Class certification for privacy breaches, not so easy to come by

September 23, 2022

By Melanie Szweras, Parnian Soltanipanah and William Audet

Institutions in Canada are subject to various privacy-related statutes as well as common law torts in relation to privacy breaches. As a business owner or operator, it is important to not only understand the intersection of these acts with common law causes of action, but the ramifications of not abiding by them.

The recent decision in *Stewart v Demme* [2022 ONSC 1790] is perhaps a small comfort for businesses, as the decision signals that the bar to certification of a class action for the tort of intrusion upon seclusion, is a high one.

The common law tort of invasion of privacy, as established in *Jones v Tsige* [2012 ONCA 32], requires an intentional act that invades the plaintiff's private affairs without lawful justification, that a reasonable person would regard as highly offensive causing distress, humiliation, or anguish.[1] No proof of economic harm is required to establish this cause of action.[2] Despite the emotional turmoil that can result from an invasion of privacy, damages for intrusion upon seclusion are generally capped at approximately $20,000, with the availability of additional aggravated and punitive damages in exceptional circumstances.[3]

In *Stewart v Demme* [2022 ONSC 1790], the defendants appealed the decision of the certification judge to certify a class action for intrusion upon seclusion. One of the defendants, Ms. Demme, a nurse at the defendant hospital, improperly accessed thousands of patient records and used the information to steal painkillers from the hospital's automated medication dispensing unit, over the span of 10 years.[4] The certification judge certified the class action based on the reasoning that improper access to private health information specifically, could be considered highly offensive.[5] The Ontario Superior Court of Justice (the "Court") disagreed.

In this case, the Court considered the *impact* of the breach, as opposed to the nature of the information. They held that the patient information accessed was not particularly sensitive, it did not alter the course of treatment for the patients, nor was the information recorded or disseminated. Rather, the information was used as a means to an end – for Ms. Demme to obtain painkillers for herself. Given the minimal impact on the plaintiffs, the Court was comfortable setting aside the certification for class action.

This case sets a precedent for reviewing the impact of the privacy breach on complainants and makes it more difficult to certify future class actions. While this is a plus for businesses, proper privacy policies are still necessary. Businesses must also comply with federal and/or provincial statutory privacy laws.

Private Sector Canadian Data Protection Laws

There are four main laws that regulate how private sector organizations must collect, use and disclose personal information in the course of their commercial activities. These include:

- **Canada's** federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), overseen by the Office of the Privacy Commissioner (OPC),

- **Alberta's** *Personal Information Protection Act* ("AB PIPA"), overseen by the Officer of the Information and Privacy Commissioner of Alberta (AB OIPC),
- **British Columbia's** *Personal Information Protection Act* ("BC PIPA"), overseen by the Office of the Information and Privacy Commissioner for British Columbia (BC OIPC), and
- **Quebec's** *Act Respecting the Protection of Personal Information in the Private Sector* ("QC ARPPIPS"), overseen by Québec's Commission d'accès à l'information (CAI).

As *PIPEDA* is a federal act, it applies nationwide, except in circumstances where it has been displaced by provincial legislation which the Governor in Council has declared to be substantially similar in nature to PIPEDA. In British Columbia, Alberta, and Quebec, their respective provincial legislation governs, and most provincially regulated organizations are exempted from the application of PIPEDA. Nonetheless, *PIPEDA* still applies to federally regulated businesses with respect to their employees' personal information.[6] It also continues to apply to organizations in addition to applicable provincial laws, to personal information that crosses provincial or natural borders in the course of an organization's commercial activities. In this article, *PIPEDA*, *BC PIPA*, *AB PIPA,* and *QC ARPPIPS* may collectively be referred to as "Canadian Data Protection Acts". In addition, all provinces and territories except for Nunavut have their own legislation with respect to personal health information.[7]

The Canadian Data Protection Acts establish procedures for the relevant commissioner to receive complaints about a given organization (or initiate a complaint themselves), conduct reviews and inquiries, and issue their findings, which may be made public.[8] While the provincial commissioners have the power to issue a binding order on the organization in question, the OPC can only make a non-binding recommendation to the Federal Court.[9] Furthermore, none of the commissioners have jurisdiction to impose fines (this is subject to change in Quebec, given Bill 64).[10] However, each provincial Act lays out a number of offences the breach of which can result in monetary penalties.

Nonetheless, there are generally two avenues under which a contravening business may face financial penalties under the statutes. The first avenue is being held liable for damages for breach of the Canadian Data Protection Acts. Following a final order by the BC OIPC or AB OIPC affected individuals may bring a civil action or class action for breach of the respective legislation.[11] Under *PIPEDA*, once the OPC has submitted their report to the Federal Court, a person can initiate litigation in Federal Court.[12] While the *QC ARPPIPS* does not currently disclose a private right of action, an individual may appeal a final decision of the CAI to the Court of Quebec (this is subject to change, when Quebec's Bill 64 takes effect).[13] The second avenue is if the person or business in question commits any of the offences articulated in the Canadian Data Protection Acts. Each of the Canadian Data Protection Acts articulates its own set of offences, examples of which can include using deception or coercion to collect personal information, punishing whistleblowers, obstructing the commissioner in the course of their duties, failing to comply with the commissioner's order etc.[14] Individuals and organizations can be prosecuted for committing these offences, and liable for fines as disclosed in *PIPEDA*, *BC PIPA*, *AB PIPA*, and *QC ARPPIPS*, which range anywhere from $1000 – $100,000.[15]

Bill 64 in Quebec introduces new deterrent measures. For example, as part of its new supervisory powers, the CAI could impose monetary administrative penalties for a broad range of violations under the *QC ARPPIPS*. A person could be fined up to $50,000, or if not a natural person, the greater of $10,000,000 or the amount corresponding to 2% of worldwide turnover for the preceding fiscal year.[16] Similarly, Bill 64 will amend the current penal provisions for described offences and allow fines of $5,000-$100,000, or if not a natural person, between $15,000-$25,000,000, or an amount corresponding to 4% of worldwide turnover for the preceding fiscal year (whichever is greater).[17] In addition, Bill 64 articulates that a breach of the new *QC ARPPIPS* could result in punitive damages in an amount of at least $1000, if the breach is intentional or results from gross fault.[18] The majority of sections in Bill 64 are set to come into force September 22, 2023.

While *Steward v Demme* indicates the increased difficulty in certifying class actions, it is still vital to ensure that institutions have proper privacy policies in place to avoid liability, which can stem from common law and statutory causes of action. For more information, feel free to contact us.

---

[1] *Jones v Tsige* [2012 ONCA 32] at para 71

[2] *Ibid.*

[3] *Jones v Tsige* [2012 ONCA 32] at para 87.

[4] *Stewart v Demme* [2022 ONSC 1790] at paras 1-6.

[5] *Stewart v Demme* [2022 ONSC 1790] at paras 24-27.

[6] Office of the Privacy Commissioner of Canada, "Summary of Privacy Law in Canada" (January 2018), online <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/>

[7] McIsaac at § 5A:1.

[8] Barbara McIsaac, Kris Klein & Shaun Brown, *Law of Privacy in Canada*, (Toronto: Thomson Reuters Canada, 2022) at § 4:46; 4:64; 4:70 [McIsaac].

[9] McIsaac at § 4:46; 4:64; 4:70.

[10] McIsaac at § 4:50; 4:62; 4:81; Office of the Information and Privacy Commissioner of Alberta, "What We Do", online < https://oipc.ab.ca/what-we-do/ >

[11] *Personal Information Protection Act*, SBC 2003, c 63, s 57 [*BC PIPA*]; *Personal Information Protection Act*, SA 2003, c P-6.5, s 60(1) [*AB PIPA*].

[12] McIsaac at § 4:27.

[13] McIsaac at § 4:80.

[14] *Protection of Personal Information in the Private Sector,* SC 2000, c 5, s 28 [*PIPEDA*]; *Act Respecting the Protection of Personal Information in the Private Sector,* CQLR, c P-39.1 ss91-92.1 [QC ARPPIPS]; *BC PIPA*, s 56; AB PIPA ss 59(1), 59(2)(a), and 59(2)(b).

[15] *Ibid.*

[16] Bill 64, *An Act to Modernize Legislative Provisions as Regards the Protection of Personal Information*, 1st Sess, 42nd Leg, Quebec, 2021, cl 159 (assented to 22 September 2021) [Bill 64] < http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2021C25A.PDF>.

[17] Bill 64, cl 160.

[18] Bill 64, cl 161.