July 2013

mcmillan class action bulletin

authorization of a class action for privacy violations granted in Quebec

As the amount of personal information available to and used by businesses continues to increase exponentially, protection of individual privacy is a rapidly spreading concern thanks in part to intensified media attention on security breaches and the ways in which personal information may be misused. A consequence has been a rise in privacy law class actions in North America. This trend has recently appeared in Quebec, where robust privacy laws and the possibility of punitive damages increase the risk of costly and time consuming litigation.

Different types of security violations can propel a privacy class action. Some are initiated after a security breach involving personal information, such the one recently filed in Quebec following the Investment Industry Regulatory Organization's (IIROC) breach in April 2013, which was widely reported by the provincial and national media. In this instance, an employee lost an unencrypted laptop containing the financial information of over 52 000 brokerage firm clients.

Other privacy class actions are challenging the models that digital service providers rely on to store, transmit or use personal information. An accusation that has most enraged consumers is that programs may not only store their personal information, they may also transmit the information to third-party businesses for targeted advertising purposes; all without prior consent, or even knowledge that it is being collected.

The most recent decision that is likely a precursor to litigation regarding new technologies and privacy law was an authorization for a class action against Apple and Apple Canada by the Quebec Superior Court on June 27th. The suit alleges that Apple has violated users' right to privacy by transmitting or allowing Apps to transmit private data to advertisers. The lawsuit mirrors those filed in the United States; all flow from a Wall Street Journal investigation. The court will consider whether Apple caused or facilitated the creation of personally identifiable profiles of Class Members, and whether they failed to disclose the tracking and compiling of information by the App.

what are the damages?

A major challenge for members in privacy class actions is proving their damages. The reality is that despite a privacy breach, courts may, in certain situations, find that there is no damage whatsoever and that monetary relief is not an appropriate remedy. We note that a number of class action privacy lawsuits in the U.S. have been unsuccessful due to class members' failure to prove "actual harm".[1]

Establishing a tangible prejudice is also important to Canadian courts in privacy class actions. In the Quebec case of *LaRose c. Banque Nationale du Canada*,[2] the Superior Court authorized a class action in connection with the theft of a laptop which contained the personal information of a group of mortgagees of National Bank. The judgment stated that under Quebec law, *fear* of identity theft or fraud did not constitute a harm or injury in and of itself and thus

---

[1] See, for example, the following judgments where the court found that plaintiff(s) failed to establish cognizable injury and damage: *Ruiz v Gap, Inc*., 2010 WL 2170993 (C. A. 9 Cal.)); *Allison v Aetna Inc*., No. 09-2560 (E.D. Penn. 2010); *People's United Bank and Bank of New York Mellon Inc*., 2009 U.S. Dist. LEXIS 78065 (D.Conn. 2009); *Randolph v ING Life Insurance and Annuity Company*, 973 A. 2d 702 at 710 (D.C. Court of Appeals 2009); *Cherny v Emigrant Bank*, 604 F. Supp. 2d 605 (S.D.N.Y. 2009); *Ryan v Delhaize America, Inc. d/b/a Sweetbay, and Hannaford Bros. Co*. (D. Maine 2008); *Bell v Acxiom Corporation*, 4:06-cv-00485-WRW (E.D. Ark. 2006).

[2] [2010] J.Q. no 11510, 2010 QCCS 5385.

could not provide the foundation for a class action. Only because there was evidence of actual identity theft was authorization granted.

In the Apple lawsuit, in addition to punitive damages, the class claims material damage for prejudice caused by the device's resources being consumed by the third parties, misrepresentation of the value of the device, and an injunction requiring Apple to cease authorizing Apps to use personal information. On the privacy front, a more subjective type of harm is claimed, that Apple allowed third parties to collect and disseminate the personally identifiable information of its users, maintained a log of their movements, and allowed third parties to access this information. That this claim is filed in Quebec is interesting because the province's privacy framework is tougher than in the rest of Canada.

privacy legal framework in Quebec

Quebec has one of the most stringent legal frameworks for privacy in Canada, not to mention a Consumer Protection Act that shields consumers more than most jurisdictions do. Until now, the amounts granted by courts for privacy breaches in individual claims have usually been low. However, in the context of class action privacy suits, the amount of damages usually awarded for a breach for a single individual might raise dramatically given the high amount of members.

For instance, the Apple class action authorizes two groups: (i) all Quebec residents who have purchased or otherwise acquired an iPhone or iPad and who have downloaded free Apps from the App Store onto their devices since December 1, 2008 through to the present; and (ii) all residents in Quebec who have purchased or otherwise acquired an iPhone and turned Location Services off on their iPhones prior to April 27, 2011 and have unwittingly, and without notice or consent transmitted data to Apple's servers. Privacy class actions of this nature have potentially thousands or even hundreds of thousands of class members, meaning the sum

total in damages, if the claims eventually succeed, may be significant.

Claimants in Quebec privacy class actions can invoke sections 35 or 36 of the Civil Code of Quebec as the basis for their invasion of privacy claims. The Quebec Charter of Human Rights and Freedoms[3] can also be used to obtain punitive damages as a result of privacy violations, where there has been an "unlawful and intentional interference".[4] As the objective of punitive damages is prevention, they are determined in light of all the circumstances, particularly the gravity of the fault, the debtor's patrimonial situation, and the extent of the reparation for which he is already liable to the creditor.[5] In a handful of judgments, Quebec courts have awarded punitive damages for privacy violations, specifically upon illegal transfers of personal information taking place.[6]

While it remains to be seen what kind of damages will be granted, businesses should realize that these types of privacy class actions often involve a high number of members and therefore, the amount in damages at stake may be quite high. Their increasing popularity and the court's willingness to authorize them might encourage businesses to invest in prevention measures and implement proper privacy policies that encourage best practices. Preventive measures may involve more comprehensive analyses of the privacy issues of a product before it is marketed at large, and increasing transparency

---

[3] section 49, RSQ, c C-12;

[4] *Quebec (Public Curator) v Syndicat national des employés de l'hôpital St-Ferdinand*, [1996] 3 SCR 211, par. 121. The Supreme Court decisions states that "there will be unlawful and intentional interference within the meaning of the second paragraph of s. 49 of the Charter when the person who commits the unlawful interference has a state of mind that implies a desire or intent to cause the consequences of his or her wrongful conduct, or when that person acts with full knowledge of the immediate and natural or at least extremely probable consequences that his or her conduct will cause".

[5] s. 1621, Civil Code of Quebec.

[6] See for example *Roy v Société sylvicole d'Arthabaska-Drummond*, J.E. 2005-279 (C.Q.); *St-Amant v Meubles Morigeau ltée*, J.E. 2006-1079 (S.C.); *Boulerice v Acrofax inc.*, [2001] R.L. 621 (C.Q.); *Stacey v Sauvé Plymouth Chrysler* (1991) inc., J.E. 2002-1147 (C.Q.).

by ensuring that customers are properly informed and consent to the collection and disclosure of their information through their technology use. More training of employees to better detect and avoid potential security breaches may also be in order. Surely such prudence is preferable to cleaning up the reputational fallout after a widely reported security breach or being a defendant in a privacy class action, with all the costs that it implies.

For more information on this topic, please contact:

Montréal Éloïse Gratton 514.987.5093 eloise.gratton@mcmillan.ca

a cautionary note