Blaney McMurtry LLP

PUBLICATION

From Bricks and Mortar to Data and Privacy

Date: August 16, 2017

Original Newsletter(s) this article was published in: Blaneys' Coffee House: August 2017

The litigation landscape is shifting in Canada, and a new breed of litigation claims is emerging – the data/privacy claim.

Data breaches, privacy breaches, and technology errors and omissions are some of the new types of loss being claimed by plaintiffs. One of the problems for insurers and potential defendants is figuring out from where these claims can arise. Two recent decisions of the Supreme Court of Canada illustrate this uncertainty.

Privacy Rights labelled as "Quasi-Constitutional"

In *Douez v. Facebook* (released on June 23, 2017), the Supreme Court of Canada allowed a class action against Facebook to proceed in British Columbia, despite a jurisdictional clause contained in Facebook's terms and conditions.

The proceeding arose out of Facebook's "Sponsored Stories" campaign in 2011. "Sponsored Stories" was a marketing initiative whereby Facebook would include the name and photograph of a Facebook user to advertise goods and services to other Facebook users. The plaintiff alleged that Facebook used her name and likeness without consent, and violated her privacy, in contravention of British Columbia's *Privacy Act*. Facebook challenged the lawsuit, on the basis of jurisdiction.

Facebook's terms and conditions contain a forum-selection clause, which mandates that all proceedings against Facebook be brought in California. In order to become a user of Facebook, one has to accept its terms and conditions. Facebook argued that bringing the class action in British Columbia ran afoul of its terms and conditions.

The Supreme Court rejected Facebook's argument, ruling in favour of the plaintiff. There were several factors that contributed to the Court's decision including the following: that privacy rights are "quasi-constitutional". While the right to privacy is not expressly stated in Canada's

Constitution, characterizing privacy rights as quasi-constitutional signaled the Court's belief that Canadian governments have an obligation to protect its citizens' privacy.

Furthermore, the Court took into account that Facebook's terms and conditions constitute a contract of adhesion - a take-it-or-leave-it contract, where a user or customer, who usually has much less bargaining power than the entity offering the contract, is forced to choose between accepting the terms and conditions or rejecting the goods or services. As the jurisdictional clause at issue was not negotiated, and the plaintiff had essentially no bargaining power, the Court ruled that the terms and conditions should not abrogate Canadian law.

The Supreme Court exercises Global Jurisdiction

In *Google Inc. v. Equustek Solutions Inc.* (released on June 28, 2017), the Supreme Court of Canada allowed a global interim injunction against Google despite the fact that Google was not a party to the action.

The action arose out of a dispute concerning intellectual property. The defendants (the plaintiffs' former distributors) allegedly unlawfully appropriated the plaintiffs' trade secrets. They also allegedly designed and sold counterfeit versions of the plaintiffs' products (i.e. networking devices). The plaintiffs requested that Google de-list or de-index the defendants from its search engine. Google refused to do so.

The plaintiffs sought an interim injunction (i.e. until there is a final judgment in the proceeding) against Google, requiring it to de-list the defendants. Injunctions are rarely granted by Canadian courts, as the bar for granting one is high. In this instance, however, given the global reach of Google's search engine, the Supreme Court imposed a worldwide interim injunction.

Implications for Future Claims

Data breaches and other similar technology-related claims often result in privacy claims being made by those alleged to be affected. Depending on the jurisdiction, Canadian claimants have certain statutory and common-law remedies for violations of their privacy. As the *Facebook* case demonstrates, the highest court in Canada has ruled that privacy rights are nearly on par with Canadian *Charter* (i.e. constitutional) rights such as the right to life, liberty and security of the person (section 7 of the *Charter of Rights and Freedoms*). Affording privacy rights this elevated status means that one is more likely to see results similar to the *Facebook* case, where a global technology company, which had arguably contracted out of litigation in Canada, was forced to litigate in Canada.

So, what if a company is relatively smaller than Facebook, but still has extra-territorial reach? What if that company never anticipated litigating anything in Canada and, therefore, never thought to protect itself with insurance that applies to Canadian claims? Alternatively, what if an insurer had issued a technology errors and omissions policy to Facebook with global coverage, anticipating that all claims against it would eventually end up in California? It is not hard to imagine an underwriter issuing a liability policy (whether it is a cyber liability, technology liability,

or some other type of liability policy) to an insured, on the assumption that any claim outside of California would be struck due to a forum-selection clause in its terms and conditions. After all, this type of clause is common to many websites and applications. What's more, a website's terms and conditions will almost always be a contract of adhesion - a product created by parties of unequal bargaining power. If privacy rights override this contractual language, then claims could arise from a vast number of jurisdictions.

The *Google* case demonstrates that Canadian courts are willing to grant orders against global technology companies that potentially reach beyond Canada's borders. Of course, that doesn't mean that courts in other jurisdictions will enforce those orders, but Canada is a respected legal jurisdiction, so one would expect many common-law jurisdictions to follow suit.

The *Google* case alone could realistically create a logistical nightmare for insurers. Even if Google has not made a claim for coverage (as there is arguably no claim against it), its insurers may be monitoring this matter for potential future claims. This would likely also require retaining legal counsel in the various jurisdictions in which the plaintiffs may seek enforcement of that injunction.

The reality of the global economy is that claims can come from anywhere in the world – or at least anywhere a company's website or application reaches.

Privacy and related laws are not uniform, which means that not only can claims come from anywhere and everywhere, but there will, likely, be different rulings depending on the jurisdiction.

Insurers must therefore take this into account when assessing the risk of doing business in any given jurisdiction. Moreover, insurers who issue liability policies to those companies must ensure that they have assessed those risks, and have considered the full extent of the risks of liability claims impacting the policies they issue.