Privacy Class Action Certified against Employer

By: Jeremy Schwartz and Jessica Young

Heightened vigilance is the order of the day. In the wake of a recent decision of the Ontario Superior Court, employers who fail to properly watchdog confidential information accessible to employees may face significant vicarious liability for those employees' unlawful access and use.

The tort of intrusion upon seclusion was recognized by the Ontario Court of Appeal just over two years ago in **Jones v Tsige**. This was a significant development in Ontario privacy law. The case involved two employees of the Bank of Montreal. The defendant, Tsige, had accessed the plaintiff, Jones', personal bank records at least 174 times over a four year period. Jones chose not to sue her (current) employer, Bank of Montreal. But the employer community gleaned they could be exposed to vicarious liability for the actions of their employees for such privacy breaches. Read our update on that decision.

This issue has surfaced most recently in **Evans v Bank of Nova Scotia**, a class action certification decision in which the claim alleges the Bank of Nova Scotia is vicariously liable for privacy breaches committed by one of one of its employees.

Evans v Bank of Nova Scotia

The Bank employed Mr. Richard Wilson as a Mortgage Administration Officer, and in that role he had access to highly confidential client information. Mr. Wilson admitted to taking private and confidential information related to Bank clients. He gave the information to his girlfriend who provided it to third parties for fraudulent and improper purposes.

The Bank notified all clients whose accounts were accessed by Mr. Wilson that there may have been unauthorized access to their private information. In total, the Bank identified 643 clients whose files had been accessed by Mr. Wilson from July 1, 2011 until his computer access was terminated by the Bank on May 18, 2012. The Bank compensated all clients who had been victims of identity theft or fraud and who had suffered pecuniary losses.

Despite the Bank's good faith efforts to rectify the situation, Evans initiated a class action lawsuit, alleging the Bank was vicariously liable for the tort of inclusion upon seclusion.

Intrusion upon seclusion requires plaintiffs to prove three elements: (1) that the defendant's conduct was intentional (including reckless), (2) that the defendant invaded the plaintiff's private affairs or concerns without lawful justification, and (3) that a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish.

Evans has not alleged on behalf of the class that the Bank intentionally invaded their privacy. The Bank had no knowledge of Mr. Wilson's rogue actions. Instead the claim asserts that the

Bank is vicariously liable for the tort of intrusion upon seclusion committed by Mr. Wilson. The claim relies on the Bank's acknowledgement that it lacked of oversight of its employees with respect to improper access to personal and financial customer information.

The court emphasized that the Bank created the opportunity for Mr. Wilson by providing him with unsupervised access to client confidential information, and neglecting to put any sort of monitoring system in place. The court noted that Bank clients are entirely vulnerable to an employee releasing their confidential information and that there is a significant connection between the risk created by the employer in this situation and the wrongful employee conduct.

The court found that it was not plain and obvious (which is the low standard applicable for determining whether to certify a class action) that in these circumstances the Bank would not be held vicariously liable for the serious wrongful conduct of its employee. Since this was a class certification application, the court did not address the merits of the allegations in the claim, including whether the Bank is indeed vicariously liable. That will be determined later at trial.

What employers should know

Although this decision was on whether to certify the class action to proceed, and not a decision on the merits of the case, it signals to employers the importance of having mechanisms in place to safeguard confidential information. This applies to both client confidential information and employee confidential information.

Employers should prepare and implement workplace policies and rules outlining the expectations on employees related to confidential information and the use of the employer's computer and data systems. Confidentiality policies should expressly prohibit the unauthorized viewing, use and disclosure of confidential information. Access to confidential information should be limited, and employees who do have such access should be supervised.

Employers should also expressly reserve the right to monitor all such access, including through surveillance and other unannounced investigative techniques. Like posting a sign that warns people of speed cameras up ahead, doing so has a deterrent impact and reduces the likelihood that acting on evidence gathered from such surveillance and monitoring would be rejected in subsequent legal proceedings against such rogue employees.

For more information, please contact:
Jeremy Schwartz at jschwartz@stringerllp.com or 416-862-7011 or
Jessica Young at jyoung@stringerllp.com or 416-862-1687

UPDATE is an electronic publication of Stringer LLP
110 Yonge Street, Suite 1100, Toronto, Ontario M5C 1T4
T: 416-862-1616 Toll Free: 1-866-821-7306
E: info@stringerllp.com I: www.stringerllp.com