Published on *The National Law Review* https://natlawreview.com

Morrisons Data Breach – Revisiting the "Rogue Employee" Question

Article By:

Andrea Ward

As reported last week in our sister blog, Employment Law Worldwide, the UK Supreme Court in a landmark decision has reversed the earlier decision of the Court of Appeal, finding that Morrisons is not vicariously liable for the actions of a disgruntled employee who unlawfully disclosed personal data belonging to nearly 100,000 colleagues.

How did the claim arise?

In March 2014, Morrisons became aware that a file containing the personal data of 99,998 employees had been posted to a file-sharing website. This file contained personal data including names, dates of birth, addresses, National Insurance numbers and bank account details, all of which had been entrusted to Andrew Skelton, a senior internal IT auditor, who had been tasked with collating the information for the supermarket's auditors. Apparently motivated by a grudge against the company, Skelton had downloaded the data onto a personal USB stick and later posted it to the file-sharing website and to several newspapers. Skelton was subsequently convicted of offences under the Computer Misuse Act 1990 and the Data Protection Act 1998 (DPA) and was sentenced to eight years in prison.

Around 5,000 of the employees whose data had been unlawfully disclosed by Skelton brought claims against Morrisons, arguing that as his employer, it was vicariously liable for Skelton's actions. This group had grown to over 9,000 by the time of the Supreme Court hearing.

With respect to data protection, the Court of Appeal, upholding the High Court's decision, found that Morrisons was not directly liable for the data breach. Morrisons had taken appropriate technical and organisational measures to protect the data. However, Morrisons was held vicariously liable for Skelton's actions. Skelton's intention was to damage Morrisons, but the way he chose to do so was by releasing the personal information of a large group of employees. "*The issue is not so much at whom the conduct was aimed, but rather upon whose shoulders it is just for the loss to fall*." was how the judge put it. Against that backdrop, Morrisons faced multiple claims for compensation from the affected employees and appealed the decision to the Supreme Court.

What did the Supreme Court decide?

Morrisons asked the Supreme Court to consider whether Morrisons could be found vicariously liable for its employee's conduct and if so, whether the DPA excludes vicarious liability for statutory torts committed by an employee who himself is acting as a data controller under the DPA.

The key question was whether Skelton's unlawful disclosure was closely connected to the work he was authorised to do and, for the purposes of his employer's liability to third parties, whether his wrongful disclosure could be regarded as done by him in the ordinary course of his employment.

During the proceedings, counsel for Morrisons attempted to rely on section 13 DPA and mooted that they should not be liable for the rogue employee's acts even if he had been acting within the course of his employment. They recognised the potential liability placed on controllers i.e. the rogue employee in this case under sections 13(1) and (2) DPA, but argued that they had exercised all reasonable care and had met the defence available under section 13(3) DPA.

Although the above argument was not accepted, the Supreme Court overturned the Court of Appeal's decision. The Supreme Court found that although Skelton's employment gave him the opportunity to commit the wrongful act, it would not be sufficient to warrant the imposition of vicarious liability on Morrisons. The Court reasoned that: *"In the present case, it is abundantly clear that Skelton was not engaged in furthering his employer's business when he committed the wrongdoing in question. On the contrary, he was pursuing a personal vendetta, seeking vengeance for the disciplinary proceedings some months earlier."*

Morrisons could not, therefore, be vicariously liable for the actions of the individual in this case. The Court also found that vicarious liability was not excluded by the DPA.

What is our view?

This case is important in the context of liability for data breaches. It highlights that if employers can demonstrate they have met their own obligations as data controllers then they cannot be found liable for the actions of employees acting on their own personal motives outside the scope of their duties.

Whilst most data breaches are caused by human error or malicious external attacks, we are seeing an increase in the number of thefts or leaks of data by employees. The Information Commissioner's Office is taking a more active approach in the prosecution of such cases. Companies should continue to take appropriate measures to protect and prevent such actions, as the risk of vicarious liability remains.

Employers need to be careful to ensure that the responsibilities of those allowed to access and protect personal data are constantly reviewed.

Cases like this one highlight the costs to businesses of such actions by rogue employees. Morrisons had reportedly spent more than £2m in dealing with the fallout of the disclosure, most of this on identity protection measures for its employees. Even if a data controller is deemed compliant, if an employee acts in a malicious way whilst carrying out their duties, the cost both in terms of financial and brand reputation can be huge – particularly, as in this case, where class action is brought by aggrieved individuals. If the Supreme Court had rejected Morrisons' appeal, there would have been thousands of compensation claims to pay or settle.

What do controllers need to consider?

It is unclear whether the final outcome in the UK, based on the Supreme Court's interpretation of UK employment law, would be the same if this case had arisen in one of the EU Member States in continental Europe. Furthermore, it is important to note that the data breach took place before the GDPR came into in force, and arguably the strict obligations (and financial penalties, not to mention claims for compensation) under the GDPR make data security even more important. Moreover, the GDPR's introduction of the so-called Accountability Principle for data controllers could have an impact on the liability assessment going forward.

Bearing in mind the enhanced obligations that the GDPR places on data controllers, employers should ensure that all appropriate access measures and other technical controls are put in place to protect confidential information and personal data, including protection against unauthorised downloads/use of personal storage devices, and ensure that all staff are aware of the business' information security rules. Controllers should also ensure that appropriate training and awareness-raising measures have been put in place and are refreshed, so that the chances of a rogue employee being able to carry out this kind of action are minimised.

More than anything, the Morrisons case underlines the requirement to stay abreast of best practice in systems and data security and putting the maximum reasonable measures in place to safeguard against breaches. These are decisions that need to trickle down from the top, whether from the IT Director in larger organisations or from owners of SME businesses who have responsibility for IT. It is about perception of the risk and then mitigating and insuring against it. Getting that right takes time, effort, knowledge and experience. An understanding of the Computer Misuse Act 1990 and the principles of good information handling outlined in the Data Protection Act 2018 provide a sound starting point.

Co-authored by Samikah Ahmed

National Law Review, Volumess X, Number 97