OSLER

Canadian privacy class actions evolve beyond traditional data breaches

JANUARY 11, 2023 7 MIN READ

Related Expertise

- Class Action Defence

Author: Robert Carson

In 2021, we reported that courts across the country exercised their gatekeeping role to bring an end to data breach class actions that lacked evidence of harm to the proposed class members. Ontario courts also confirmed significant limitations on the intrusion upon seclusion tort, holding that it does not apply where a defendant merely failed to prevent a hacking incident. In 2022, in a significant victory for "database defendants," the Court of Appeal for Ontario upheld this reasoning.

Many plaintiffs' lawyers now appear to be shifting their focus, at least in part, away from traditional data breach claims. Common allegations in new class action filings ranged from misuse of information to a lack of protections for children and teenagers who use online services. Canadian courts are also continuing to consider and grapple with potential new privacy torts.

Wither intrusion upon seclusion?

In 2021, the Ontario Divisional Court decided in *Owsianik v. Equifax Canada Co.* (*Owsianik*) that the tort of intrusion upon seclusion was not available in data breach cases where the information at issue was hacked by a malicious third party and the defendant merely failed to prevent the intrusion. In November 2022, the Court of Appeal for Ontario decided the appeals in *Owsianik* and other cases involving the tort.

The Court's decision is a significant vindication of the rights of database defendants. It is also an important articulation of the limits of the tort of intrusion upon seclusion and any other novel privacy torts.

The Court reasoned that there are three components to the tort of intrusion upon seclusion. First there is a conduct component, which requires the defendant to have invaded or intruded upon the plaintiff's private affairs or concerns without lawful excuse. Second, there is a state of mind requirement, which stipulates that the intrusion must have been done intentionally or recklessly. Finally, there must be consequences from the intrusion. This requires that a reasonable person would regard the intrusion as highly offensive, causing distress, humiliation or anguish. The Court found that, where information in the possession of a database defendant is accessed by a third-party hacker, the conduct component of the tort is not fulfilled for the database defendant as the database defendant cannot be said to have "invaded or intruded."

The decision is a notable victory for defendants. The plaintiffs had argued that the tort of intrusion upon seclusion was necessary for privacy class actions because "the remedies

available in contract and negligence require proof of pecuniary loss." The Court expressly rejected this logic, holding that "[it] is true that the inability to claim moral damages may have a negative impact on the plaintiffs' ability to certify the claim as a class proceeding. In my view, that procedural consequence does not constitute the absence of a remedy. Procedural advantages are not remedies."

Earlier this year – before the release of the *Owsianik* decision – several courts had grappled with the nature and limits of the tort of intrusion upon seclusion. For example, in *Stewart v. Demme*, the Ontario Divisional Court overturned an earlier decision certifying a class proceeding based on the tort of intrusion upon seclusion. The Divisional Court held that the case should not have been certified where a hospital employee had only "fleeting and incidental" access to health information in the course of another allegedly wrongful act.

In a separate decision, the Court of Appeal for Ontario rejected the same employee's appeal from a denial of insurance coverage. In so doing, the Court found that the insurance policy's intentional act exclusion applied to the claims that the employee had committed the tort of intrusion upon seclusion. The Court found that the exclusion applied regardless of whether the pleading was of an "intentional" or "intentional or reckless" intrusion.

In *Campbell v. Capital One Financial Corporation*, the B.C. Supreme Court certified a class action arising from a data breach. Despite certifying the action, the court declined the plaintiff's request to revisit B.C. jurisprudence that held that the tort of intrusion upon seclusion had been ousted by the provincial *Privacy Act*. We previously reported on the parallel Ontario action, which was dismissed.

In *Sweet v. Canada*, the Federal Court certified a privacy class action brought against the Government of Canada by taxpayers whose CRA MyAccount pages were accessed in attacks by a third party. The Federal Court found that the plaintiffs' allegations of recklessness in that case were sufficient to certify an intrusion upon seclusion claim, finding the application of the tort to database defendants was not "bound to fail."

Employer vicarious liability

Class actions in which the plaintiffs allege that an employer-defendant is liable for the wrongdoing of an employee are becoming increasingly common. These cases may become even more prominent given the Ontario jurisprudence limiting the application of the tort of intrusion upon seclusion.

For example, in *Ari v. ICBC*, the B.C. Supreme Court granted summary judgment on certain certified legal issues in a factually remarkable privacy class action. The defendant, the Insurance Company of British Columbia (ICBC), operates B.C.'s public vehicle insurance scheme. The ICBC had employed an adjuster who, for pay, looked up and provided address information associated with licence plates provided by a third party. Unbeknownst to the adjuster, the third party was acting on behalf of a fourth party who had a drug-induced paranoid belief that he was being targeted by the Justice Institute of British Columbia and had observed the licence plate numbers in the Justice Institute parking lot. The fourth party subsequently carried out arson and shooting attacks on certain of the addresses. He was sentenced to a substantial prison term.

This interesting fact pattern resulted in a class action proceeding against the ICBC. In its decision, the B.C. Supreme Court found that the plaintiff had established that the adjuster had breached the *Privacy Act*. The Court also found that, although the ICBC itself was innocent, it was vicariously responsible for the adjuster's misconduct because her conduct fell within an area of risk that was created by the ICBC's collection of information. The Court

further rejected the ICBC's argument that the attacks by the fourth party were unforeseeable or a *novus actus interveniens.*

The certification requirement of 'some basis in fact' remains a meaningful hurdle in privacy class actions

Courts across the country continue to confirm that plaintiffs in privacy actions cannot obtain certification without evidence that the proposed class was actually affected by the alleged breach of privacy. Two examples involve claims against Facebook, Inc.

In the first case, *Simpson v. Facebook, Inc.*, the plaintiff alleged that a third party named Cambridge Analytica had obtained information about Facebook users from a third-party application developer. The Ontario Superior Court of Justice dismissed the plaintiff's certification motion on the basis that there was no evidence that any Canadian user data was shared with Cambridge Analytica. As a result, there was no justification for a class proceeding.

In upholding this decision on appeal, the Divisional Court emphasized that the plaintiffs bore an evidentiary burden to show "that a common issue exists beyond a bare assertion in the pleadings." Osler defended Facebook in this action.

In *Chow v. Facebook, Inc.,* the B.C. Supreme Court declined to certify a case in which the plaintiffs alleged that Facebook misused call and text log data from users of its Messenger application on Android phones. The Court found that plaintiffs had failed to establish any basis in fact for their allegations that Facebook "collected, used, retained and commercialized call and text data and profited from that collection at users' expense." Absent a basis for the allegations there was similarly no justification for a class proceeding. Osler also defended Facebook in this action.

A pivot away from data breach claims

We have previously reported that plaintiffs are increasingly bringing class actions alleging that the defendants misused or improperly collected data, rather than claims that they were victims of a data breach. Numerous misuse of data cases were commenced in 2022. These include a series of class actions alleging improper sharing of information regarding new mothers by the provincial governments. We also saw a number of prominent data-misuse settlements in 2022, including settlements concerning the allegedly improper collection and use of geolocation information. The *Owsianik* decision will likely contribute to this trend.

Conclusion

Despite the proliferation of privacy class action filings, courts across Canada continue to make it clear that certification is not a rubber stamp and that it will not automatically follow from a data breach or incident. Courts expect plaintiffs to show that they were actually affected by the incident. While it remains critical for businesses to respond quickly and effectively when data incidents occur, defendants have a variety of tools to defend privacy claims or to resolve them early on. It can be valuable to seek early advice on how best to implement such tools in circumstances where there is a risk of a class action or where a claim is commenced.