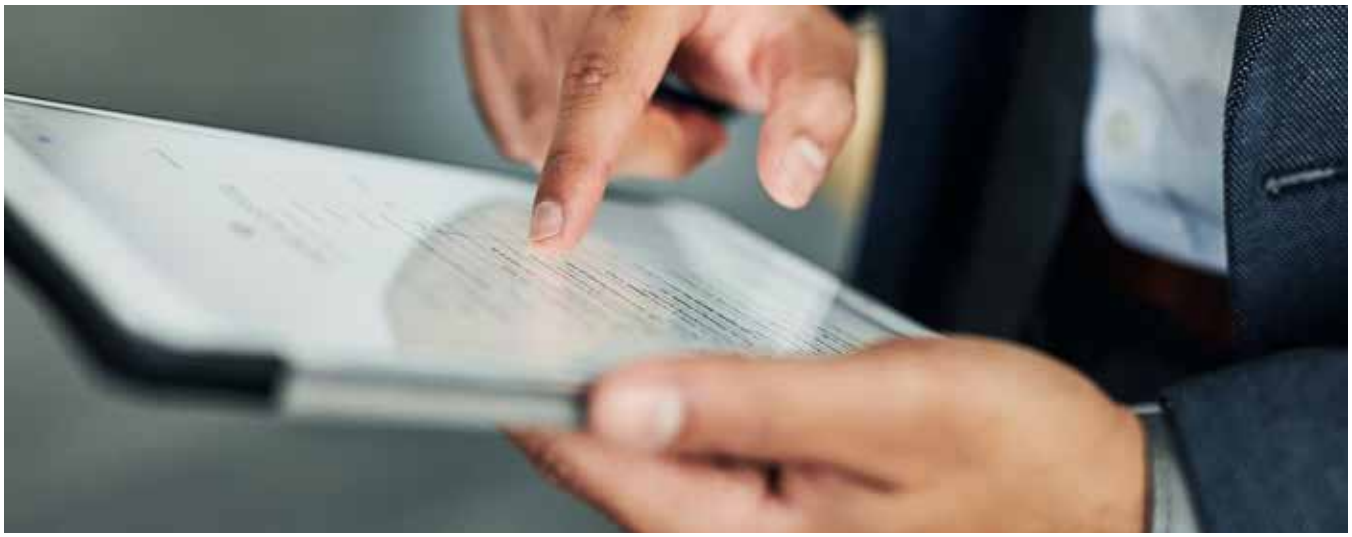
Decision

The court rejected the application for anonymization and a publication ban.

Discussion

Justice Lussier noted both the importance of the open courts principle and the need to balance it against other fundamental rights and freedoms, including the right to privacy and reputation. He noted that victims of sexual offences are typically protected by the courts by anonymization in order to ensure that they feel comfortable coming forward to seek justice. However, in the case of those denounced as abusers, Justice Lussier noted that courts are generally reluctant to grant anonymization.

Justice Lussier quoted extensively from the prior decision in *T.M. c. Dis son nom*, and noted that he would have been content to adopt the reasons from this case. However, he felt it was necessary to address the recent Supreme Court of Canada decision in *Sherman Estate*. He observed that the Supreme Court had ruled that where the privacy interest impacted on the dignity of the individual it could be a basis for limiting the open courts principle. The dignity interest, however, affects only the most intimate of details at the



biographical core of an individual's identity. Justice Lussier found that in the case before him, the applicant had failed to establish the impact on his dignity. The accusations against the applicant had already circulated on social media and the applicant had never sought a court order to prevent the publication of this information. Further, the initial accusations had appeared over a year before the hearing, and the applicant had demonstrated no loss of income over that period. Justice Lussier also observed that the applicant is a public figure who profits from having a somewhat colourful image. He found that there was no serious risk to the administration of justice if the case proceeded without anonymization. There were other means available to manage the risk to the applicant's reputation, and anonymization and a publication ban were not proportionate in the circumstances.

Insurer has no duty to defend in intrusion upon seclusion lawsuit

Demme v. Healthcare Insurance Reciprocal of Canada, 2021 ONSC 2095

Facts

The applicant sought a declaration that the respondent insurance company had a duty to defend her in a series of civil actions relating to her improper access to and misuse of patient information at the hospital where she had worked. The applicant had been found to have misused patient information in order to use an automatic dispensing machine to gain access to Percocet tablets. She faces eight civil actions related to the misuse of patient information. The claims in these actions are based upon the tort of intrusion upon seclusion.

The insurance policy covers all harms arising from an "occurrence", and these harms specifically include injury arising from "Invasion or violation of the right to privacy". They also include "Mental anguish, injury, shock, [and] humiliation" (at para 26). An occurrence is defined as "an accident, including continuous or repeated exposure to substantially the same general conditions, which results in bodily injury or property damage neither expected nor intended from the standpoint of the insured" (at para 27). The policy also specifically excludes coverage for bodily injury arising from a criminal act.

The respondent insurance company took the position that it had no duty to defend her in the lawsuits because the claims did not arise out of an "occurrence" and therefore outside of the insurance policy.

Decision

The court ruled that the insurer had no duty to defend the applicant.

Discussion

Justice Chalmers noted that the tort of intrusion upon seclusion is an intentional tort. Any invasion of privacy must therefore be deliberate. The applicant argued that she never intended to intrude upon the patients' privacy; she simply sought to gain access to narcotics. Nevertheless, Justice Chalmers ruled that the relevant intention for the

tort of intrusion upon seclusion was found in the deliberate accessing of patient files. Any negligence claims in the suit were derivative of the main claim of intrusion upon seclusion and thus did not independently trigger the duty to defend.

Justice Chalmers noted that the insurance policy requires that damages arise from an "occurrence" – in other words an accident. Here, any damage would arise as a result of the applicant's intentional accessing of patient records. Although the applicant argued that she did not intend or expect that the plaintiffs would suffer damage as a result of her actions, Justice Chalmers found that with the tort of intrusion upon seclusion, damages arise once the improper access is carried out. As a result, "the intention to access the records is an intention to cause injury." (at para 48)

Justice Chalmers went on to find that had he concluded that the claims were within the scope of the insurance policy, he would have ruled that they were excluded by the clauses which excluded coverage for intentional and/or criminal acts. The applicant argued that her principal intention was to get access to Percocet tablets and she did not intend to harm the patients. However, Justice Chalmers found that the intention to intrude upon seclusion is an intention to cause harm, and the harm alleged by the plaintiffs relates directly to the breach of their privacy. He also found that there was a causal link between the applicant's separate guilty plea to theft of the Percocet tablets and her accessing of the patient files. Because it was necessary to access the files in order to get the tablets, he found that the accessing of the files "was a necessary and integral part of the performance of the criminal act of theft" (at para 63).

The applicant had argued that finding no coverage for the tort of intrusion upon seclusion would effectively nullify the specific coverage in the policy for breach of privacy. Justice Chalmers disagreed, noting that there are many different ways in which privacy breaches could occur in the healthcare context – including the inadvertent faxing of records to the wrong recipient, sending the wrong email attachment, or the improper disposal of or storage of medical records. The coverage for privacy breaches could apply in these circumstances.

As lawsuits relating to privacy breaches become more common, and as insurance coverage is increasingly sought to protect against such breaches, the scope of coverage provided by these policies is important. An employer's insurance may cover claims against employees, but as this case makes clear, where the employee acted deliberately and intentionally, such coverage may effectively be excluded, depending on the wording of the insurance contract.

Professor Teresa Scassa, Canada Research Chair in Information Law and Policy, University of Ottawa

No breach of privacy rights in dispute between neighbours

Zeliony v. Dunn, 2021 MBQB 136

Facts

The plaintiff and the defendants shared a common entryway to their condominium units. They were the only ones sharing this entryway, which was approximately 30 square feet in area and which also contained their unit storage lockers. Shortly after the defendant moved into his condo, he found that his exterior porch light was regularly tampered with. He installed a surveillance camera inside his unit that looked outward toward the light. The camera view was subsequently blocked by a sign and the light was tampered with again. The defendant then installed an Amazon Ring doorbell, which contains a video camera with a motion detection trigger. After installation, he found that someone had taped over the camera lens. He later installed his indoor video surveillance camera over his storage locker. This camera was also interfered with.

At different points in time the condo board became involved in the dispute and the police were called by the defendant after one incident of tampering with the video cameras. It became evident that it was the plaintiff who was interfering with both the light and the cameras. The plaintiff's partner enjoyed a late cigarette on the doorstep, and the defendant's outdoor light attracted insects. As a result, they had tried to disable the light. Things escalated from there. The plaintiff argued that the placement of the doorbell camera captured the entrance to their storage locker and could also capture images of the interior of the locker when it was open. The plaintiff eventually sold her unit and moved. She claimed damages for breach of privacy, including moral damages as well as damages related to having to sell the unit at a reduced price.

Decision

The court issued summary judgment dismissing the plaintiff's claims.

Discussion

The plaintiff claimed both invasion of privacy under Manitoba's *Privacy Act* and the tort of intrusion upon seclusion, although she argued that the tort was subsumed by the legislation. In considering this claim, Justice Perlmutter found that in order to commit an invasion of privacy it was necessary to show that the violation was committed "unreasonably, and without claim of right" (*Privacy Act*, s. 2(1)). It is also a defence that the act is "reasonable, necessary for, and incidental to, the exercise or protection of a lawful right of defence of person, property or other interest of the defendant." (s. 5(c))

Justice Perlmutter considered, as part of the contextual analysis, the extent of the plaintiff's reasonable expectation of privacy. Location is a relevant, though not a determinative factor. He noted that it is still possible to have a reasonable expectation of privacy in a place that "would normally be characterized as a public place" (at para 29). In this case, the shared entryway was a common element of the condominium complex – a factor which lowered the plaintiff's expectation of privacy. Although he found that the plaintiff had an expectation of privacy with respect to her storage locker and its contents, he did not find that the placement of the cameras or their operation intruded upon her privacy. He noted in particular that there was no evidence that any recordings captured the interior of the storage locker, nor was there any evidence of the number of times she had accessed the storage locker during the relevant period. The defendant had testified that the motion detection setting for the doorbell camera was always at the lowest range of 5 feet – it would not be triggered by access to the plaintiff's storage locker. It would not even necessarily be triggered by the plaintiff entering or exiting her unit. Justice Perlmutter found that "this was not a situation of intentional constant surveillance" (at para 31).

Justice Perlmutter also found that the evidence of the plaintiff tampering with the property of the defendant was relevant to the contextual analysis. He found that the defendant's actions were "reasonable, necessary for, and incidental to, the exercise or protection of his lawful right of defence of his property." (at para 33) In his view, the

use of the cameras "was overall a reasonable and proportional response... in the totality of the circumstances". (at para 34)

Although Justice Perlmutter found no invasion of privacy and dismissed the plaintiff's other claims, he did carry out a provisional assessment of damages in the event that his decision might later be overruled. Section 4(2) of the *Privacy Act* sets out a number of considerations to take into account in assessing damages. He found that the plaintiff had established no actual damages. He reviewed the case law on moral damages and concluded that only nominal damages were warranted. Taking all of the circumstances into account, he indicated that he would have set the non-pecuniary damages at $2,000. The factors motivating this low-end award included the fact that the defendant had installed the cameras to determine who was interfering with his property.

The court in this case takes a contextual approach in determining whether the plaintiff had a reasonable expectation of privacy. It is worth noting that Justice Perlmutter found that the public or semi-public nature of the space did not eliminate the possibility of a reasonable expectation of privacy.

Professor Teresa Scassa, Canada Research Chair in Information Law and Policy, University of Ottawa

Court considers expectation of privacy in ex-employee's work computer

Pascal Métal inc. c. Turcotte, 2021 QCCS 1828

Facts

The defendant was being sued by his former employer for breach of his duty of loyalty and unfair competition. At issue in this proceeding was whether the defendant had privacy rights in the contents of his work computer which he had been compelled to turn over to the plaintiff.

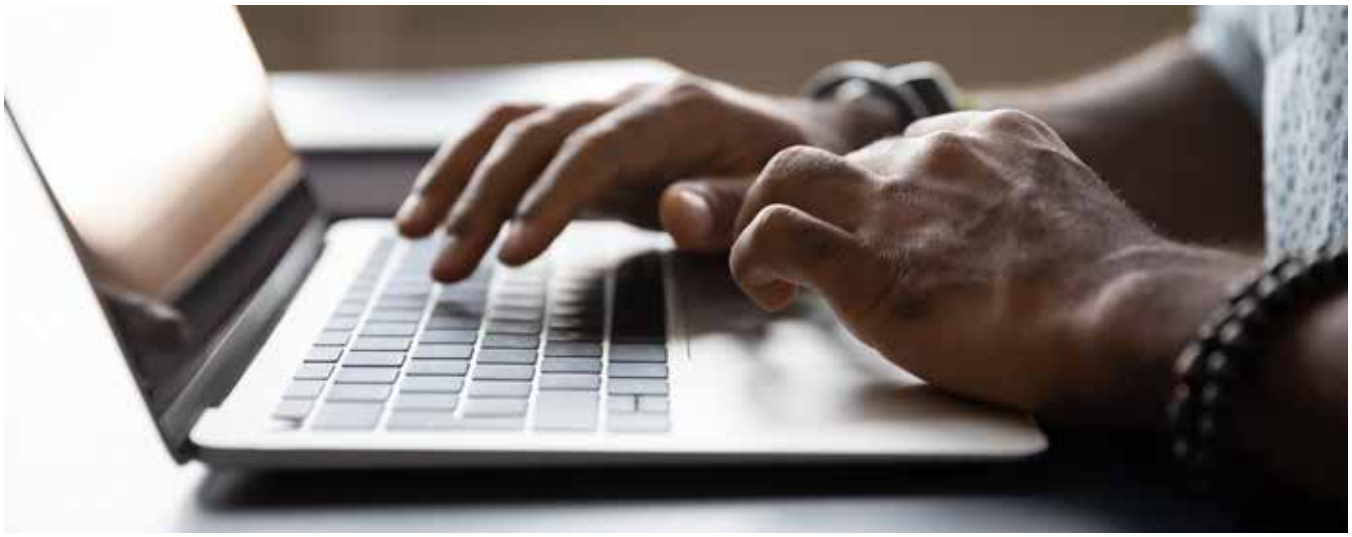
Decision

The court found that the defendant had no reasonable expectation of privacy in those elements of contents of the computer that the employer sought to introduce as evidence.

Discussion

Justice Brodeur observed that an employee using a work-issued computer could not expect to freely use it as if it were their own. Nevertheless, there might still be a reasonable expectation of privacy depending on the circumstances. For example, an expectation of privacy might exist where an employer requires an employee to use their personal computer for work purposes. Assessing the reasonable expectation of privacy in any given case requires consideration of the nature of the information being sought; the location where the information is stored; the technological measures of protection; and whether the information has been erased. Justice Brodeur noted that because of the imbalance of power in the work relationship, the employee cannot be presumed to have consented to any breach of their privacy. At the same time, however, information relating to the company's business is not information in which an employee would have a reasonable expectation of privacy. Justice Brodeur noted that what was required was a balancing of the relative interests and expectations of the parties.

In this case, Justice Brodeur found that there was no reasonable expectation of privacy in a series of notes taken by the defendant and stored on the computer. These were brief notes, and although some might possibly be reminders about personal matters, Justice



Brodeur found that there was a low expectation of privacy in information stored on an employer's computer and used in the course of employment. She found that most of the information in the notes was work-related. Certain email exchanges were also at issue – these were sent from the defendant's personal and not corporate email account. However, Justice Brodeur found that the messages were about work, even if they had been sent from a personal account.

Some of the information from the iPad that the plaintiff sought to introduce as evidence was not about the plaintiff's business. However, it was information about the competing business that the defendant was attempting to establish. Justice Brodeur found that ruling this evidence inadmissible would undermine the objectives of justice since it was highly relevant to the matters in dispute. Ultimately, she found that all of the material from the iPad that the plaintiff sought to have admitted as evidence was admissible.

About AccessPrivacy

AccessPrivacy by Osler is an integrated service offering, complementary to the Osler, Hoskin & Harcourt LLP privacy and data management law practice. We offer a suite of solutions designed to help chief privacy officers, in-house counsel and compliance professionals stay current and navigate the increasingly complex range of privacy issues facing their organizations in the private, public and broader public sectors. Our team has a unique blend of consulting and legal experience that allows us to provide timely, practical and cost-effective business solutions. For more information, visit AccessPrivacy.com.

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 400 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
accessprivacy.com

ACCESSPRIVACY BY OSLER