Morrison Escapes Responsibility for Cyber-Rogue Employee – the Limits of Vicarious Liability

By: Andrew Shindler

On 1 April 2020, the UK Supreme Court handed down its judgment in WM Morrison Supermarket v. Various Claimants. The Court’s decision, significant under both data protection law and the general law of tortious liability, will come as a relief to all businesses, whatever their size, who employ people to carry out activities in the UK.

Background
The case concerned an appeal by WM Morrison, the supermarket chain, against a 2018 Court of Appeal decision rejecting its earlier appeal against a High Court ruling.

Both the High Court and the Court of Appeal ruled against Morrison in favour of nearly 10,000 current or former employees. Specifically, both courts had held Morrison vicariously liable for the unlawful actions of another employee, Andrew Skelton, who worked in its internal audit team at the relevant time.

Skelton harboured a grudge against Morrison because of disciplinary action it had previously taken against him. With the sole intention of damaging it, he surreptitiously copied the payroll data of Morrison’s entire workforce, over 100,000 people, onto a personal USB stick while sending it to KPMG, its external auditor, as part of his duties. A couple of months later, in January 2014, Skelton uploaded a file containing the data to a public website, using a false email account set up in the name of another employee. He also posted links to the data on other websites.

This data breach did not become widely known and did not have the harmful effect on Morrison that Skelton desired. So, in March 2014, as Morrison was due to announce its 2013 financial results, Skelton sent the file anonymously to three UK newspapers pretending to be a concerned member of the public. One of the newspapers alerted Morrison. The police were involved and swiftly detected and arrested Skelton. He was convicted and sentenced to eight years’ imprisonment for fraud, securing unauthorised access to computer material and disclosing personal data. Morrison spent over £2 million in dealing with the aftermath.

Legal Proceedings
The claimants brought proceedings against Morrison arising out of Skelton’s misuse of their personal payroll data. Their claim was for breach of confidence, breach of the Data Protection Act 1998 (DPA), and misuse of private information. They claimed damages for “distress, anxiety, upset and damage.” Although the claim related to the 1998 DPA, the issues in the case apply equally to the GDPR and the UK’s related 2018 DPA.

The High Court ruled that Morrison was not primarily liable for any of the claims, Skelton’s acts not being authorised by it. However, it did hold Morrison vicariously liable for Skelton’s acts.

Morrison appealed. The Court of Appeal dismissed its appeal on similar grounds to the High Court. It ruled:

• the DPA did not exclude causes of action for misuse of private information or breach of confidence;
• The DPA did not exclude the principle of vicarious liability; and

• Morrison was vicariously liable because Skelton’s wrongful acts were “within the field of activities assigned to him…. The relevant facts constituted a seamless and continuous sequence…or unbroken chain of events.”

Morrison appealed again, to the highest court in the UK, on the grounds that this was a point of law of public importance in which the lower courts had reached the wrong conclusion.

**The Supreme Court’s Decision**

The President of the Court, Lord Reed, gave the leading judgment in a unanimous decision. The predominant issue was whether, on the facts and applying the law, Morrison was vicariously liable for Skelton’s actions. Analysing previous case law, Lord Reed stated that the general principle (which applied in all but certain exceptional categories of case) is that employers are vicariously liable to third parties where their employees’ wrongful conduct is

“so closely connected with acts [they are] authorised to do that…it may fairly and properly be regarded as done by [them] while acting in the course of [their] employment.”

His Lordship went on to explain that this principle must be applied with regard to the circumstances. He emphasised: “’Fairly and properly’ is not an invitation…to judges to decide cases according to their personal sense of justice but requires them to consider…the guidance derived from decided cases.”

Lord Reed concluded that the lower courts had erred in their decisions, based on their misinterpretation of the previous Supreme Court case on vicarious liability, *Mohamud v WM Morrison* (2016). In that case, Morrison was held vicariously liable for its petrol station attendant’s violent assault on a customer he was serving in the course of his duties.

Lord Reed ruled that the “close connection” test is not based on a temporal or causal connection or a matter of social justice. He considered that the lower courts had taken references in *Mohamud v Morrison* to ‘an unbroken sequence of events’ out of context and given them an unmerited significance. They had also wrongly discounted Skelton’s motive. The following factors were particularly important:

• Disclosing data on the internet was not part of Skelton’s functions.

• A temporal or causal connection does not itself satisfy the close connection test.

• It was highly material that Skelton’s motive was personal rather than for his employer’s business.

The Supreme Court had therefore looked at the facts afresh and compared them to those of previous cases. The key distinction in past cases was between circumstances where employees were engaged, however misguided, in furthering their employers’ business and those where they were solely pursuing their own interests — to use the time honoured phrase — “on a frolic of [their] own.” Here, Skelton was pursuing a personal vendetta and his conduct did not meet the close connection test.

The second issue in the appeal was whether the DPA excluded the imposition of vicarious liability. This was of theoretical interest only in the case, given the finding that Morrison was not vicariously liable for Skelton’s acts, but is important for future cases where the acts of an employee breach implicate GDPR or other data protection laws. Morrison’s argument was a technical construct based on Skelton rather than Morrison being the data controller of the data he unlawfully published. The Court was entirely unpersuaded that there was any explicit or implicit exclusion of vicarious liability in GDPR or the DPA and rejected this argument out of hand.

**Conclusions**

The Supreme Court’s decision will come as welcome relief to Morrison and its insurers, which faced potentially huge financial liability to around 100,000 possible claimants.
The decision will also provide some comfort to other organisations, and their insurers, that they will not be liable for wrongful acts of their employees, which has some connection, however tenuous, with their employment.

However, there remains a reasonably fine line between the circumstances in which the “closely connected” test for vicarious liability is satisfied and those in which it is not. Employers should therefore remain prudent and base their risk management decisions on the general principle that they will usually be liable for their employees’ acts, where those acts reasonably relate to their employment.

With regard to vicarious liability in the context of data protection and its sister, cyber-security, it is no surprise that English courts will hold employers vicariously liable for breaches of GDPR and other data protection laws committed by their employees where “closely connected” with their employment. This decision does not therefore reduce the need for good data protection practice in the workplace, including training employees and monitoring their knowledge, awareness and compliance. These remain essential to avoid or reduce the risk of GDPR fines, negative publicity and liability for compensation.

For more information on the matters discussed in this Locke Lord QuickStudy, please contact the author.

Andrew Shindler  |  +44 (0) 20 7861 9077  |  andrew.shindler@lockelord.com