UK Supreme Court Rules Employer Not Liable for Rogue Employee's Malicious Data Breach

3 April 2020

In a welcome decision for UK employers, the UK Supreme Court has ruled that WM Morrison Supermarkets plc ("Morrisons"), the supermarket chain, was not vicariously liable when an employee deliberately disclosed the personal details of almost 100,000 co-workers. The Supreme Court ruling overturns decisions of the High Court and Court of Appeal. The fact that his employment gave the employee the opportunity to commit the wrongful act was not sufficient to warrant the imposition of vicarious liability. Companies should still be alert to the possibility of being held vicariously liable for data breaches resulting from the acts of a malicious employee where the connection to the employee's duties is closer than in this case and they should continue to implement robust technical and organizational measures to address that risk.

Background. The data breach in this case was committed deliberately by a senior internal auditor employed by Morrisons, Andrew Skelton. The court decision reports that Skelton harboured a grudge against Morrisons, following a previous disciplinary issue, which motivated his actions. In order to facilitate an external audit, Skelton was given access to payroll data relating to the whole of Morrisons' workforce: around 126,000 employees. These consisted of the name, address, gender, date of birth, phone numbers, national insurance number, bank sorting code, bank account number, and salary of each member of staff. Skelton transmitted the data to the external auditor, as he was instructed to do. He also copied the data to a personal USB stick. He then used the username and date of birth of a fellow employee to create a false email account, in a deliberate attempt to frame the colleague. Skelton uploaded a file containing the data of 98,998 of the employees to a publicly accessible file-sharing website. He made the disclosure when he was at home, using a mobile phone he had purchased for the purpose and the false email account.

Skelton subsequently sent CDs containing the file anonymously to three UK newspapers, purporting to be a concerned member of the public. The newspapers did not publish the data, but one of them alerted Morrisons. As well as taking remedial steps, Morrisons informed its employees and undertook measures to protect their identities. The police were also informed. Skelton was arrested a few days later and

eventually sentenced to eight years' imprisonment. In total, Morrisons spent more than £2.26 million dealing with the breach's immediate aftermath.

Claims. A large number of employees whose data had been disclosed brought a claim for compensation against Morrisons under a group litigation order (an opt-in collective claims procedure under the Civil Procedure Rules), arguing that it had breached its statutory duty under S.4(4) Data Protection Act 1998 ("DPA 1998", now replaced by the Data Protection Act 2018). S.4(4) DPA 1998 created an obligation on data controllers to comply with the data protection principles set out in the legislation which were similar to, but less onerous in some ways than, those under the 2018 Act and the European General Data Protection Regulation. The claimants also brought claims under common law for misuse of private information and in equity for breach of confidence. They argued that Morrisons had both primary liability for its own acts and omissions, and vicarious liability for Skelton's actions.

Earlier decisions. The High Court, with which the Court of Appeal agreed, held that Morrisons had no primary liability as it had not committed the breaches alleged, but concluded that there was a sufficient connection between Skelton's actions and his employment to mean that Morrisons was vicariously liable on each basis claimed. The fact that the disclosures were made from home using personal equipment, and on a non-working day, were not enough to break that connection, according to the lower courts. Morrisons appealed.

No vicarious liability. The Supreme Court held that the mere fact that Skelton's employment gave him the opportunity to commit the wrongful act was not sufficient to warrant the imposition of vicarious liability. The Supreme Court decided that it was "abundantly clear" that Skelton was not engaged in furthering Morrisons' business when he made the unlawful disclosure, as he was pursuing a personal vendetta, and that his wrongful conduct "was not so closely connected with acts which he was authorised to do that, for the purposes of Morrisons' liability to third parties, it can fairly and properly be regarded as done by him while acting in the ordinary course of his employment", which remains the correct test for whether vicarious liability is established.

Impact. The decision is a welcome confirmation that, where employees deliberately use personal data for a purpose which is clearly outside the scope of their duties or authority, the employer should not be liable for the resulting losses merely because the breach was carried out by an employee who legitimately had access to the data as part of his role. Employers must still of course maintain adequate security measures and safeguards, and restrict access to personal data only to those employees who need to have access to carry out their roles, as well as conducting regular training on data protection obligations and the steps employees must take to comply. This is particularly important given that the

Supreme Court's reasoning leaves open the possibility that, on different facts, an employer might still be held liable for a data breach caused by the malicious acts of one of its employees, if there was a closer connection to their employment than with Skelton.

Separately, Morrisons sought to argue that it is not possible in principle for an employer to have vicarious liability for actions carried out by an employee who is a data controller in his own right, which may occur, for example, where the employee has decided to process personal data for a particular purpose not directed by the employer such as to further their own personal business ventures. Although it was not necessary to make a definitive ruling on this issue because of its other findings, the Supreme Court expressed its view that there is no reason that an employer cannot be vicariously liable for breaches of data protection legislation where its employees are data controllers in their own right, as this was not expressly excluded by the wording of DPA 1998. The same would apply for its successor, the Data Protection Act 2018. The door remains open for vicarious liability claims where the actions leading to a data breach are carried out by an employee in circumstances more closely linked to the employee's duties for the employer.

* * *

Please do not hesitate to contact us with any questions.

LONDON

Karolos Seeger
kseeger@debevoise.com

Jane Shvets
jshvets@debevoise.com

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Christopher Garrett
cgarrett@debevoise.com

Robert Maddox
rmaddox@debevoise.com