Ontario court dismisses cyber attack class action: Why ‘intrusion upon seclusion’ didn’t work

September 17, 2021

The Ontario Superior Court of Justice has dismissed another class action in which the plaintiff used ‘intrusion upon seclusion’ to claim damages for a cyber attack.

Justice Perell’s decision in *Del Giudice v Thompson* (*Thompson*) reinforces recent findings in similar cases where the intrusion upon seclusion tort was not upheld and organizations were not found vicariously liable for their employees. *Thompson* also shows how important carefully drafted contract and privacy policy terms can be to an organization’s cyber risk management.

The context

Organizations and their insurers have been carefully watching plaintiff counsel’s use of the intrusion upon seclusion tort, especially its application to data loss claims and resulting class actions, since the Court of Appeal for Ontario recognized the tort in 2012. While plaintiff counsel can rely on many causes of action when seeking a remedy for the consequences of data loss, intrusion upon seclusion was a novel way to attempt to obtain a sizeable award for moral damages when there was no compensable injury.

Almost immediately after the tort was recognized, plaintiff counsel began using it to claim that organizations intentionally or recklessly “intruded” upon the privacy of affected individuals when personal information was compromised by those outside the organization. In cases involving a malicious insider, plaintiff counsel began to allege that organizations were vicariously liable for the insider’s intentional intrusion.

Fast forward to early 2021, when the Divisional Court issued a significant favorable decision for Ontario organizations and insurers in *Owsianik v Equifax Canada Co (Owsianik)*. This decision held that custodians of personal data cannot be liable for intrusion upon seclusion when third parties steal or access that data. The Divisional Court’s majority decision was brief and focused on the lack of wrongful intent held by organizations who fall victim to attack. The decision did not address the issue of vicarious liability.

The Thompson case: Attack and data theft by a former insider

Thompson is about the theft of credit card application data by a former employee of a bank's cloud service provider. The former employee, who faces criminal charges in the United States, is alleged to have used the understanding she developed while working for the service provider to exploit system misconfigurations and perpetrate her attack.

The plaintiff sued the bank, the service provider and the former employee (among others) and sought certification. She pleaded 19 causes of action, including intrusion upon seclusion and vicarious liability. She alleged that the bank:

- collected application information for one purpose and retained and used it for other purposes;
- continued to retain the information despite increasing security risks (including risks arising from its outsourcing to a service provider in the United States);
- failed to warn of the increasing security risks; and
- lost the information in breach of various duties.

The Thompson decision on intrusion upon seclusion and vicarious liability

The Court struck the claim in *Thompson* without leave to amend because the claim did not set out a reasonable cause of action.

In disposing of the intrusion upon seclusion claim, the Court adopted and reinforced the key finding from *Owsianik*: "A failure to prevent an intrusion, even a reckless failure to prevent, is not an intrusion." It also stated that recklessness should take its meaning from established criminal and civil law jurisprudence – jurisprudence that defines recklessness as conceptually distinct from negligence and involving a state of mind exhibiting conscious indifference to risk.

The Court went further. While the *Owsianik* panel found that the organizational loss of data was "highly offensive," Justice Perell did not. He said:

> As pleaded against them, [the bank's and the service provider's] conduct amounts to making mistakes in safeguarding not particularly sensitive information that largely consists of information to identify the applicant for a credit card and to provide means to contact them. [The defendants'] conduct, which might be wrongful and expose them to some other cause of action, is not offensive in the requisite legal sense that would constitute the tort of intrusion on seclusion.

In dismissing the plaintiff's vicarious liability claim, it was of no consequence to the Court that the former employee was alleged to have used the knowledge she gained while working for the service provider to perpetrate her attack. It said it would be "absurd and unfair" to impose liability on a defendant for the actions of a former employee.

The Court quoted the bank's credit application terms, privacy policy, and cardholder and credit card agreement in detail and used the terms to invalidate numerous causes of action, including intrusion upon seclusion. It then struck the action without leave to amend based on a finding that the plaintiff's entire case theory, which focused on data misuse, "imploded" based on the contract terms.

Conclusion

Cyber attacks are inevitable, and even the best-defended organizations can expect to suffer cyber attacks and data loss. The degree to which organizations and insurers are exposed to third-party civil liability will be influenced heavily by whether the law provides a remedy on a strict basis and without proof of negligence and compensable loss. The law in Ontario has taken a noticeable turn with the *Owsianik* and *Thompson* decisions because they limit the degree of exposure. It remains to be seen how the Court of Appeal for Ontario will treat these types of cyber attack claims, however.

Thompson also illustrates the importance of contractual terms. Data misuse claims, in particular, will put the focus on notifications, privacy policies and other "contractual" documentation that define the scope of an organization's authorized use of data. *Thompson* shows how careful attention to these documents will help limit all kinds of privacy violation claims, including claims that follow a cyber attack.

Contact your BLG privacy lawyer or any member of BLG's Cybersecurity, Privacy & Data Protection team to ensure that your contract and privacy policy terms will strengthen your case in the event of a data or privacy dispute.

If you would like to learn more about the use of intrusion upon seclusion – or any other cause of action in a data, privacy or cyber attack case – reach out to any of the key contacts listed below.

By

Daniel J. Michaluk

Expertise

Cybersecurity Disputes, Class Actions, Cybersecurity, Privacy & Data Protection, Compliance with Privacy & Data Protection, Privacy & Security Breaches

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 725 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