Blaney McMurtry LLP

PUBLICATION

# Invasion of Privacy Claims Expanding -- Business Should Take Note

Date: March 22, 2016
Co-Authors: John Polyzogopoulos, Stephen Gaudreau

Original Newsletter(s) this article was published in: Commercial Litigation Update: March 2016

*Republished in the June 2016 edition of the LexisNexis Canadian Privacy Law Review:*

Download PDF

In the judiciary's constant effort to keep pace with new technology and privacy concerns, a recent Ontario Superior Court decision in *Jane Doe 464533 v. N.D* has provided citizens with more privacy protection. In *Jane Doe*, Justice Stinson expanded on the recently created tort claim of "invasion of privacy" or "intrusion upon seclusion" by creating a new tort of "public disclosure of private facts".

The facts in *Jane Doe* were straightforward and uncontested, as the defendant failed to defend the action. In 2011, the plaintiff and the defendant, both 18 years old at the time, dated in a small Ontario city. The couple broke up, and by the fall of 2011, the plaintiff had moved away to university.

Despite the break-up, the parties kept in touch and continued to text and call each other. The defendant began to pressure the plaintiff to send him a sexually explicit video of herself. He promised to keep the video private, but when she finally relented and sent him a video, he immediately uploaded it to a pornographic website. The video remained on the website for approximately three weeks before it was removed. There was no way of knowing how many times it was viewed, shared, downloaded, or copied. The plaintiff found out that some of her friends had seen the video, as well as others from her hometown. The news devastated her. She fell into a depression. The effects of the video haunted her years later. The defendant showed no remorse.

The victim of this dishonourable act sued the defendant for the recognized torts of breach of confidence and intentional infliction of mental distress. Justice Stinson found that the plaintiff

had proven those claims. Notwithstanding that he found for the plaintiff under established tort claims, the judge also found that the defendant was liable to the plaintiff for the new tort of "public disclosure of private facts".

In his decision, Justice Stinson said that the common law has a role to respond to the problems posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form. He relied heavily on *Jones v. Tsige*, a 2012 decision that created the tort of "breach of privacy" or "intrusion upon seclusion". *Jones* involved a bank employee who repeatedly accessed and examined the confidential banking records of her husband's ex-wife without permission. The employee was found liable under the newly-created tort. In *Jones*, there was no public disclosure of the banking information.

In *Jane Doe*, the wrong related to the public disclosure of private information rather than the unauthorized access to private information. *Jones* therefore did not go far enough to provide protection to the plaintiff in *Jane Doe*. Justice Stinson expanded the tort of breach of privacy as first set out in *Jones* by holding that one who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized or the act of the publication:

(a) would be highly offensive to a reasonable person; and

(b) is not of legitimate concern to the public.

The Court found the defendant liable for the tort of public disclosure of private facts and awarded judgment to the plaintiff in the amount of over $140,000.

It should be noted that at the time the offending video was posted, the defendant was not in contravention of any criminal laws (although the Criminal Code has since been amended to prohibit such unauthorized postings). Despite the fact that no crime was committed, that did not absolve the defendant of civil liability.

*Jane Doe* serves as a reminder that once personal information has been posted in cyberspace, there is really no turning back. When determining liability, Justice Stinson did not place any emphasis on the fact that there was no way of knowing the number of times the video had been viewed. He determined that a plaintiff bringing a breach of privacy claim does not have to prove that the information was actually downloaded, shared, viewed, or copied in order to succeed. It is therefore not a defence to plead that the information was removed immediately, or that there is no evidence that anybody viewed the posting.

The next stage in the evolution of privacy law in Ontario after *Jane Doe* may well be liability for the unintentional facilitation of privacy breaches. Business should therefore be paying attention to these developments and taking steps to mitigate against the risks of potentially massive liability. Prudent business practice dictates that internal policies and procedures be implemented in relation to the collection, storage, safeguarding and use of private information. A failure to

protect confidential information of customers or employees could result in catastrophic financial losses.

The very recent and highly publicized *Erin Andrews* jury verdict in the U.S. provides an example of where the law in Ontario is likely heading. In the *Andrews* case, a Tennessee jury awarded the ESPN sportscaster a $55 million judgment as a result of the posting on the internet by a stalker of surreptitiously recorded videos of Ms. Andrews in the nude. On multiple occasions, Andrews' stalker, Michael Barrett, rented hotel rooms next to Andrews' rooms and videotaped her through the peep holes of the doors between their rooms. Barrett uploaded the videos to the internet. The videos were viewed by millions of people and blurred photos of Andrews were plastered on the front pages of tabloid newspapers nationwide.

Andrews sued Barrett for negligence, negligent infliction of emotional distress, invasion of privacy and public disclosure of private facts. More interestingly and unlike in *Jane Doe*, where there was no commercial actor to sue, Andrews also sued the hotels for negligence, negligent infliction of emotional distress, and invasion of privacy. Not surprisingly, the Tennessee jury found Barrett liable. More interestingly, however, was that the jury also found one of the hotels liable to Andrews. The jury apportioned 51% liability to Barrett, and 49% liability to the hotel, meaning the hotel is on the hook for almost $27 million.

Because this was a jury decision where no reasons were delivered, we will never quite know which legal claims were relied upon by the jury to find liability. However, a review of the claim filed by*Andrews* reveals that the allegations against the hotel were as follows: the hotel revealed Andrews' hotel room number to Barrett, it facilitated Barrett's conduct by placing him in a room next to Andrews, and it failed to discover that Barrett had altered the peep hole in the door between Andrews' and Barrett's rooms. In the result, the hotel's failure to safeguard its guest's privacy was enough for a jury to award massive damages against the hotel. This, despite the fact that the hotel's acts and omissions were no doubt unintentional and the result of those acts and omissions was not easily foreseeable.

It remains to be seen whether claims similar to *Andrews* will be successful in Ontario against unwitting businesses who unintentionally facilitate privacy breaches and, if so, whether damage awards will approach anything close to the award in *Andrews*. We may not have to wait that long to find out. The recent and also notorious *Ashley Madison* privacy breach case is already the subject of a class action in Ontario. *Ashley Madison* is an online dating service that caters to married people interested in engaging in extra-marital affairs. A group of morally outraged computer hackers broke into *Ashley Madison*'s electronic databases and threatened to publish the identities and other personal information of *Ashley Madison* clients if the site did not shut down. When *Ashley Madison* refused to accede to the hackers' demands, they published the client information. Many of the exposed clients were Canadian. Even though *Ashley Madison* did not publish its clients' information and no doubt had computer data security systems in place, it is nonetheless at serious risk of being found liable for the data breach and publication of client information. *Jones*, *Jane Doe* and now *Andrews* provide several arrows in the quiver of plaintiffs' class counsel.

In conclusion, the pace of technological change has facilitated the exponential growth in the rate of collection, storage and dissemination of sensitive and confidential personal information. The law, particularly statutory laws passed by Parliament and provincial legislatures, has been slow to keep pace with the growing need to protect individual privacy rights. The courts have done their best to fill the legislative void. *Jane Doe* is the latest Ontario example of that. Businesses need to be vigilant and to ensure that they have adequate measures in place to protect the privacy of their customers and employees in order to mitigate against the risk of potentially massive liability in the event of a security breach.