ASHLEY MADISON – A NEW ERA IN PRIVACY CLASS ACTIONS FOR CANADA?

Posted on October 2, 2015

Categories: Insights, Publications

In recent years, the phrase "data breach" has firmly established its place in the public vernacular, and it is not difficult to understand why this has occurred. In the past 3 to 5 years, the seemingly constant barrage of high profile "hacking" incidents have served as a reminder that it is not only web-centric companies that can suffer the embarrassment of a privacy or data security breach. It seems that no organization is safe from these attacks. Online retailers, brick and mortar shops, government bodies, private banks, health care providers, airlines, social networks, movie studios, and now dating sites, have all been targeted. The sheer variety of companies who have been recent victims of a data breach demonstrates that, as the end of 2015 nears, data security should be top of mind for every business that has sensitive or private electronic data that they want to protect.

The latest high profile attack targeted the dating website Ashley Madison. Ashley Madison's slogan is "*Life is short. Have an affair*" and as of writing they continue to promote themselves as "*the world's leading married dating service for **discreet** encounters*". [emphasis in original]

In mid July, 2015, a group identifying themselves as the "Impact Team" made an open allegation that they had taken over Ashley Madison's systems, and threatened to release customer records, profiles, and other compromised data within their control, if Ashley Madison did not shut down immediately and permanently. On August 18, 2015, the group followed through on this ultimatum, publically releasing information relating to what has been variously estimated at between 30 and 40 million Ashley Madison user profiles. In addition to containing names and other personal information, the leaked data is reported to include seven years worth of payment transaction details. Furthermore, the leaked data contained personal information of users who had previously paid Ashley Madison to delete their personal information.

While the reputational impact of this data breach may, itself, prove to be a significant challenge for Ashley Madison, the breach has also triggered a number of class proceedings both north and south of the border. This may be old news for the United States, since they have seen a myriad of class action lawsuits following cyber attacks in recent years. However, this is a relatively novel case in Canada, where prior privacy-related class actions have centered around cases of lost portable media devices containing sensitive personal information

(and other employee errors) as well as employee "snooping" cases. In these earlier cases, the argument could be made that the company should be vicariously liable for the actions and omissions of their employees. However, the concept that an organization should also potentially be held liable for the consequences of being victimized by cyber criminals is relatively new to Canada.

In August class action proceedings were commenced in Ontario, alleging that Ashley Madison's parent companies Avid Dating and Avid Life are liable to the representative plaintiff and class members for breach of contract, breach of Ontario's *Consumer Protection Act*, negligence, intrusion upon seclusion, breach of privacy, and publicity given to private life, and it seeks general damages in the amount of $750 million dollars. The representative plaintiff claims to be a disabled retiree who lost his wife of 30 years to breast cancer, and joined Ashley Madison to seek companionship.

Class proceedings against Avid Dating and/or Avid Life have also been commenced in the United States, in (as of writing) at least 8 states. In addition to the causes of action contemplated in the Ontario proceedings, the US pleadings also variously allege intentional infliction of emotional distress, bailment, conversion, unjust enrichment, fraud, and violations of various state and federal communications, trade practice, merchandising, and identity theft statutes.

Central to the array of ongoing litigation are allegations that Ashley Madison failed to exercise reasonable care or take reasonable or appropriate steps to safeguard member data before or after breach, failed to disclose the breach in a timely and transparent manner and made false representations, or breached contract, with respect to their paid data deletion service. While the various proceedings are still in very early stages, it will be useful to monitor this litigation to see how the courts deal with a number of unsettled legal issues, such as:

- Is there a duty of care to customers with respect to protecting their personal information?
- If a duty of care exists, what is the standard of care? For example, what constitutes reasonable or industry standard safeguards in the era of seemingly constant high profile breaches?
- Will Canadian courts impose liability on companies that have been victims of cyber attacks, for the consequences of such attacks?
- What legal obligations exist with respect to breach response and/or notification, especially under common law if statutory gaps exist?
- Does the tort of intrusion upon seclusion apply to data breaches caused by cyber attacks? If not, will the courts be prepared to create a new tort to address such situations? Or will these types of claims be decided under existing causes of action, such as negligence and breach of contract?
- Do companies have any obligation to try and avoid disclosure of personal information or contain a breach by reasoning with or conceding to the demands of breach perpetrators?

While few would characterize the Ashley Madison site as vital infrastructure, or perhaps even view the significance of their operations as comparable to companies like Home Depot, eBay, Target, Sony or many of the other recent high profile breach targets, it is difficult to deny that the impact of the breach is significant. Notwithstanding the potentially questionable social utility of Ashley Madison, the reality is that data pertaining to one's sexual infidelity and proclivities (whether actual or merely ambitious) is highly sensitive information, and the disclosure of such information certainly has the potential to create severe personal (and potentially financial) consequences for many people.

From a business impact perspective, it will be valuable to observe the progression of Ashley Madison's post-breach operations, both in terms of their navigation through numerous legal challenges, and in terms of their ability to attract and retain users in order to operate as a going concern. This is particularly true in the present case, because Ashley Madison's service model is fundamentally premised and reliant on preventing exactly the type of breach that ultimately occurred. In other words, it will be interesting to see if a website that explicitly offers secrecy to users can survive after users are publicly exposed.

While it may be tempting to discount the significance of the Ashley Madison breach based upon the nature of the site itself, doing so overlooks the broader issues of online security and consumer confidence in web-based transactions. Ashley Madison's attempt to weather the fallout of this summer's data breach, successful or not, is likely to be instructive for all businesses, even those with more traditional service offerings.

by Lyndsay A. Wasser and Rohan Hill

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.