Case Study: Grossman v. Nissan Canada

Defence + Indemnity

June 2020 - 7 min read

An employer who is innocent of negligence or other misconduct can be vicariously liable for the tort of intrusion upon seclusion based on a data breach committed by one of its employees.

***Grossman v. Nissan Canada*, 2019 ONSC 6180, per Belobaba, J.**

Facts + Issues

In December 2017 one of Nissan's employees (who was unidentified) stole personal information relating to Nissan customers. The employee then emailed a sample of the stolen data along with a ransom demand to Nissan threatening to disclose the data unless the ransom was paid.

The Court noted that "[a]t all material times, the unknown employee was an employee authorized to conduct business on behalf of the Defendants" and that "[t]his authority included accessing the information at issue for some purposes." (para 50).

The B.C. Privacy Commissioner investigated and was "satisfied that [Nissan] has made every reasonable effort to mitigate any potential harm to the affected individuals that may result from the breach and that appropriate steps have been taken to prevent future breaches".

Two years later there was no evidence that any of the stolen data had been disclosed publicly or misused. There was no evidence of any fraud or identity theft perpetrated against Nissan's customers. Since the customers' out-of-pocket expenses arising from the data breach were acknowledged to be "minimal to non-existent" they sought certification of a class action against Nissan alleging vicarious liability for the employee's commission of the tort of intrusion upon seclusion. The Plaintiffs relied on ***Jones v. Tsige***, 2012 ONCA 32 which had recognized that tort and held that nominal damages were available even in the absence of evidence of actual harm suffered.

Nissan opposed certification arguing, *inter alia*, that the minimal damages claim did not merit certification of a class action.

HELD: For the Plaintiffs; class action certified.

1. The Court held that the Plaintiffs' claim to a cause of action in vicarious liability for the tort of intrusion upon seclusion committed by one of its employees was not doomed to fail, following ***Evans v. Bank of Nova Scotia***, 2014 ONSC 2135; lv. to app. ref'd 2014 ONSC 7249. In that case the Court had certified an action against a bank in vicarious liability where one of its employees had disclosed personal information of bank customers to his girlfriend who, in turn, disclosed it to third parties for fraudulent purposes. (see paras 20 – 21.)
2. The Court found that the Plaintiffs shared common issues, including vicarious liability for intrusion upon seclusion (para 60).
    a. The Court held that although each individual's damages would be modest, a base amount "could be reasonably determined without proof by individual class members" (para 57)

Services
Intellectual Property

Industries
Cyber Liability Insurance

People
Brian Vail Counsel
bvail@fieldlaw.com

3. The Court held that a class action was preferable than requiring the Plaintiffs to bring their own individual claims, even though they could be brought in Small claims court:

64 Here, however, I have also certified the vicarious liability/intrusion issue and the related aggregate (base amount) damages issue. These are more contentious questions and their answers would not only advance but probably end the litigation. A class proceeding would allow both the vicarious liability and the aggregate damages issues to be decided once and for all on a class-wide basis.

[footnotes omitted]

COMMENTARY:

This decision recognizes the existence of the tort of intrusion upon seclusion and that an employer can be vicariously liable for such a tort as committed by one of its employees. Liability in vicarious liability, by definition, is imposed where the employer itself is innocent of any negligence or wrongdoing. Accordingly, a blameless employer can be liable for a data breach committed by one of its employees. **However, with respect, this decision is somewhat shaky as a precedent in light of recent authority from the United Kingdom.**

There has been recent U.K. authority where a blameless company was exonerated of vicarious liability based on vicarious liability law that is similar to Canada's: ***Various Claimants v. Wm Morrisons Supermarket PLC***, [2017] EWHC 3113 (Q.B.); aff'd [2018] EWCA Civ 2339 (Eng. C.A.); rev'd [2020] UKSC 12. A rogue employee of a supermarket company disclosed the confidential data of many of its employees as part of a personal vendetta to gain vengeance against the company for having disciplined him for another matter. The employee was a Senior IT Auditor who had been given the data for the legitimate purpose of transmitting it to the company's auditors. He did transmit it to the auditors but in the process copied it and went on to post it online. The U.K. Queen's Bench and Court of Appeal held that the company was not liable in direct liability for negligence or breach of data legislation but held it vicariously liable.

The U.K. Supreme Court reversed and exonerated the employer. It held that the Courts below had erred in interpreting the legal test for vicarious liability. It held that disclosure of the company's data online was not part of the employee Skelton's employment functions or within his field of activities. He had not been acting in the conduct of his employment when he publicly disclosed the data. The employee's motive for disclosure the data, pursuing a personal vendetta while engaged in a "frolic of his own" was not irrelevant. The temporal and causal link between the provision of the data to Skelton to submit to the company's auditors did not, in and of itself, satisfy the close connection test for vicarious liability.

In my view, the ***Morrisons*** case will be considered a significant precedent in Canada. The principles enunciated will likely be followed on the Canadian side of the pond. It is probable that the decisions at all three levels in the U.K. will be considered in analyzing any Canadian case. The three levels of the U.K. courts differed mainly about the application of the principles to that fact situation as opposed to the principles themselves. I suspect that ***Morrisons*** will be distinguishable on the facts of many cases which come before the courts. In many data breach situations the particular facts may be such that the employee's handling of the data is part of his or her employment duties or closely enough related to them or the employee's breach as opposed to a "frolic of his own" motivated by a desire to pursue a personal vendetta or wreak vengeance against the employer.

In ***Evans v. Bank of Nova Scotia***, 2014 ONSC 2135; lv to app. ref'd 2014 ONSC 7249, a bank employee disclosed confidential information pertaining to bank customers to his girlfriend who, in turn, disseminated them to third parties "for fraudulent and improper purposes". A class action was certified against the bank on the basis that an argument that the bank was vicariously liable for the employee's misconduct was not doomed to fail – the law was held to be "unsettled". As to the scope of the employee's employment, the Court held as follows:

22 In this case, the Bank created the opportunity for Wilson to abuse his power by allowing him to have unsupervised access to customers' private information without installing any monitoring system. The release of customers' confidential information by Wilson to third parties did not further the employer's aim of generating profits on good loans. Also, Wilson's wrongful acts were not related to friction, or confrontation inherent in the Bank's enterprise, but they were related to his necessary intimacy with the customers' personal and financial information. Wilson was given complete power in relation to the victims' (customers) confidential information, because of his unsupervised access to their confidential information. Bank customers are entirely vulnerable to an employee releasing their confidential information. Finally, there is a significant connection between the risk created by the employer in this situation and the wrongful conduct of the employee.

The Court in ***Evans*** did not refer to any of the ***Morrisons*** decisions. However, ***Morrisons*** may be distinguishable on the basis that the employee had unsupervised access to the data as part of his job description.

In ***Daniels v. McLellan***, 2017 ONSC 3466 a class action was certified by consent against a hospital in vicarious liability for the improper access to a number of patients' records. A patient (Daniels) who was also a hospital employee was visited by a number of other employees who ought not to have known that Daniels had been admitted. When Daniels complained the hospital investigated and discovered that 14 people on hospital staff had accessed Daniels' records and that another employee (McLellan) had improperly accessed the health records of 5,803 other patients (for which McLellan was dismissed). There was no analysis of whether or not the improper data access was sufficiently connected to McLellan's employment duties, as this was not in issue. The hospital admitted that the Plaintiffs had a cause of action against the hospital and, indeed consented to the certification.

In our view, the ***Evans*** and ***Daniels*** are not clearly inconsistent with principles set out in the U.K. Supreme Court in ***Morrisons*** as the factual basis of the Canadian cases does not disclose much detail about the scope of the employees' employment. These Canadian decisions did not hold that the employers were liable in vicarious liability but only that there was a cause of action that could be litigated.

However, with respect, the ***Grossman*** decision is quite arguably inconsistent with the ***Morrisons*** U.K. Supreme Court decision. The Court in ***Grossman*** did not refer to any of the decisions in ***Morrisons*** and, indeed was decided before the U.K. Supreme Court decision was issued. In ***Grossman*** the identity of the rogue employee was unknown. Aside from a desire to personally profit as part of an extortion scheme nothing was known as to the employee's motivations. Accordingly, the same may be said as to the scope of that employee's employment duties. With respect, the Court undertook little or no analysis of the employee's job description, noting only that the employee was "authorized to conduct business on behalf of the Defendants" and that"[t]his authority included accessing the information at issue for some purposes". It may be that more detail was available to the litigants on this point but the decision reveals nothing further. After ***Morrisons*** in the U.K.S.C., it seems clear that a criminal personal motive on the part of the rogue is a relevant fact.

Accordingly, the law in Canada on this point is unsettled and will remain so until our Courts grapple with it in more detail. It remains to be seen whether the Canadian courts will follow ***Morrisons*** in the U.K. Queen's Bench and Court of Appeal or the decision of the Supreme Court. There is much useful analysis of the relevant law in all three U.K. decisions. Much will depend on the facts in any Canadian case.