WeirFoulds LLP

Court of Appeal Clarifies Scope of the Tort of Intrusion Upon Seclusion in Cases of Data Breaches

January 11, 2023

By Lia Boritz

On November 25, 2022, the Ontario Court of Appeal released a trilogy of decisions (*Owsianik v Equifax Canada Co.*, 2022 ONCA 813, *Obodo v TransUnion of Canada, Inc.*, 2022 ONCA 814, and *Winder v Marriott International, Inc.*, 2022 ONCA 815, collectively, the "**Data Breach Cases**") which all related to whether the tort of intrusion upon seclusion was a viable cause of action against defendants who, for commercial purposes, collect and store the personal information of others ("**Database Defendants**") and whose failure to take adequate steps to protect that information allowed third-party hackers to access and/or use the personal information.

Each of *Owsianik, Obodo* and *Winder* were class action proceedings at the certification stage and, in each case, the court below refused to certify the intrusion upon seclusion claim (although other causes of action in each claim were allowed and were not in issue on appeal).

Ultimately, the Court of Appeal determined that the Database Defendants could not be held liable for the tort of intrusion upon seclusion because they had not done anything that would constitute an act of intrusion or invasion into the privacy of the plaintiffs. Rather, the actual acts of intrusion were committed by unknown, third-party hackers.

The Tort of Intrusion Upon Seclusion

The tort of intrusion upon seclusion was first recognized by the Ontario Court of Appeal in *Jones v Tsige*, 2012 ONCA 32. The Court of Appeal set out the elements of the tort of intrusion upon seclusion as follows:

- the defendant must have invaded or intruded upon the plaintiff's private affairs or concerns, without lawful excuse (the conduct requirement);
- the conduct which constitutes the intrusion or invasion must have been done intentionally or recklessly (the state of mind requirement); and
- a reasonable person would regard the invasion of privacy as highly offensive, causing distress, humiliation or anguish (the consequence requirement).

In establishing this new tort, the Court of Appeal specifically recognized that technological changes posed a novel threat to the right of privacy and that the common law would likely have to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form.[1]

The Court of Appeal held that where the tort of intrusion upon seclusion is established, the plaintiff could recover "symbolic" or "moral" damages of up to $20,000 without any proof of loss.

Application of the Tort of Intrusion Upon Seclusion to Data Breach Cases

Cybersecurity attacks and data breaches occur regularly, and it is not surprising that the victims of data breaches would attempt to use the tort of intrusion upon seclusion to hold those parties whom they entrust to store highly sensitive and personal information liable for their failure to adequately protect this information.

However, in *Jones*, the conduct component of the tort of intrusion upon seclusion was never in dispute. The defendant had repeatedly accessed the private banking records of the plaintiff, the former wife of the defendant's common-law partner, without justification. In the Data Breach Cases, the conduct component of the tort was very much at issue.

In *Owsianik*, the conduct which was alleged to have constituted the interference with the plaintiffs' privacy was the Database Defendants' failure to take appropriate steps to protect the plaintiffs' personal information against unauthorized access. On the alleged facts, Equifax (the defendant in *Owsianik*) did not unlawfully access any information. No one acting on Equifax's behalf, or in consort with Equifax, did so. No one for whom Equifax could be held vicariously liable accessed any private information. A third-party stranger to Equifax accessed the information. It may have been possible to find that Equifax acted recklessly in respect of its storage and protection of the plaintiff's personal information. However, the Court of Appeal held that it is not sufficient for the Database Defendants to have acted recklessly:

The defendant must either intend that the conduct which constitutes the intrusion will intrude upon the plaintiffs' privacy, or the defendant must be reckless that the conduct will have that effect. If the defendant does not engage in conduct that amounts to an invasion of privacy, the defendant's recklessness with respect to the consequences of some other conduct, for example the storage of the information, cannot fix the defendant with liability for invading the plaintiffs' privacy.[2]

As a result, the claim against Equifax failed at the conduct component of the tort of intrusion upon seclusion. The Court of Appeal went onto note that to award "moral damages" against Equifax for what is essentially negligence or breach of contract ran contrary to the purposes underlying the award of such damages:

Moral damages are awarded to vindicate the rights infringed, and in recognition of the intentional harm caused by the defendant. These purposes are served only if the damages are awarded against the actual wrongdoer, that is the entity that invaded the privacy of the plaintiff.[3]

The Court of Appeal applied its findings in *Owsianik* to the other Data Breach Cases, rejecting the class certification of the intrusion upon seclusion claim in each proceeding. In all cases, the Court of Appeal left open the possibility that the Database Defendants could be held liable for any damages flowing from their negligence, or from breaches of any contractual, or statutory duties potentially owing to the plaintiffs or other class members.

Takeaways

As noted by the Court of Appeal in *Owsianik*, it may be that the existing common law remedies do not adequately encourage Database Defendants to take all reasonable steps to protect the personal information under their control. As a result, it is up to Parliament and provincial legislatures to enact legislation to protect informational privacy and to provide remedies against Database Defendants who do not take appropriate steps to secure the information under their control.

Steps have started to be taken in this regard. For example, at the federal level, Bill C-27 (now in its second reading) would enact the *Consumer Privacy Protection Act*, which creates a private right of action against an organization who contravenes the Act for damages for loss or injury that the individual has suffered as a result of the contravention. However, this remedy would only be available if the Federal Privacy Commissioner or the Personal Information and Data Protection Tribunal makes a final determination

that there has been a contravention of the proposed *Consumer Privacy Protection Act*.

The information and comments herein are for the general information of the reader and are not intended as advice or opinion to be relied upon in relation to any particular circumstances. For particular application of the law to specific situations, the reader should seek professional advice.

[1] *Jones v Tsige*, 2012 ONCA 32 at para 68.

[2] *Owsianik v Equifax Canada Co.*, 2022 ONCA 813 at para 59.

[3] *Owsianik* at para 77.

For more information or inquiries:

Lia Boritz

Toronto
416.947.5067

Email:
lboritz@weirfoulds.com

Lia Boritz is a Partner in the Litigation & Dispute Resolution practice group at WeirFoulds. She has a broad litigation practice which includes civil, commercial and employment matters.