



Paul-Erik Veel
416-865-2842
pveel@litigate.com



Brianne Westland
416-865-2907
bwestland@litigate.com

November 28, 2022

Intrusion Upon Seclusion Without Being the Intruder? The Ontario Court of Appeal Limits Claims Against Database Holders

Last Friday, the Ontario Court of Appeal released decisions in *Owsianik v Equifax Canada Co*, *Obodo v Trans Union of Canada, Inc.*, and *Winder v Marriott International, Inc.*—a trilogy of decisions clarifying whether the tort of intrusion upon seclusion applies to the owners of databases when there are data breaches caused by third party hackers. Thankfully for database owners, the Court of Appeal concluded that intrusion upon seclusion cannot apply in those circumstances.

The Trilogy

In *Owsianik*, the defendants (Equifax) offer a credit reporting and credit protection service around the world. To do this, Equifax collects and aggregates a large amount of sensitive personal and financial data about individuals, which they organize and analyze in order to assess credit worthiness. Equifax collects and uses this data without consumer's consent. Equifax also accumulates and stores information pertaining to its clients who purchase credit protection services. Between mid-May and late July 2017, unidentified hackers gained access to Equifax's database and the personal information stored on it. Equifax notified its customers of the breach in September 2017.

The defendant in *Obodo* (Trans Union) is also a credit reporting company similar to Equifax. As in *Owsianik*, Trans Union's database was subject to a breach by an unknown hacker. In this case, the hack was accomplished by using credentials stolen from a Trans Union customer. It occurred over a two-week period in June and July 2019.

In *Winder*, the defendants (Marriott) are a hotel chain that maintains a database of customer information. In November 2018, Marriott discovered that hackers had been accessing the database over a four-year period.

In all three cases, the plaintiffs commenced class actions as a result of the breaches and tried to certify claims for intrusion upon seclusion. In all three cases, the plaintiffs pointed to the failure of the defendants to maintain the security of the

information in their possession as grounding their liability for intrusion upon seclusion.

The History

In *Owsianik*, the Superior Court certified intrusion upon seclusion as a common issue in 2019, finding that the merits of the intrusion upon seclusion claim should be determined at trial, and there was no settled law on whether a defendant who recklessly permitted a hacker attack on a database was liable for intrusion upon seclusion. This decision was overturned on appeal by a panel of the Divisional Court, with a lengthy dissent written by Justice Sachs. The Divisional Court decision authored by Justice Ramsay (with Justice McWatt concurring) found that the tort of intrusion upon seclusion has to do with the humiliation and emotional harm suffered by an intrusion into private affairs, and had “nothing to do with a database defendant”. They found that there was no “intrusion” by Equifax, and to extend liability to a defendant who fails to prevent intrusion would risk a danger of “opening the floodgates”. The decision also cited to *Atlantic Lottery Corporation v Babstock* for the proposition that novel claims doomed to fail should be disposed of at an early stage.

In *Obodo*, the Superior Court in 2021 declined to certify intrusion upon seclusion as a common issue, finding that the decision of the Divisional Court in *Owsianik* was binding authority for the proposition that “the tort of intrusion upon seclusion ‘has nothing to do with a database defendant’.” Leave to appeal was refused by the Divisional Court.

In *Winder*, the Superior Court in 2022 declined to certify intrusion upon seclusion as a common issue, as it found the case to be indistinguishable from *Owsianik* and *Obodo*.

The Court of Appeal

Acknowledging the similarity across the three cases, the Court of Appeal focused its reasons on *Owsianik*, answering the question of whether the tort of intrusion upon seclusion can apply to a database defendant who failed to take adequate steps to protect the information, thereby allowing third-party hackers to access or use the information.

The Court of Appeal has now definitively answered this in the negative.

In its decision, the Court of Appeal first engaged in an in-depth discussion about the application of *Babstock* to novel issues at the certification stage, affirming that courts have the ability to decide questions of law at the pleadings stage, and should do so. The Court of Appeal found that this power is justified in a case like this where:

- (1) the legal question to be answered can be answered on the facts as pleaded;
- (2) there was no unfairness to either party in deciding the merits of the legal question on the pleadings motion;
- (3) the issue was fully briefed and argued on the pleadings motion; and
- (4) the institutional considerations articulated in *Babstock* favoured deciding the legal question on the merits.

The Court of Appeal also commented on the unfairness to defendants where a claim for intrusion upon seclusion, that could have been decided at the certification motion, is permitted to continue beyond the certification stage. This is because intrusion upon seclusion does not require proof of actual loss, the nature of damages in intrusion upon seclusion cases offers support to the plaintiffs in an argument that a class proceeding is the preferable procedure. This gives plaintiffs a “leg up” in both a certification motion and any resulting settlement negotiations.

Second, the Court of Appeal clarified that the tort of intrusion upon seclusion requires active conduct by the defendant to invade privacy. An allegation of negligent storage of information is not conduct that amounts to an “intrusion into” or “an invasion of” the plaintiff’s privacy. The conduct of the defendant must amount to an intentional intrusion.

Third, the Court of Appeal held there are significant policy reasons not to extend the tort of intrusion upon seclusion beyond its current bounds. The Court of Appeal expressed great reservation about setting a precedent that could allow other intentional torts to apply to a failure by a defendant to prevent an intentional tort being committed by a third party. The Court of Appeal did not find a need to extend the tort of intrusion upon seclusion, as the law already provides remedies for this sort of alleged misconduct, such as through the law of negligence and contract.

Finally, the Court of Appeal noted that the plaintiffs’ concerns about a lack of remedy if intrusion upon seclusion were not certified as a common issue came down to the unavailability of damages under contract and negligence if a plaintiff cannot prove pecuniary loss. The Court of Appeal dismissed this

concern, finding that the requirement to prove pecuniary loss under contract and tort merely puts the plaintiffs in the same position as anyone else who advances this sort of claim. The fact that the unavailability of moral damages in the class proceedings context may affect the plaintiffs' ability to certify the claim does not constitute an absence of a remedy.

The Implications

The tort of intrusion upon seclusion has been increasingly popular in the class action space, in large part due to the availability of moral damages that can be awarded, without proof of any economic loss, once the tort has been proven. Moral damages can be a boon to class action plaintiffs who can point to such damages as a reason in favour of certifying a class proceeding as the preferable procedure and making the damages available on an aggregate level. Moreover, while the quantum of damages on an individual level is relatively modest, in the class context, even the *Jones v Tsige* cap on damages (set at \$20,000 in 2012), when multiplied across hundreds or thousands of individuals in a class, represents a very large potential liability for defendants.

The Court of Appeal's decision brings welcome certainty to the law in this area. Companies who hold data can breathe a sigh of relief. In the case of data breaches, they can still be subject to claims for negligence and breach of contract, but the damages should be limited to actual losses rather than the potentially much larger moral damages available under intrusion upon seclusion.

For privacy law generally, the clarification from the Court of Appeal that the tort of intrusion upon seclusion is an intentional tort, which is narrowly confined to cases where a defendant "engaged in the proscribed conduct with a specified state of mind", is welcome. The Court of Appeal reinforced the purpose of "moral damages" in the case of intrusion upon seclusion as being in part to recognize "the intentional harm caused by the defendant", and thus only available against an intentional wrongdoer. The fact that this removes what has to this point been an advantage to plaintiffs is not relevant. As the Court clarified: "Procedural advantages are not remedies".

Privacy class actions will certainly continue. However, in class actions involving database defendants, it is likely the class actions will be more often limited to scenarios where there are actual, provable losses to class members. Class actions for intrusion upon seclusion should, moving forward, be properly limited to those where the defendant itself deliberately invaded the privacy of the class.

Finally, the Court of Appeal's discussion of *Babstock* reaffirms

both the powers of a judge on a certification motion to decide questions of law and prevent common issues from being certified where there is no prospect of success, and reaffirms the importance of doing so. We expect to see *Owsianik* cited at certification motions going forward in all contexts by defendants seeking to limit the common issues certified. As the Court of Appeal rightly points out, this may have implications for the arguments that can be advanced by the plaintiffs, such as arguments regarding preferable procedure, and the availability of aggregate damages.