Blaney McMurtry
BARRISTERS & SOLICITORS LLP

EXPECT THE BEST

A Higher Price Tag on Privacy? An Ontario Court Certifies a Class Action for Breach of Privacy

by Christopher McClelland
Originally published in *Employment Update* (July 2014)

Christopher McClelland is a Partner at Blaney McMurtry and a member of the Employment and Labour Group and the Privacy Group. His practice includes labour, employment, human rights and privacy law.

Christopher has been involved in matters before all courts in Ontario, as well as before the Ontario Labour Relations Board, the Canada Industrial Relations Board and the Human Rights Tribunal of Ontario.

Christopher can be reached at 416.597.4882 or cmcclelland@blaney.com.

Organizations that collect or handle personal information are generally aware that they have an obligation to protect that information from loss or misuse. However, recent developments in the area of privacy law have highlighted the significant financial liabilities such organizations may face if they are found to be directly or indirectly responsible for privacy breaches.

In a recent example, the Ontario Superior Court of Justice certified a class action on behalf of 643 customers of a bank who allegedly had their private and confidential information misappropriated by an employee of the bank named Richard Wilson. In the case of *Evans v. Bank of Nova Scotia*[1], the plaintiffs have claimed damages against Mr. Wilson for breaching their privacy rights. However, the plaintiffs have also claimed damages against the bank on the basis that it was negligent in its supervision of Mr. Wilson and is vicariously liable for his improper acts.

Background

Mr. Wilson was employed by the bank as a mortgage broker. In the normal course of his duties, he had access to a significant amount of confidential information about the bank's customers, including sensitive financial information. During a period of approximately 10 months beginning in 2011, Mr. Wilson copied the information belonging to 643 customers and provided it to his girlfriend, who then disseminated the information to third parties for fraudulent and improper purposes. At least 138 of the bank's customers subsequently complained that they were the victims of identity theft or fraud, which negatively affected their credit rating. Two of those customers brought a class action against Mr. Wilson and the bank.

The Claims Against the Bank

For purposes of the certification motion, the Court found that the plaintiffs had made out a viable cause of action against the bank on the following grounds:

- **Negligence**: The bank acknowledged that it had failed to adequately supervise Mr. Wilson's activities, which in turn provided Mr. Wilson with the opportunity to access and remove confidential information for improper purposes. Mr. Wilson was able to access numerous customer accounts in a short period of time (as many as 47 customers profiles in 46 minutes on one occasion) and at odd hours during the night. Accordingly, it was possible that the bank could be found liable for being negligent in its supervision of Mr. Wilson.
- **Vicarious liability**: Mr. Wilson did not defend the case and therefore was deemed to admit that he had misappropriated the plaintiffs' information and breached their privacy rights. By failing to properly supervise its employees, the bank created a situation where there was a risk that Mr. Wilson could engage in the wrongful conduct that harmed the plaintiffs. It was therefore possible that the bank could be found vicariously liable for the breach of privacy committed by Mr. Wilson.

[1] 2014 ONSC 2135 (CanLII).

The plaintiffs relied on the tort of "intrusion upon seclusion" in support of their claim that their privacy rights had been breached. This tort was initially recognized in the decision of the Ontario Court of Appeal in *Jones v. Tsige*[2], which we reported on back in January 2012[3]. In that case, the Court of Appeal noted that the tort was limited to "deliberate and significant invasions of personal privacy" involving "financial or health records, sexual practices and orientation, employment, diary or private correspondence." In the *Evans* case, the Court found that the claim against Mr. Wilson (and, indirectly, against the bank) met that standard.

Implications for Employers

The decision in *Evans* was limited to the preliminary issue of whether to certify the plaintiffs' action as a class proceeding. The determination of whether the bank is ultimately liable for damages in this case will require a full trial. However, the Court of Appeal in *Jones* held that a single individual who suffered a breach of privacy was entitled to damages of $10,000. If the bank is found vicariously liable for the breach of privacy suffered by 643 individuals, the potential damages are significant.

There are steps employers can take to minimize the likelihood that they will find themselves the subject of a class action for breach of privacy. For example:

- Most employers will collect personal information from their employees and customers in the course of doing business. Employers must keep in mind that they are responsible for protecting this information from loss or misuse.
- Employers should be proactive in avoiding privacy breaches by establishing both administrative safeguards (policies on privacy and confidentiality and training on how to handle personal information) and technical safeguards (electronic monitoring and encryption technologies).
- Employers should monitor and supervise employees who have access to private and confidential information to protect against the actions of a "rogue employee" for whom they might be held vicariously liable.

While none of the above steps will eliminate the risk of a privacy breach, they could be critical in demonstrating that the employer is not responsible for creating the situation that led to the breach. ■

---

[2] 2012 ONCA 32 (CanLII).

[3] "A New Price Tag on Privacy? Ontario Court of Appeal Recognizes Tort of 'Intrusion Upon Seclusion'." *Employment Update* (January 24, 2012). Blaney McMurtry LLP.