Del Giudice: Weeding out meritless claims in privacy class actions

March 19, 2024

Introduction

Since the Court of Appeal for Ontario's decision in *Jones v. Tsige*, 2012 ONCA 32, there has been a wave of privacy class actions attempting to expand the scope and application of privacy torts. The Court in *Jones v. Tsige* recognized for the first time the tort of "intrusion upon seclusion." The Court envisioned an intentional tort that would be available only when a breach of privacy would be "highly offensive" to an ordinary person. In subsequent cases, plaintiffs attempted to expand the application of the cause of action to encompass claims against companies that had not deliberately invaded privacy, but had failed to protect confidential information in their possession. In a trilogy of cases decided in late 2022, the Ontario Court of Appeal clarified that defendants who collect and store personal information of individuals in databases cannot be held liable for intrusion upon seclusion when cybercriminals illegally access or steal that information.

That trilogy left plaintiffs in a number of pending privacy class actions in a difficult position, because their claims for intrusion upon seclusion were no longer viable. In some cases, plaintiffs amended their pleadings to assert different causes of actions in lieu of intrusion upon seclusion. An example is the recent decision in *Del Giudice v. Thompson*, 2024 ONCA 70, in which the Court of Appeal for Ontario held that the plaintiff had failed to plead a viable cause of action against a database defendant. In doing so, the Court confirmed that one of the main purposes of the cause of action criterion of the certification test under section 5(1)(a) of the *Class Proceedings Act*, 1992, S.O. 1992, c. 6, is to weed out claims that are doomed to fail, prior to the inevitable increase in legal costs at the discovery stage.

More generally, this decision provides an example of how defendants may attack a proposed class's pleadings to terminate the entire action at an early stage.

Background

Capital One collected data from credit card applicants and stored it on servers of Amazon Web Services (Amazon). When a former rogue employee of Amazon hacked

its servers, the data collected by Capital One became vulnerable to public exposure. The rogue employee then posted the data on a website where software developers share information.

Individuals impacted by the breach attempted to certify a class action against Capital One and Amazon for various torts related to data misappropriation and data misuse. The plaintiffs pleaded 19 causes of action (generally variations of data breach and data misuse claims), claiming damages of $240 billion, after amending their pleadings four times.

Motion judge decision

The motion judge concluded that the plaintiffs had advanced a case that was "doomed to fail." Their pleadings were struck without leave to amend, and their certification motion was dismissed. The motion judge directed that the certification motion would follow a bifurcated process. Phase 1 would address the preliminary question of whether the appellants had satisfied the cause of action criterion under s. 5(1)(a) of the *Class Proceedings Act*.

Justice Perell found that the statement of claim "egregiously" contravened the rules of pleading and failed to plead a viable cause of action. Justice Perell also found that the amendments made had transformed a straightforward data breach claim into a $240 billion action for data misappropriation and misuse.

Court of Appeal decision

The Court of Appeal dismissed the appeal and agreed with Justice Perell's analysis. The Court outlined various helpful points for defendants.

First, courts are entitled to consider contractual documents that contradict pleadings. A statement of claim is deemed to include documents to which the claim refers–and the contractual documents, which were filed with the Court in the motion record, were incorporated by reference into the pleading. In this case, the motion judge had instructed the respondents not to file any materials, but Capital One filed a document brief anyway. The appellants argued that these documents were evidence and thus, it was improper for the motion judge to take them into consideration. The Court of Appeal disagreed with the appellants and reiterated that a document incorporated by reference in a pleading is not evidence, and a judge considering such a document in assessing a pleading is not making findings of fact.

Second, the Court of Appeal confirmed the discretionary power that courts possess with respect to striking out claims without leave to amend. In this case, the motion judge found the statement of claim to have "egregiously" violated the rules of pleading. Given that the appellants were provided with numerous opportunities to amend their pleading, the Court of Appeal deferred to the motion judge's decision not to grant leave to amend. After four amendments, the motion judge found no purpose in allowing them another opportunity to reframe their theory of liability.

Third, courts will not unduly broaden the scope of the tort of intrusion upon seclusion by finding data custodians to be liable for third-party hacks. Aside from the initial hurdle of

establishing that Capital One obtained the personal information without the appellants' consent, the Court found that this conduct would not humiliate or offend a reasonable person. This is a high threshold, and any claim that does not meet this threshold will likely fail. Nothing in Capital One's conduct was considered to be an intrusion, as the data was aggregated and inputted into algorithms to be used for marketing purposes.

Finally, the Court of Appeal upheld the cost award of $1.2 million. The motion for leave to appeal costs was filed a month past the deadline, and the Court refused to grant an extension of time to allow them to file for leave to appeal the costs.

Takeaways

- At the pleadings stage, courts are entitled to consider contractual documents that are incorporated by reference into the pleading, and which directly contradict the opponent's pleadings.
- Plaintiffs will not be entitled to limitless pleading amendments. If given numerous opportunities to rectify a claim, courts may take a more rigorous approach in striking claims and denying leave to amend.
- A hack of a database by a third party does not constitute intrusion upon seclusion by the database operator, and courts will be unlikely to find businesses liable for third-party hacking under this tort. While plaintiffs may still be able to sue in negligence or for breach of contract, they will only be able to recover damages under those causes of action if they can prove pecuniary losses or a "serious and prolonged mental injury." This makes those causes of action far more complex to litigate as class actions than the tort of intrusion upon seclusion, for which symbolic damages are available.
- For a pleading to disclose a viable claim for intrusion upon seclusion, it must allege conduct that is highly offensive and humiliating to the reasonable person. The collection and use of personal information obtained by Capital One (even if done without consent) would not meet that test.

By

Nadine Tawdy

Expertise

Cybersecurity, Privacy & Data Protection, Disputes, 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 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