Ontario Court of Appeal rules against plaintiffs in trilogy of privacy class actions

December 02, 2022

In a highly anticipated trilogy of privacy class action certification appeals, the Ontario Court of Appeal refused to certify three class actions based on the tort of intrusion upon seclusion. In Oswianik v. *Equifax Canada Co.*, *Obodo v. Trans Union of Canada, Inc.*, and *Winder v. Marriott International, Inc.*, the Ontario Court of Appeal held that defendants who collect and store personal information of individuals in databases (Database Defendants) cannot be held liable under the tort of intrusion upon seclusion when cyber criminals illegally access or steal that information.

In recent years, claimants have attempted to expand the tort's application to cyber security and privacy breaches and sought to have class actions certified, seeking aggregate assessment of the moral or symbolic damages that are available for intrusion upon seclusion. This decision trilogy from the Court of Appeal is likely to slow this trend. However, as noted by the Court of Appeal, Database Defendants could remain liable in negligence where their failure to take adequate steps to protect information causes actual – as opposed to symbolic – damages.

Background

The Court of Appeal first codified the tort of intrusion upon seclusion in ***Jones v. Tsige*, 2012 ONCA 32**. This case involved an individual action brought against a bank employee who repeatedly accessed and examined the financial records of her ex-husband's new partner. Finding that the facts presented before him would otherwise not be actionable, Justice Sharpe concluded the situation "cried out for a remedy," adopting the tort of inclusion upon seclusion from the *American Restatement (Second) of Torts*.

In *Jones*, the Court set out the three elements of the tort:

1. Intentional or reckless conduct by the defendant;
2. An invasion, without lawful justification, into the plaintiff's private affairs or concerns; and
3. That a reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish.

Notably, proof of harm was not listed as an element of the tort – a welcome development for plaintiffs (and class counsel) who must ordinarily prove actual damages under other tort claims like negligence or breach of contract. However, in Jones the Ontario Court of Appeal noted the tort's recognition was not meant to "open the floodgates" of privacy litigation.[1] Justice Sharpe limited its application to deliberate and significant invasions of personal privacy that can be described as highly offensive in the eyes of a reasonable person.[2]

In the decade following ***Jones v. Tsige***, courts have had to clarify the scope of the tort. At the certification stage, many courts found that it was a stretch to say that a Database Defendant's failure to take adequate steps to protect personal information satisfied the "recklessness" requirement of the tort of intrusion upon seclusion. At the same time, courts were reluctant to refuse to certify such claims in light of the low legal threshold applicable to certification motions.

The three cases: Owsianik, Odobo and Marriott International

Owsianik, Odobo and Marriott International all involved privacy class action certification motions against Database Defendants for the tort of intrusion upon seclusion following large-scale data breaches by third-party cyber criminals.

In ***Owsianik***, the representative plaintiff pleaded that Equifax's "reckless" data management practices constituted an intrusion that would be highly offensive to a reasonable person.[3] A majority of the Court disagreed, holding the tort "has nothing to do with the database defendant."[4] Absent an actual intrusion, the majority said other categories of liability could adequately control the behaviour of the defendant – namely, the tort of negligence.[5] While the majority agreed that Jones might not be the final word on the tort of inclusion upon seclusion, they nonetheless declined to extend liability to non-intruders as doing so risked opening the floodgates the court in Jones intended be left firmly closed.[6] The decision included a strong dissent, with reasons that are considerably longer than those of the majority.

In ***Obodo***, the Court applied Owsianik as binding authority and rejected certification for intrusion upon seclusion on the basis that the tort has nothing to do with a Database Defendant.[7]

In ***Winder***, the claimants attempted to argue that Marriott's behaviour in obtaining the Class Members' personal information deceptively by false premises made it a "reckless" intruder.[8] While Justice Perell found that, at most, Marriott's behaviour might have rendered it a "constructive" intruder, he ultimately determined on policy grounds that the tort of inclusion upon seclusion should have a narrow scope of application. Referencing the Jones decision, Justice Perell concluded that extending the tort of intrusion upon seclusion to "constructive" intruders would open the floodgates of litigation and assign liability to conduct that other causes of action already adequately control, such as negligence or breach of contract.[9] Finding no gap in the law of privacy that would be filled by extending the tort to the Database Defendant who suffered the cyber attack, Justice Perell held the tort of intrusion upon seclusion is restricted to defendants who are "real" intruders.[10]

The trilogy

The Court of Appeal heard the three cases consecutively in June 2022, and released its decisions together in November 2022.

The Court of Appeal agreed with the decision of the majority in *Oswianik*. The Court of Appeal refused to extend liability under the tort of intrusion upon seclusion to the Database Defendants for failure to take steps to protect databases of personal information. In doing so, the Court declined to certify the class actions on the basis that the plaintiffs had not pled viable intrusion upon seclusion claims.

Although the *Jones v. Tsige* decision recognized that the defendant's conduct can be intentional or reckless to satisfy the first element of the tort, the trilogy clarifies that the prohibited state of mind, whether the intention or recklessness, must relate to the act of the invasion. The defendant must either intend to invade the plaintiffs' privacy, or the defendant must be reckless about whether his or her conduct will result in the defendant invading the plaintiffs' privacy. The Court of Appeal wrote that "[T]he 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."

In the Court's view, holding the Database Defendants liable for the intentional torts of unknown cyber criminals would have would created a new and potentially very broad liability for intentional torts and go beyond the incremental change to the common law that *Jones v. Tsige* sought to bring about.

Finally, the Court of Appeal rejected the argument that the plaintiffs were left without a remedy. The plaintiffs could pursue claims against Database Defendants whose negligent storage of information allows cyber criminals to access or steal that information if the plaintiffs could prove actual damages.

Takeaways

In this trilogy, the Court of Appeal refused to expand the scope of the tort of intrusion upon seclusion and confirmed Database Defendants cannot be held liable under this new tort when third party cyber criminals illegally access or steal personal information. It is not yet known if the plaintiffs will seek leave to appeal the decision to the Supreme Court of Canada.

The trilogy of cases is part of a broader trend of decisions in 2021 and 2022 that are favourable to defendants and that limit the scope of tort of intrusion upon seclusion. In narrowing the circumstances in which symbolic damages are available for breaches of privacy, the decision has also made the law of Ontario more consistent with that of Québec.[11]

Previously, plaintiffs had an advantage in the certification process and, as a result, in any settlement negotiations. That was because claims for intrusion upon seclusion could potentially be well suited for class-wide determination given that damages do not require proof of any actual pecuniary loss and can be awarded on a "symbolic" or "moral" basis. With this trilogy, plaintiffs may have lost that advantage.

In the future, plaintiffs who wish to claim against Database Defendants following cyber attacks will need to seek remedies under contract, negligence or statute, which generally require proof of economic harm or a "serious and prolonged mental injury." [12]

To the extent that existing common law remedies do not adequately encourage Database Defendants to take all reasonable steps to protect the private information under their control, the Court of Appeal invited Parliament and provincial legislatures to provide more effective remedies against Database Defendants who do not take proper steps to do so.

Given that Parliament recently completed its second reading of Bill C-27, a remedy for individuals who suffer damages related to the negligent storage of information may arrive sooner rather than later. This bill introduced the *Consumer Privacy Protection Act* (CPPA) and a private right of action for those affected by contraventions of the CPPA. As is the case under Canada's current privacy legislation, the CPPA requires organizations to protect personal information in a way proportionate to the sensitivity of the information. Via this new right of action, plaintiffs could claim damages for loss or injury resulting from a Database Defendant's act or omission. Given this potential legislative development, it remains to be seen how courts will treat cases like those in this trilogy, and to what degree it will hold Database Defendants liable.

1 *Jones* at para 72.

[2] Ibid.

[3] *Owsianik v Equifax Canada Co*, 2021 ONSC 4112 at para 5.

[4] *Ibid* at para 54.

[5] *Ibid* and at para 57.

[6] *Ibid* at para 54.

[7] 2021 ONSC 7297 at paras 114-115.

[8] 2022 ONSC 390 at para 9.

[9] *Ibid* at paras 13-16.

[10] *Ibid* at para 13.

[11] See *Lamoureux c. OCRCVM*, 2022 QCCA 685 (BLG Bulletin summarizing the decision), see also Anne Merminod, Karine Chênevert and Markus Kremer, "Two solitudes of privacy: privacy class actions in Quebec and the rest of Canada," in *Barreau du Québec*, *Service de la formation continue, Colloque national sur l'action collective Développements récents au Québec*, *au Canada et aux États-Unis*, vol 480, Montréal (QC), Éditions Yvon Blais, 2020, 67 ; Eloïse Gratton and Elisa Henry, Managing Privacy in a Connected World, LexisNexis, 2020;. Alexandra Hébert, Anne Merminod, *Maximus in Minimis*: Damages for Stress, Worry and Inconvenience in Class Actions, Annual Review of Civil Litigation, Thomson Reuters, 2020; Anne Merminod,

Qian Hui Sun, “Privacy Class Actions Across Canada: Does the Degree of Invasion Matter”, *Class Action Defense Quarterly,* Volume 14, Number 3, 2020

[12] See, for example, *Mustapha v. Culligan of Canada Ltd.*, 2008 SCC 27 at par. 9; *Saadati v. Moorhead*, 2017 SCC 28 at par. 37 and *Healey v. Lakeridge*, 2011 ONCA 55 at par. 43-44

By

Marc Vani, Shane Morganstein, Daniel Girlando, Eric S. Charleston, Hanna Rioseco

Expertise

Cybersecurity, Privacy & Data Protection, Class Action Defence

---

BLG | Canada’s Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary
Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa
World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver
1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal
1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG’s privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.