fogler rubinoff

Privacy Law Bulletin

January 11, 2017

PUTTING A DOLLAR FIGURE ON BREACH OF PRIVACY IN CANADA

By Ravi Shukla

Ravi Shukla
Partner

t: 416.864.7612
rshukla@foglers.com

Damages in Canadian Privacy Breach Cases

The purpose of the Canadian federal *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") is to establish rules that recognize both the right of privacy of individuals with respect to their personal information ("**PI**"), as well as the needs of organizations engaged in commercial activities to collect, use and/or disclose PI for purposes that a reasonable person would consider appropriate in the circumstances (substantially similar provincial equivalents have been enacted in Alberta, British Columbia and Quebec - Manitoba has also passed legislation, which is expected to be declared substantially similar to PIPEDA once it has been proclaimed in force). Section 16 of PIPEDA authorizes courts to award damages, including damages for humiliation that a complainant has suffered, arising from a breach of the legislation. Over the past few years there has been an evolution towards courts awarding greater damages amounts. In the notable case of *Chitrakar v. Bell TV*, involving a non-consensual credit check the Federal Court awarded the applicant $10,000 in damages, $10,000 in exemplary damages, plus $1,000 in costs. The court acknowledged the difficulty of assessing damages absent evidence of direct loss, but in a marked departure went on to say "there is no reason to require that the violation be egregious before damages will be awarded". Nevertheless, given the PIPEDA requirement that a complaint assessment by the Privacy Commissioner be completed prior to an application being filed with the Federal Court, it has been difficult to envision how the statutory damages regime could be leveraged in support of a class action lawsuit.

Changes to the Risk Exposure Landscape

That risk exposure landscape began to shift dramatically in 2012 when the Ontario Court of Appeal recognized a new common law cause of action for breach of privacy in a non-class action setting. The tort of intrusion upon seclusion was recognized as co-existing with PIPEDA in the case of *Jones v. Tsige*, the facts of which involved improperly accessed bank-held PI by a co-worker, but notably did not include evidence of economic harm suffered by the plaintiff.

The tort clearly applies in Ontario and may also apply in Alberta, Nova Scotia, New Brunswick and Prince Edward Island (a provincial statute-based breach of privacy claim can potentially issue in British Columbia, Saskatchewan, Manitoba and Newfoundland - a similar provision is also included in the Quebec Civil Code). Liability for tortious intrusion upon seclusion has fallen in the general range of $10,000 to $20,000, depending on the egregiousness of the facts in each particular case (a requirement of the new the privacy specific tort is that the defendant's conduct must have been intentional or at least reckless). In addition, aggravated and punitive damages may be available in exceptional cases.

Ontario's First Certified Privacy Tort Class Action

In June of 2014 the first Ontario class action was certified based on the tort of intrusion on seclusion in the case of *Evans v. The Bank of Nova Scotia* (there have subsequently been other intrusion on seclusion based class actions certified both in Ontario and elsewhere in Canada).

Richard Wilson, an employee of The Bank of Nova Scotia, admitted to providing bank account information to his girlfriend, who then sold that information to third parties. 643 of the Bank's customers were notified of the breach and 165 of those individuals (some of whom did not initially report their case to the bank) eventually became victims of identity theft and fraud.

The Ontario court certified the class action against the bank for the privacy breach and for negligence (which latter general tort requires proof of damages suffered), despite the bank's claim that they should not be held vicariously liable for its employee's deliberate theft of client PI (consistent with the approach taken in Jones the bank did not take the position that PIPEDA provided a comprehensive code precluding tort claims). The bank had offered a complimentary subscription to a credit monitoring and identity theft protection service. The Bank also compensated the then-identified 138 victims of identity fraud for the pecuniary losses that they suffered. The Court permitted the claims against the bank to proceed noting that:

"In this case, the Bank created the opportunity for Wilson to abuse his power by allowing him to have unsupervised access to customers' private information without installing any monitoring system…Also, Wilson's wrongful acts…were related to his necessary intimacy with the customers' personal and financial information. Wilson was given complete power in relation to the victims' (customers) confidential information, because of his unsupervised access to their confidential information. Bank customers are entirely vulnerable to an employee releasing their confidential information."

The *Evans* case was settled in 2016 when the bank agreed to pay each of the identity theft victims an additional amount of approximately $7,000 (giving rise to a total payout of approximately $1.1M plus actual losses suffered) in return for a full release. Class members who were merely notified by the bank that their information had been wrongfully accessed were not compensated. The bank did not admit any wrongdoing or liability on its part. Nevertheless, this settlement provides additional support for the argument that organizations must seriously consider appropriately monitoring the manner in which their representatives access and use PI. The $7,000 per individual additional payment clearly demonstrates that when the privacy tort damages range is multiplied by the number of individual plaintiffs in a class action, the overall potential monetary exposure may be very significant.

Key take-Aways

The settlement in *Evans* involving a deep-pocketed and well-advised defendant should be seen as important additional evidence that the activist stance taken by Canadian courts in response to innovative lawsuits launched by individuals seeking redress for alleged breaches of privacy rights must be accommodated and that policies, procedures and technologies aimed at minimizing the risk of privacy breaches are to be pro-actively implemented by organizations operating in this fast changing enhanced risk exposure environment. In the other Ontario based privacy class action which settled in 2016 involving Home Depot, the judge found that Home Depot was in the process of building a strong case that it had done nothing wrong and essentially characterized the case against it as weak. As a result of having been found to have taken the appropriate risk reduction steps both before the breach and in its immediate aftermath, Home Depot emerged relatively unscathed from its litigation and that outcome further reinforces the key message to be gleaned from the outcome in *Evans*.