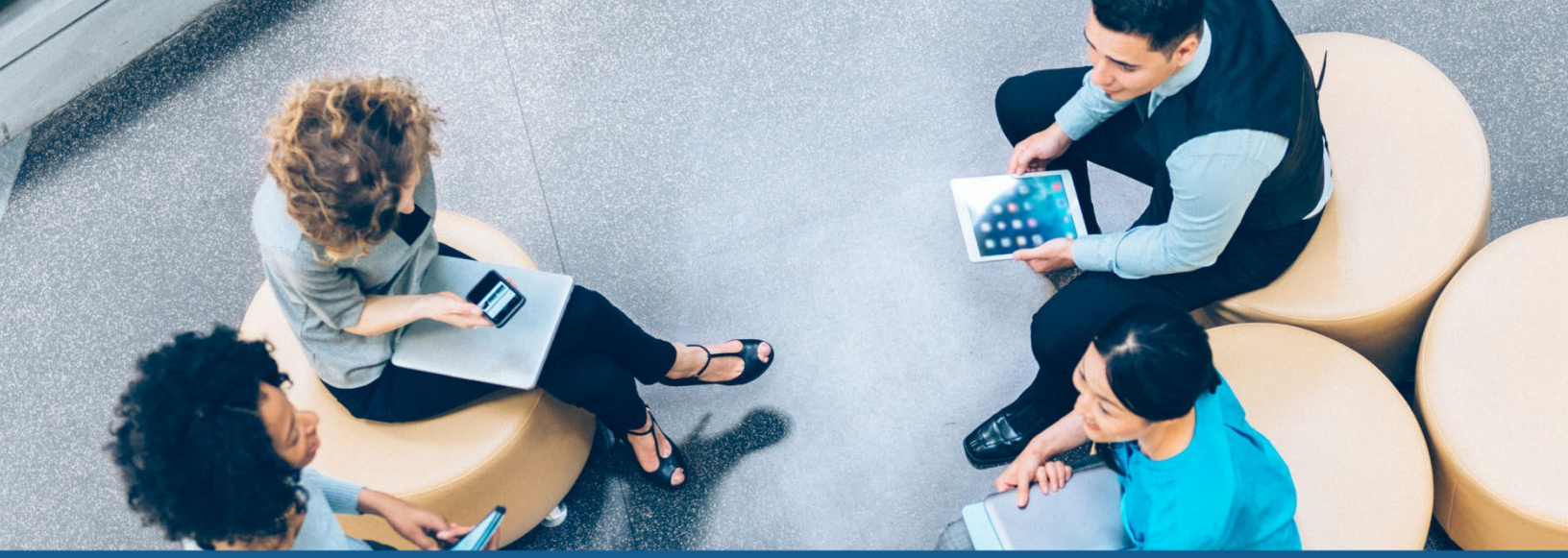

What's New in HR Law

Court of Appeal Confirms Database Defendants Are Not Liable for Data Breaches by Third Parties

December 9, 2022 | By **Spencer Knibutat**

Bottom Line

In a recent trilogy of decisions, the Ontario Court of Appeal held that organizations do not breach the tort of intrusion upon seclusion where they have been subject to a data breach caused by a third-party "hacker" or independent "threat actor".

The Privacy Tort of Intrusion upon Seclusion

In its 2012 decision of *Jones v. Tsige*, the Ontario Court of Appeal first recognized the common law tort of intrusion upon seclusion. Since the tort's recognition a decade ago, recurring questions have been raised across dozens of class action lawsuits regarding how this tort should be interpreted and applied.

One key question is whether organizations are liable for the tort of intrusion upon seclusion where independent threat actors gain unauthorized access to personal information in the organizations' control. Such organizations (often called "Database Defendants") are sued in lieu of the hackers responsible for the breach, as the hackers are often difficult to identify and Database Defendants have sufficiently "deep pockets" to compensate the plaintiffs' perceived and actual losses.

Despite this issue being frequently raised in Canadian lawsuits, Ontario courts have refrained from deciding whether Database Defendants can be found liable for failing to adequately protect data from being breached by an independent or third-party hacker. The resulting uncertainty has caused significant concern for organizations subject to third-party data breaches, as they remain unaware of the scope of their potential liability.

The Trilogy

Finally, on November 25, 2022, the Ontario Court of Appeal directly addressed the issue of Database Defendants' liability in a trio of decisions arising out of three separate appeals: *Owsianik v. Equifax Canada Co.*, 2022 ONCA 813 ("*Owsianik*"); *Obodo v. Trans Union of Canada, Inc.*, 2022 ONCA 814 ("*Obodo*"); and *Winder v. Marriott International, Inc.*, 2022 ONCA 815 ("*Winder*"). Given the shared issues and similar facts at hand, the Court set out the majority of its reasoning in *Owsianik* and addressed a few additional issues in *Obodo* and *Winder*, respectively.

Relevant Facts

The three appeals in the decision trilogy related to proposed class actions in which representative plaintiffs alleged breaches of the tort of intrusion upon seclusion by Database Defendants. The defendants in each case allegedly failed to take proper steps to store and secure data within their custody from unauthorized access by third-party hackers.

In prior litigation, the defendants argued that the lawsuits against them should not be certified as class actions because the plaintiffs' claims did not disclose a proper cause of action as required by section 5(1)(a) of the *Class Proceedings Act, 1992*.

The representative plaintiff in *Owsianik* initially succeeded in certifying an intrusion upon seclusion claim as part of a class action. However, the Ontario Divisional Court reversed the certification decision and held that the tort did not apply as the information in question had been accessed by a third-party hacker acting independently of the defendant.

The Decision in *Owsianik*

In *Owsianik*, the Ontario Court of Appeal confirmed the following test from *Jones v. Tsige* for the tort of intrusion upon seclusion:

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

Applying this test, the Court held that Database Defendants are not liable for intrusion upon seclusion where independent threat actors or third-party hackers access data without authorization.

First, the Court concluded the defendant did not commit an "invasion" or "intrusion" into the putative class members' private affairs. The representative plaintiff alleged that the defendant had breached the tort of intrusion upon seclusion by failing to "take appropriate steps to guard against unauthorized

access to sensitive financial information involving the Class Members' private affairs or concerns." The Court, however, found that, at most, the defendant had failed to meet its obligations to the plaintiffs to protect their privacy interests. There was no conduct by the defendant that amounted to an intrusion into or invasion of the plaintiff's privacy, so the Conduct Requirement was not established.

Second, the Court rejected the representative plaintiff's argument that the data breach was caused by the defendant's recklessness. Under the State of Mind Requirement, the privacy-invading conduct must be done intentionally or recklessly. As the defendant had not engaged in an invasion of privacy, any recklessness relating to the defendant's other conduct could not satisfy the State of Mind Requirement.

The Court also firmly refused to extend the tort of intrusion upon seclusion to apply to entities that fail to adequately protect information in their possession. According to the Court, to impose liability of Database Defendants for the tortious conduct of unknown hackers would be a "giant step in a very different direction" from how the law had developed.

The foregoing reasoning was relied upon by the Court in *Obodo* and *Winder*, and resulted in the dismissal of all three appeals in the trilogy.

Check the Box

While this trilogy of decisions brings some relief, organizations should remain mindful that they may still face liability in relation to data breaches that occur. For instance, where a threat actor is an employee or otherwise affiliated with the organization, the organization may be vicariously liable for the actor's tortious conduct. Further, organizations might be liable for negligence or violations of their contractual/statutory obligations if a data breach arises from the organization's inadequate storage, protection, disposition, or transfer of information.

To mitigate these risks, organizations storing large quantities of data should, in consultation with legal counsel, take proactive steps to protect the personal information in their custody and to prevent and detect data breaches where possible. This may include implementing policies and procedures to prevent unauthorized data access and training employees on cybersecurity laws and best practices.

Need More Information?

For more information or assistance with issues regarding privacy law or data breaches, contact Spencer Knibutat at sknibutat@filion.on.ca, or your regular lawyer at the firm.

Filion Wakely Thorup Angeletti LLP
management labour and employment law

PROUD MEMBER OF L&E GLOBAL
Alliance of Employers' Counsel Worldwide

aec ADVOCATES for EMPLOYERS of CANADA

Toronto
Bay Adelaide Centre
333 Bay Street
Suite 2500, PO Box 44
Toronto, Ontario M5H 2R2
tel: 416.408.3221
fax: 416.408.4814
toronto@filion.on.ca

London
252 Pall Mall Street, Suite 100
London, Ontario N6A 5P6
tel: 519.433.7270
fax: 519.433.4453
london@filion.on.ca

Hamilton
1 King Street West
Suite 1201, Box 57030
Hamilton, Ontario L8P 4W9
tel: 905.526.8904
fax: 905.577.0805
hamilton@filion.on.ca

Kitchener-Waterloo
137 Glasgow Street
Suite 210, Office 175
Kitchener, Ontario N2G 4X8
tel: 519.433.7270
fax: 519.433.4453
kitchener-waterloo@filion.on.ca