Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Employers May Be Liable For Employee Data Breaches

By **Pulina Whitaker** (March 16, 2018, 2:45 PM EDT)


Pulina Whitaker

In December 2017, the U.K. High Court, in Various Claimants v. WM Morrisons Supermarket PLC, held for the first time that an employer could be vicariously liable for an employee's misuse of data. The case is also the first example of class action litigation in the data protection arena in the U.K., potentially marking a new risk for employers at a time when the spotlight is on data protection obligations with the forthcoming General Data Protection Regulation ("GDPR") in force on May 25, 2018.

Background

Andrew Skelton was a disgruntled senior IT auditor employed by Morrisons and had been involved in a project involving payroll data. In 2014, Skelton took the personal information of around 100,000 colleagues via a USB stick and published it on the internet. He subsequently sent it to various newspapers. Skelton was subsequently convicted of offences under the Computer Misuse Act 1990 and the Data Protection Act 1998 and he is currently serving a term of eight years in prison. There was no substantive allegation that Morrisons had breached its obligations as the data controller to protect this personal data.

The claimants in the current case were a group of over 5,500 Morrisons employees affected by the data leak. They sought compensation from Morrisons for breach of the DPA, as well as common law claims for the tort of misuse of private information and an equitable claim for breach of confidence. The claimants alleged both a direct breach of the DPA by Morrisons for failing to protect their data and that Morrisons was vicariously liable for the actions of Skelton.

Decision

Morrisons, as the employer, would ordinarily be regarded as the data controller of payroll data. It determines how the data is used for its own purposes. Morrisons sought to argue that, in relation to Skelton's unlawful and unauthorized disclosure of the payroll data, Morrisons was not the data controller and that Skelton was a data controller in his own right. As such, he, not they, should be found liable for breaching the DPA. The High Court rejected the direct breach claim since Morrisons was not the "data controller" (as defined in the DPA) at the relevant time with respect to the data breach. The court also found that Morrisons had in place proper control mechanisms to protect employees' personal data. There was no finding that Morrisons had breached the DPA in their system of control and security processes regarding the data (there was a finding of one minor breach of the DPA which did not give rise

to any loss to the claimants). This is an important finding for Morrisons, as it means they were not directly liable for breaching their obligations to protect the employees' data under the DPA.

The High Court, however, found in favor of the claimants with respect to the vicarious liability claim. This finding, however, means that employers can still be liable even though they had correct policies and procedures in place to train employees and protect personal data because of the actions of rogue employees.

The High Court held that the DPA does not exclude the possibility of vicarious liability and that an employer can be vicariously liable for the actions of employees in relation to data breaches. In the current case, the High Court held that there was a sufficient connection between Skelton's employment and the wrongful conduct to hold Morrisons liable. The High Court found that "there was an unbroken thread that linked his work to the disclosure: what happened was a seamless and continuous sequence of events," even though the disclosure itself did not occur on a company computer or during working hours.

The case is now set to be heard in the Court of Appeal.

What Does it Mean for Employers?

The decision is significant for all organizations who handle personal data. It demonstrates that even where an employer has done everything it reasonably can to prevent employees misusing personal data, and is not itself legally at fault, it may nevertheless be vicariously liable for the actions of those employees. The judgment also illustrates the broad approach given to the "close connection" between employers and their employees test. Employers should therefore be alive to potential liabilities in this area and review employee monitoring practices as well as recruitment and training measures.

It is also the first case of group action litigation being brought against an employer in relation to data protection. Such class actions are common in the US and this case indicates a greater trend to class actions in the English legal system. The Court has already granted Morrisons permission to appeal given the sensitive nature of the case.

The new GDPR can give rise to significant liabilities of up to the higher of 4% of global turnover or EUR 2 million for data breaches. It remains to be sign how the data protection authorities and/or courts will apply this vicarious liability approach to such stringent fines.

What more can employers do to protect themselves against being found vicariously liable for acts of their employees, where there is no suggestion that they have breached their obligations to have "appropriate technical and organizational security measures" to protect the data? It was suggested by the claimants that Morrisons should have monitored Skelton's conduct after a prior disciplinary hearing after which it is believed that he became disgruntled with his employer. Clearly, this raises privacy issues in itself as employees need to have good reason to conduct monitoring of their employees and must do so in a manner that is proportionate to the concern and mindful of their privacy rights. A general conclusion that all disciplined employees need to be monitored is unlikely to be a sufficient reason to conduct specific monitoring of those employees. Technological solutions such as controls over the downloading of data to USB sticks in an authorized manner and audits of the location of such USB sticks where downloaded data has been authorized are entirely reasonable in the current environment of data breach risks. Automatic red flags being raised for certain internet searches may also have alerted Morrisons that he was researching how to conceal his identity using The Onion Router (TOR).

The case serves to underline the importance of robust recruitment and screening procedures as well as culture of the workplace and having in a place a “speak up” culture that may have allowed other employees to raise concerns about Skelton’s conduct.

Pulina Whitaker is a partner with Morgan Lewis & Bockius LLP in London.