THE EXCLUSION OF INTRUSION UPON SECLUSION: *ONTARIO COURT OF APPEAL DEFINITIVELY DETERMINES THAT "DATABASE DEFENDANTS" CANNOT BE HELD LIABLE FOR INTRUSIONS COMMITTED BY THIRD-PARTY HACKERS*

Posted on December 1, 2022

Categories: Insights, Publications

On November 25, 2022, the Court of Appeal for Ontario (the "**Court**") released a trio of decisions that materially impact the viability of class actions against organizations that fall victim to a cybersecurity attack. More particularly, the Court considered and definitively determined the issue of whether organizations that collect and store personal information about individuals for commercial purposes ("**Database Defendants**"), can be held liable for the tort of "intrusion upon seclusion", if they fail to take adequate steps to protect the information from third-party "hackers".

In *Owsianik v Equifax Co.* ("***Owsianik***"),[1] *Obodo v Trans Union of Canada, Inc.* ("***Obodo***")[2] and *Winder v Marriot International, Inc.* ("***Winder***")[3] (collectively, the "**Intrusion Cases**"), three proposed class actions, the Court found that Database Defendants cannot be held liable for an intrusion upon seclusion caused by unknown, malicious third parties. While plaintiffs may continue to pursue other claims against Database Defendants, such as negligence or breach of contract, other causes of action often require proof of actual pecuniary loss. Accordingly, by eliminating the potential for plaintiffs to allege intrusion upon seclusion (which allows for claims of "symbolic" or "moral" damages), the Court has weakened support for the argument that a class proceeding is the preferable procedure for claims against Database Defendants that are subject to a cyberattack.

The Underlying Breaches

In *Owsianik*, hackers gained unauthorized access to Equifax's servers in 2017. The breach allegedly impacted personal information about approximately 20,000 Canadians, including social insurance numbers, government identification numbers and payment card information.

In *Obodo*, hackers used stolen account credentials to gain access to Trans Union's database through a customer portal, allegedly resulting in unauthorized access to personal information about approximately

37,000 Canadians, including social insurance numbers and information on debts owing.

In *Winder*, hackers gained access to Marriot's reservation database, allegedly resulting in unauthorized access to personal information, including some customers' passport numbers and payment card information.

None of the Intrusion Cases involved allegations that the defendant acted together with the hackers, or otherwise authorized the activities of such third parties. Rather, in each case, the plaintiffs alleged that the Database Defendant failed to take adequate steps to protect class members from intrusions upon their privacy by the unknown hackers.

Intrusion upon Seclusion

The Court first recognized the tort of intrusion upon seclusion *Jones v. Tsige*[4] in circumstances where a bank employee repeatedly accessed the private banking records of her husband's ex-wife without any lawful justification. In recognizing that the facts of the case demanded a remedy, the Court laid out the following elements for the novel cause of action:

1. The defendant must have invaded or intruded upon the plaintiff's private affairs or concerns, without lawful excuse;
2. The conduct that constitutes the intrusion or invasion must have been done intentionally or recklessly; and
3. A reasonable person would regard the intrusion or invasion of privacy as highly offensive, causing distress, humiliation or anguish.

Moreover, the Court held that plaintiffs can recover "symbolic" or "moral" damages of up to $20,000, without any proof of loss, for intrusions upon seclusion, which is particularly significant in the context of class action cases.

In establishing the new tort, the Court acknowledged the unprecedented power of organizations to capture and store vast amounts of personal information using modern technology, and indicated that the common law must evolve in response to this modern technological environment.[5] In particular, the Court described risks related to the fact that highly sensitive personal information can now be accessed and collated with relative ease, including financial and health information as well as data related to individuals' whereabouts, communications, shopping habits and more.

Application of Intrusion Upon Seclusion to Database Defendants

Given the commentary in *Jones* regarding the risks associated with collecting, storing and aggregating large amounts of personal information, and the ability of plaintiffs' to claim damages without proof of loss, it is

unsurprising that the tort of intrusion upon seclusion has frequently been alleged in class action lawsuits following a data breach.

However, the first element of the tort requires that the defendant must invade or intrude upon a plaintiff's private affairs or concerns. In the Intrusion Cases, the Court found that the Database Defendants did not do anything that could constitute an act of intrusion or invasion into the privacy of the plaintiffs. Rather, the intrusions were committed by unknown third parties that acted contrary to the interests of the companies they attacked.

The Court also clarified that, although "recklessness" is sufficient to establish liability for intrusion upon seclusion (i.e., not just intentional conduct), this is only relevant if the defendant commits an intrusion or invasion of privacy. Recklessness with respect to the consequences of negligent storage of data does not render a Database Defendant liable for an intentional invasion of privacy committed by an independent third-party hacker.

Why the Intrusion Cases are Important

The Court's finding that Database Defendants cannot be liable for the tort of intrusion upon seclusion for failing to prevent a cybersecurity attack by an unknown third party stands as a practical impediment to the viability of class actions in this context.

As noted above, the tort of intrusion upon seclusion allows claims for symbolic or moral damages, without proof of loss, whereas most other potentially applicable causes of action require plaintiffs to prove actual losses in order to recover damages. For this reason, it is often difficult to certify a claim based in negligence or breach of contract as a class proceeding. Therefore, allowing intrusion upon seclusion claims against Database Defendants in the past, despite uncertainty as to the legal viability of such claims, gave plaintiffs "a leg up" in the certification process and in any settlement negotiations.[6] The Court acknowledged that eliminating the ability of plaintiffs to claim moral damages for intrusion upon seclusion claims against Database Defendants may have a negative impact on the their ability to certify the claim as a class proceeding, but rejected the argument that this would leave plaintiffs without a remedy.

The Court also sought to close any remaining loopholes in *Obodo* and *Winder*, as follows: (1) In *Obodo*, the Court determined that Database Defendants cannot be held vicariously liable for breaches caused by unauthorized third parties (unlike for intrusions committed by employees); and (2) In *Winder*, the Court considered, and rejected, the argument that the defendant committed an invasion of privacy by collecting and storing customers' personal information in a manner that did not reflect the representations made to such customers, or the company's legal obligations, with respect to maintaining the security of their information.

A Cautionary Note

Although the Intrusion Cases clearly establish that the tort of intrusion upon seclusion is not applicable to Database Defendants that experience data breaches caused by unauthorized third parties, the story may not end here.

Firstly, there have been a number of class action lawsuits filed in Canada as a result of breaches committed by internal threat actors. As discussed in *Obodo*, it is possible for an employer to be held vicariously liable for the actions of its employees. Accordingly, claims of intrusion upon seclusion could still be certified against employers that directly or indirectly enable breaches by employees.

Secondly, although Ontario's highest court has determined that intrusion upon seclusion is not applicable to organizations that fail to adequately safeguard personal information, it is possible that leave will be sought (and granted) to the Supreme Court of Canada.

Finally, as noted in *Jones*, the risk to privacy presented by the accumulation of data is real. The need to address this risk is reflected in upcoming and proposed changes to privacy legislation in Canada, which provides for enhanced enforcement mechanisms including a private right of action for individuals against organizations that breach their statutory obligations to protect personal information.

[1] *Owsianik v. Equifax Canada Co.*, 2022 ONCA 813.
[2] *Obodo v. Trans Union of Canada, Inc.*, 2022 ONCA 814.
[3] *Winder v. Marriott International, Inc.*, 2022 ONCA 815.
[4] *Jones v. Tsige*, 2012 ONCA 32.
[5] *Jones v. Tsige*, 2012 ONCA 32 at paras 67-68.
[6] *Owsianik v. Equifax Canada Co.*, 2022 ONCA 813 at para 49.

by Lyndsay Wasser and Mitch Koczerginski

A Cautionary Note