

UK Supreme Court Rules Morrisons Not Vicariously Liable for Malicious Data Breach by Employee

April 20, 2020

Case: *WM Morrison Supermarkets plc v Various Claimants* [2020] UKSC 12

In a decision that employers will welcome, the UK Supreme Court recently ruled that Morrison Supermarkets (Morrisons) was not vicariously liable for a data breach committed maliciously by a former employee who, acting to satisfy a personal vendetta against Morrisons, disclosed employee payroll data online.

The judgment examined the law on employers' vicarious liability for wrongs committed by their employees and restated that the test for vicarious liability was whether the acts the employee committed were "so closely connected" with the acts their employer authorized them to carry out that it can "fairly and properly be regarded as done" by the employee acting in the ordinary course of his or her employment. In this case the employee had committed acts to further a personal vendetta rather than any objective of the employer, and there was no close connection between the acts of the employee and those that he was authorized to perform. The fact that the employer had given the employee access to the payroll data, as an internal IT auditor, was not sufficient in itself to impose vicarious liability on the employer under the Data Protection Act 1998 (DPA) (now repealed). While it was unnecessary for the Supreme Court to decide the point given its finding on vicarious liability, the Court also concluded that the provisions of the DPA, which impose statutory liability on a data controller, do not exclude the imposition of common law vicarious liability.

Following the [judgment](#), it is important that employers continue to regularly assess their obligations under the General Data Protection Regulation (GDPR) and apply appropriate technical and organizational security measures, as the judgment makes clear employers can be vicariously liable where such breaches are committed by an employee in the ordinary course of their employment. This is particularly important as enforcement actions and significant fines by European supervisory authorities under the GDPR, as well as moves to bring mass privacy claims, are increasing.

The Facts

Andrew Skelton was an auditor in Morrisons' audit team who bore a grudge against his employer following disciplinary proceedings for minor misconduct in July 2013. In November 2013, during an

external audit, Skelton had to provide payroll data to Morrisons' auditors, which he duly did. However, Skelton also made a copy of the data and, in an attempt to frame another employee involved in the disciplinary proceedings, Andrew Kenyon, uploaded the data to a file-sharing website using an email account he had created in Kenyon's name.

Later, when Morrisons was due to announce its annual financial results, Skelton sent CDs containing the data to three newspapers, purporting to be a concerned member of the public who had found the data on the file-sharing website. The newspapers contacted Morrisons, which took steps to remove the data and informed the authorities. Subsequently, Skelton was convicted of a number of offenses and sentenced to eight years' imprisonment.

The claimants brought civil proceedings alleging that Morrisons was liable both on a primary basis and vicariously for breach of statutory duty under the DPA and under common law for misuse of private information and breach of confidence. While the High Court rejected the claimants' claims that Morrisons was primarily liable, it upheld the claims that Morrisons was vicariously liable for Skelton's conduct. The Court of Appeal upheld the High Court's judgment.

The Supreme Court's Judgment

The test for vicarious liability

The Supreme Court noted that the lower courts appeared to have concluded that Lord Toulson established a test for vicarious liability in *Mohamud v WM Morrison Supermarkets plc*¹ that disregarded an employee's motive and focused instead on whether (i) there was a temporal or causal connection between the employment and the wrongdoing, and (ii) whether as a matter of social justice it was right to hold the employer liable. The Court pointed out that such a test would constitute a significant change in the law from the test set out in previous authorities, in particular *Dubai Aluminium Co Ltd v Salaam*.²

However, reading Lord Toulson's statements in *Mohamud* in context, the Supreme Court concluded that it was clear he did not intend to establish a new test for vicarious liability. In particular, he endorsed the leading authorities and expressly stated that he was summarizing the present state of the law "in the simplest terms". Crucially, Lord Toulson did not suggest departing from Lord Nicholls' (fuller) authoritative statement in *Dubai Aluminium* that the court has to decide whether the wrongful conduct is so closely connected with acts the employee was authorized to do that, for the purposes of the employer's liability, it may fairly and properly be regarded as done by the employee while acting in the ordinary course of his employment.³ Accordingly, the Supreme Court decided the courts must apply the principle set out in *Dubai Aluminium* in light of the guidance in the case law.

Further, the lower courts misunderstood Lord Toulson's statement regarding the employee's motive. In *Mohamud*, Lord Toulson concluded that there was a close connection between the employee's conduct and the acts Morrisons authorized him to do (partly) because the employee, a petrol pump attendant, purported to act on Morrisons' business when he carried out an assault on a customer, rather than his conduct being motivated by anything personal. Clearly, therefore, whether the employee was acting on his employer's business or for personal reasons was important.

Morrisons' vicarious liability

Applying the test in *Dubai Aluminium*, the Supreme Court noted that the question was whether Skelton's

unlawful disclosure was so closely connected with providing the data to the auditors that it may fairly and properly be regarded as being made while acting in the ordinary course of his employment.

Although Skelton had the opportunity to unlawfully disclose the data only because of his employment, the authorities were clear that this was insufficient to impose vicarious liability.⁴ The decided cases drew a clear distinction between instances where an employee is engaged (even misguidedly) in the employer's business and cases where an employee pursues his or her own interests.⁵ The Supreme Court concluded it was obvious that, as a result of the disciplinary proceedings, Skelton was on a personal vendetta in disclosing the data and that his conduct therefore did not meet the close connection test set out in *Dubai Aluminium*. Accordingly, the Supreme Court found that Morrisons was not vicariously liable for Skelton's conduct.

The DPA and vicarious liability

Although the Supreme Court did not have to decide whether the DPA excluded vicarious liability for the statutory and common law torts Skelton committed, it nonetheless decided to express a view.

Although, the parties accepted that Skelton was a data controller in his own right in respect of the unlawful disclosure, Morrisons contended that it was not vicariously liable for his breach of duty on the basis that the DPA impliedly excluded such liability. In particular, the provisions of the DPA that provided for compensation for failure to comply with its terms referred only to the data controller, not the employer.

However, the Supreme Court concluded that as the DPA was silent regarding the data controller's employer, there was no inconsistency between the imposition of statutory liability on the data controller and the imposition of vicarious liability on the employer. Accordingly, the DPA did not exclude the common law doctrine of vicarious liability.

While the DPA has now been replaced by the Data Protection Act 2018 (2018 Act) and the GDPR, the Supreme Court's view that the DPA does not exclude an employer's vicarious liability for statutory or common law breaches by an employee will likely apply to the 2018 Act as the definition of data controller in the 2018 Act (derived from the GDPR) remains broadly unchanged. Similarly, the compensation provisions in Article 84 of the GDPR are silent as to the position of an employer.

Conclusion and Practical Impact for Employers

Given the stringent requirements of the GDPR and the strict nature of vicarious liability, organizations will welcome the Supreme Court's ruling. The judgment provides welcome clarity regarding the correct test to apply in determining whether an employer is vicariously liable for the wrongdoing of an employee. Following the Supreme Court's judgment, if an employee commits a statutory or common law tort for personal reasons (for example, as part of a personal vendetta) and not in circumstances closely connected to the ordinary course of their employment, the employer is unlikely to be vicariously liable for his or her conduct.

However, it is important for employers to understand that they will remain directly liable for data breaches and non-compliance under the GDPR (and in the UK, the 2018 Act) and therefore vicariously liable for unauthorized acts of an employee acting in the ordinary course of his or her employment. In practice, it is much more common for a breach to occur as a result of an employee's inadvertent act —

such as sending a data file to the wrong email address, copying in a third party accidentally to an email or leaving a laptop in a taxi on the way to a business meeting — than as a result of a rogue employee deliberately publishing data on thousands of employees online as a personal vendetta. In the former examples, it can clearly be argued that these acts occur with the employee acting in the ordinary course of their employment for which the employer may be vicariously liable.

The judgment further demonstrates the importance for employers and businesses to regularly review how they address their obligations under the GDPR, including implementing appropriate technical and organizational measures. These measures should include a combination of data security controls, audits, data breach response planning, developing appropriate data protection policies and procedures and training of employees, particularly those who come into contact with personal data in their day-to-day roles.

¹ [2016] UKSC 11.

² [2002] UKHL 48.

³ *Ibid.*, para. 23.

⁴ E.g., *Morris v C W Martin & Sons Ltd* [1966] 1 QB 716, 737; *Lister v Hesley Hall Ltd* [2001] UKHL 22.

⁵ E.g., *Joel v Morison* (1834) 6 C & P 501.

CONTACTS

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work, or

Sara George , Partner	+44 20 7360 3741, sara.george@sidley.com
William RM Long , Partner	+44 20 7360 2061, wlong@sidley.com
David Smith , Senior Managing Associate	+44 20 7360 3766, david.smith@sidley.com

Attorney Advertising—Sidley Austin LLP is a global law firm. Our addresses and contact information can be found at www.sidley.com/en/locations/offices.

Sidley provides this information as a service to clients and other friends for educational purposes only. It should not be construed or relied on as legal advice or to create a lawyer-client relationship. Readers should not act upon this information without seeking advice from professional advisers. Sidley and Sidley Austin refer to Sidley Austin LLP and affiliated partnerships as explained at www.sidley.com/disclaimer.

© Sidley Austin LLP