EMPLOYMENT
LITIGATION, DISPUTE RESOLUTION AND INVESTIGATIONS
TECHNOLOGY

UK Supreme Court allows appeal in landmark decision on employers' liability in class action for mass data breach by employee

April 2020

The recent UK Supreme Court decision in Morrisons is an important development for employers concerned about their potential vicarious liability for a data breach caused by an employee and how they might mitigate such liability and/or respond to a data breach.

This decision will also be an important consideration for any Irish Courts in the context of possible data protection actions, misuse of private information and breach of confidence.

In an eagerly anticipated judgment delivered on 1 April 2020, the UK Supreme Court allowed an appeal against the decision of the High Court in December 2017 (which was upheld by the Court of Appeal of England and Wales the following year) in *WM Morrison Supermarkets plc v Various Claimants*. In overturning the earlier courts' decisions, the Supreme Court held that WM Morrison Supermarkets ("Morrisons") was not vicariously liable for the actions of a disgruntled employee who deliberately leaked approximately 100,000 employees' payroll and other data online. This decision will come as a relief to many employers who may have been concerned by the potential implications of the High Court and Court of Appeal Decisions, which gave rise to a position where even the most conscientious employers could potentially be held liable for the actions of rogue employees.

Factual background

The facts of the case are set out in our previous briefing, available on our website here. In summary, the employee at issue ("S") was a senior IT internal auditor employed by Morrisons. Following an internal disciplinary matter, S bore a grievance against his employer. Some months later, he was instructed by Morrisons to send payroll data (and other types of data) to an accountancy firm. Having copied the data onto his personal computer, S later released it onto a file-sharing website, exposing Morrisons to the risk of thousands of payouts in a collective claim by 5,518 employees for compensation over the data breach under Section 4(4) of the then UK Data Protection Act (the "DPA"), as well as claims under common law for the misuse of private information and in equity for breach of confidence.

High Court and Court of Appeal

The employees argued that Morrisons had primary liability for its own actions and was vicariously liable for the acts of S. Although Morrisons argued that by imposing vicarious liability for the employee's actions the Court would be "*acting as an accessory in furthering the employee in question's criminal aims*", the High Court and the Court of Appeal found that the employee's motive was irrelevant. The Court of Appeal adopted a broad approach to vicarious liability in its decision, ruling that the employee's wrongful act was sufficiently connected with acts which he was authorised to do such that WMMS should be held liable.

Supreme Court

The Supreme Court, in overturning this finding, has provided some long-awaited clarity to employers on vicarious liability, and consequently also on their obligations in respect of employees' personal data. The Supreme Court held that the High Court and the Court of Appeal misunderstood the principles governing vicarious liability in a number of relevant respects. In particular, the Court found that that the earlier decisions misapplied the relevant case law in finding that the leaking of the data formed part of S' functions or field of activities so that it was an act which he was authorised to do and in holding that his motives were irrelevant.

Applying the 'close connection' test of vicarious liability afresh, the Court said that the question was whether S' wrongful acts were "*so closely connected with acts that he was authorised to do" that they "may be fairly and properly be regarded as done by him while acting in the ordinary course of his employment*." Finding that they were not, the Court drew a distinction between the actions of employees who are engaged, however misguidedly, in furthering their employers' business, (in which case the 'close connection test will be satisfied') and cases where the employee is engaged "*solely in pursuing his own interests: on a 'frolic of his own', in the language of the time-honoured catch phrase*" (in which case the test will not be satisfied and the employer will not be held vicariously liable).

Comment

Although the Supreme Court judgment may have stemmed a potential wave

of data-liability challenges following on from the High Court and Court of Appeal decisions, when the 'close connection' test will be satisfied (and consequently what actions an employer may be held liable for when it comes to data breaches by employees) is not clear cut.

In the present case, it was "*abundantly clear*" that S was not engaged in furthering his employer's business when he committed the wrongdoing in question. This was an extreme situation where the employee was "*pursuing a personal vendetta, seeking vengeance for the disciplinary proceedings some months earlier*." However the distinction between when an employee will be furthering their employer's business and when they will be on a 'frolic of their own' may not always be so easily drawn and will likely be the subject of an internal investigation supported by forensic IT analysis. Employers can still be held liable for the acts of employees if those acts have a sufficient connection to acts that they are authorized to do, and post-GDPR, claimants are not required to show any financial loss in seeking compensation for non-material damage.

Despite the note of comfort given by this judgment, it is notable that Morrisons spent £2.26 million dealing with the immediate aftermath of the data breach, so employers should still take reasonable precautions to mitigate the costs of any potential claims, for example by exploring their options in terms of cyber-insurance cover as well as having well-rehearsed policies in place for dealing with data breach scenarios.

The authors wish to thank Sorcha McKendry for her contribution to this article.

KEY CONTACTS

Séamus Given
Partner, Employment
+353 1 920 1210
seamus.given@arthurcox.com

Emma Dunne
Associate, Employment
+353 1 920 1393
emma.dunne@arthurcox.com

Richard Willis
Partner, Litigation, Dispute Resolution and Investigations
+353 1 920 1154
richard.willis@arthurcox.com

Gavin Woods
Partner, Litigation, Dispute Resolution and Investigations
+353 1 920 1136
gavin.woods@arthurcox.com

Rob Corbet
Partner, Technology
+353 1 920 1211
rob.corbet@arthurcox.com