Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Morrisons Ruling Leaves Door Open For Data Breach Suits

By **Paige Long**

Law360, London (April 2, 2020, 5:56 PM BST) -- Morrisons no longer has to pay up over a rogue worker's theft of thousands of employees' data after the U.K. Supreme Court's landmark decision Wednesday, but the threat of group actions over more straightforward data breaches remains.

Lawyers say the ruling, which was a blow to the thousands of Morrisons employees and former employees that were seeking compensation from the supermarket chain, is far from an all-clear sign for employers.

While Morrisons escaped liability for the actions of a rogue employee who stole and publicized payroll data to harm the company, the ruling also clarified the extent to which a company could be held responsible for an employee who carried out a similar crime while acting in the capacity of his duties at work. And that has piqued a lot of lawyers' interest, as a number of other class actions over data breaches continue to make their way through the courts.

"We are seeing more and more actions brought by large groups of claimants for damages for the distress and anxiety caused by the misuse of personal data, irrespective of any actual financial loss, and this decision will do little to slow that trend," said Hogan Lovells partner Matthew Felwick.

In England and Wales, claimants can bring collective suits using methods like group litigation orders and representative actions, where claimants must "opt-in" or gain court approval to have their claims handled together.

In the Morrisons case, which was one of the first data breach claims in the U.K. to be granted a group litigation order, the Supreme Court was asked to determine two separate issues. The first was whether the Court of Appeal erred in law by concluding Andrew Skelton had carried out the breach during the course of his employment, making the supermarket vicariously responsible.

The second was whether the Data Protection Act 1988 excludes vicarious liability for a breach of that law, or for misuse of private information or breach of confidence.

Morrisons had argued companies should be excluded from vicarious liability under the DPA because companies are not mentioned in the legislation and including them would conflict with other rules.

But the court found that “imposing statutory liability on a data controller is not inconsistent with the co-existence of vicarious liability at common law, whether for breach of the DPA or for a common law or equitable wrong.”

In doing so, the top court has allowed employers to, in principle, still be held vicariously liable for breaches of data protection legislation where their employees are “data controllers” and performing their role when the wrongdoing occurs.

Hogan Lovells' Felwick said the court’s reluctance to totally exclude vicarious liability gives another potential tool to claimant lawyers, “further increasing the already considerable risks of data class actions in the U.K. that companies face.”

Indeed, the U.K. courts have been grappling with several other suits expected to test the strength of the rights afforded to consumers under data protection rules, including claims against Google — over allegations the search provider tracks iPhone users’ internet activity without consent, for commercial purposes — and British Airways, which was granted a group litigation order in October.

And that number is only expected to increase, with EU citizens given more power to bring class actions under the General Data Protection Regulation to claim monetary compensation from a business over a data breach. The regulation has been implemented in Britain through the Data Protection Act 2018.

All that said, the scope of vicarious liability has been decreased compared to earlier decisions in this case, and the top court has now established potential defenses for companies, according to Victoria Hobbs, a partner at Bird & Bird LLP.

Wednesday’s decision set aside the lower courts’ controversial rulings that held Morrisons liable for Skelton’s conduct, even though the supermarket had robust data protection controls in place and was in fact a victim of his actions.

The claimants had argued the criminal act could be traced back to Morrisons, pointing to an “unbroken chain” in which Skelton's authorization to collate the data and transmit it to the grocer’s external auditor KPMG led to his making of a private copy that he later published.

But the Supreme Court disagreed, concluding the acts were not “closely related.”

“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,” the court said in its judgment.

When he handed down the ruling, Justice Robert Reed said the lower courts departed from precedent around vicarious liability when they ruled that Skelton’s motive was irrelevant, and misunderstood the test that should have been applied.

Skelton, a senior auditor for the chain, had borne a grudge since he was subject to disciplinary proceedings in July 2013, according to the judgment. He even tried to frame a fellow employee who had been involved in the proceedings when he posted data from thousands of staff members, the judgment said.

There have been several decisions about employees who deliberately inflicted harm for their own reasons, and in those cases the employer was not held vicariously liable, the justice said, because it could not “fairly and properly” be considered that the employee was acting in the “ordinary course of his employment.”

Lawyers now need to look at the “field of activities” the employer has given a particular worker, and decide whether there is a sufficient connection between the role and the wrongful conduct.

If the employee is acting for purely personal reasons, and not for the employer’s business, then a company can argue there was no connection between the authorized duties and the wrongful conduct.

The Supreme Court’s approach should still lead to a collective rise in standards, lawyers say, as the threat of a vicarious liability suit in other circumstances where there is no personal vendetta will prompt businesses to make sure their systems and processes for securing data are robust.

Most data breaches are caused by human error, according to Nick McAleenan, a partner at JMW Solicitors, which represented the claimants against Morrisons. He said Wednesday’s decision “enhances the protection of data for millions of people in this country who are obliged to hand over their own information to businesses every single day.”

“Morrisons’ staff have lost their claim, but through their legal action they have enhanced the data rights of everyone in the U.K.," McAleenan added.

That is the “dual-edged result” of the Supreme Court judgment, according to Covington & Burling LLP partner Mark Young.

Although a company is off the hook if an employee “goes off the deep end” and carries out an illegal act designed to harm the employer, the ruling reinforced that employers can be held vicariously liable for employees who do something closely connected with what they are authorized to do, Young said. That includes accidents such as sending data to the wrong recipient or uploading data to a public rather than private site.

Even without facing damages in the litigation, Morrisons still faced a probe by the Information Commissioner's Office where the supermarket was ultimately cleared. Morrisons spent more than £2.6 million dealing with the immediate aftermath of the breach, including on protection measures for its employees’ bank accounts, according to the judgment.

“The case is still a reminder for all employers of the importance of robust recruitment and background screening procedures as well as monitoring IT systems and having a 'speak up' workplace culture to facilitate staff raising concerns in a protected manner,” said Pulina Whitaker, partner at Morgan Lewis.

Even after the Supreme Court's decision, several key questions remain, like what kind of damages companies might face if they are found liable — the Morrisons case never got past the initial liability phase of the trial.

“Many employees would have struggled to show they had suffered any actual loss or harm, suggesting their compensation should be minimal,” said Peter Church, counsel at Linklaters LLP. “This is relevant to the other outstanding class actions, but following the dismissal of this claim, we may have to wait longer for the answer.”

Another question is what to make of the emphasis the Court of Appeal had put on the need for companies to take out insurance to protect themselves against the risk of vicarious liability and group litigation, particularly amid the growth of cybercrime. The Supreme Court ruling, on the other hand, did not mention insurance once.

Regardless, companies would be wise to also take into account the ICO's new enforcement powers, which allow it to issue fines for data protection breaches of up to €20 million ($22 million) or 4% of a company's annual global turnover, whichever is higher.

Greig Anderson, a partner at Herbert Smith Freehills LLP, said Wednesday's ruling is "good news" for corporates and their insurers, but only up to a point. He said the main risk for corporates, and therefore insurers, is direct liability claims, which are continuing apace.

"The main challenge therefore remains and is not answered here: How much cover would I need to buy for a reasonable worst case, and is that available at reasonable cost on a good wording?" Anderson said. "Given that the measure of damages is still unclear, this issue will continue to be wrestled with."

--Additional reporting by Najiyya Budaly. Editing by Marygrace Murphy.