fogler rubinoff

PRIVACY LAW BULLETIN

Are We There Yet?

Ravi Shukla, LL.B.

Ravi Shukla

Partner

t: 416.864.7626
rshukla@foglers.com

Fogler, Rubinoff LLP
Lawyers
77 King Street West
Suite 3000, PO Box 95
TD Centre North Tower
Toronto, ON M5K 1G8
t: 416.864.9700
f: 416.941.8852
foglers.com

Another week, another international news story about a significant personal information security breach. Or so it seems. Last month John Legere of US-based T-Mobile and Dido Harding of UK-based TalkTalk added their names to the already lengthy list of company heads who have announced that the confidentiality that once attached to stored personal information had been compromised. This on the heels of other similar prominent disclosures regarding Ashley Madison, JP Morgan, Sony, Home Depot and, of course, the aptly named Target. As the list of the hacked grows ever longer, segments of the public appear to have concluded that organizations (including government agencies) are too complacent to implement the additional policies, procedures and technologies required to enhance the protections afforded to personal information collected from customers and employees. On this bleak view there is a stark choice, to either continue to provide personal information to employers and businesses with the knowledge that it is likely a question of when, not if, that information will become more broadly accessible, or to opt out of participating in the channels most likely to give rise to such requests for disclosure of personal information, despite the increased efficiencies and other benefits that generally arise from such participation.

There are, however, good reasons to believe that here in Canada we have reached the point where many senior decision makers have been convinced of the need to make investments in order to shore up the defences to intrusion being put forward by their organizations, rather than continue on in the hope that criminals will fortuitously select a neighboring enterprise. It has been clear for some time that the largest Canadian financial services providers have been actively implementing "best practices" based responses to information security threats, which could explain the relatively good performance to date of that sector in the information security breach area. Even the recently departed federal Conservative government, which was never closely associated with a meaningful concern for civilian privacy interests (as a largely political exercise it promulgated limited and exception riddled anti-spam legislation), had a late-term interest in being seen as championing a strengthening of the federal privacy legislation "PIPEDA" to, among other things, include mandatory breach notification requirements along with meaningful fines for non-compliance (up to $100,000 per offence). Likewise, insurers are reporting increased demand for cybersecurity policies despite the relatively high deductibles involved, risk transference being an aspect of overall risk management programs.

If we have indeed finally reached a tipping point, much of the credit will have to be given to an activist Canadian judiciary for "upping the ante" on privacy rights protection issues. Several Canadian class actions involving allegations of breach of privacy rights have been certified and, in a notable 2012 decision in the case of *Jones v. Tsige*[1], the Ontario Court of Appeal created a new common law cause of action for breach of privacy in Ontario. The tort of intrusion upon seclusion may also apply in Alberta, Nova Scotia, New Brunswick and Prince Edward Island. Liability in the context of the tort of 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. When this damages range is multiplied by the number of individual plaintiffs in a class action, the overall potential monetary exposure may of course be very significant.

A similar dynamic is taking place under PIPEDA. Via section 16 of PIPEDA, courts may award damages, including damages for humiliation that the complainant has suffered, arising from a breach of the legislation. In the past 3 years there has been an evolution towards courts awarding increasing damages amounts under s.16. In the recent 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".

So while there continue to be many discouraging aspects to the current situation regarding the protection of personal information globally – there is a notable need for higher encryption "cloud" services with desirable usability features – here in Canada a degree of cautious optimism is now justifiable.

---

[1] 2012 ONCA 32 (CanLII)