LK SHIELDS
YOUR LEGAL COUNSEL

TECHNOLOGY

Employer vicariously liable for the intentional data breaches of a rogue employee

by **Aoife Bradley**

Employer vicariously liable for the intentional data breaches of a rogue employee

25th October 2018 | by Aoife Bradley

Get insurance - the message from the UK Court of Appeal in significant data breach case.

The English Court of Appeal has dismissed an appeal from the supermarket chain Morrisons of a High Court decision holding Morrisons vicariously liable for the actions of a rogue employee - Mr Skelton, who had deliberately posted personal information of 100,000 of his colleagues online.

The case is likely to have significant implications for employers in all sectors. It leaves employers considerably exposed to potential claims arising from the unauthorised disclosure of personal data by rogue employees.

Wm Morrison Supermarkets Plc v Various Claimants [2018] EWCA Civ 2339

The Court of Appeal concluded:

> There have been many instances reported in the media in recent years of data breaches on a massive scale caused by either corporate systems failures or negligence by individuals acting in the course of their employment. These might, depending on the facts, lead to a large number of claims against the relevant company for potentially ruinous amounts.

The solution, according to the court, is to insure against such catastrophes; adding that insurance is “a valid answer to the Doomsday and Armageddon arguments” put forward by Morrisons in the proceedings.

The Court’s emphasis on insurance as a means of limiting exposure to risk for the actions of rogue employees is significant. Employers should review existing policies to check that they have such insurance in place and, from a risk management perspective, review their existing information security policies and processes to ensure that they meet both legal and insurance requirements.

A disgruntled employee

Skelton, employed by Morrisons as a Senior IT Internal Auditor, was the subject of disciplinary action following an incident involving his unauthorised use of the company's postal facilities. He continued to work for Morrisons, but reportedly harboured a grudge as a result of the disciplinary action. In November 2013, Skelton was tasked with transferring payroll data to Morrisons’ external auditor. He copied this data onto a personal USB and posted the personal information of almost 100,000 employees of Morrisons on a file sharing website. Within a few hours of their discovery of this alarming turn of events, Morrisons took steps to ensure that the personal information was taken down, and alerted the police.

Skelton was arrested and charged with fraud under the UK Computer Misuse Act 1990 and under section 55 of the English Data Protection Act 1998 (DPA). He was sentenced to eight years imprisonment.

Group claim in the High Court

A group civil claim was brought against Morrisons by 5,518 employees of Morrisons, for misuse of private information, breach of confidence and breach of statutory duty owed under section 4(4) of the DPA, particularly non-compliance with Data Protection Principles 1, 2, 3, 5 and 7.

The High Court ruled that Morrisons had no primary liability for Skelton's actions, it was not the data controller at the time of any breach of the Data Protection Principles, and owed no duty to the claimants under the DPA unless it was the duty to comply with the seventh principle. Data Protection Principle 7 requires that a data controller implement appropriate organisational measures which ensure a level of security appropriate to the nature of the data and the harm that might result from a breach. The High Court held that Morrisons had not taken appropriate technical and organisational measures to the extent that it had not taken steps to ensure deletion of the payroll data after it had been transferred to the external auditors.

Nonetheless, it was held that this failure "neither caused nor contributed to the disclosure which occurred." In terms of vicarious liability, the Court rejected the argument that it was excluded under the DPA.

Court of Appeal

Morrisons' appeal was heard before the English Court of Appeal on 9 and 10 October 2018. Morrisons argued that the act which caused the harm was not carried out in the course of Mr Skelton's employment, and so Morrisons could not be held vicariously liable for his actions. The reasoning for this was that, while Mr Skelton had obtained the data at work, the actual disclosure of the personal information was done "by Mr Skelton at his home, using his own computer, on a Sunday, several weeks after he had downloaded the data at work onto his personal USB stick." The Court of Appeal disagreed and found that Mr Skelton's actions were "within the field of activities assigned to him by Morrisons." It agreed with the High Court's determination of those actions as "a seamless and continuous sequence of events".

The Court noted that the "novel feature" of this case is that Skelton's motivation in acting as he did was to "harm his employer rather than to achieve some benefit for himself or to inflict injury on a third party."

It was submitted on behalf of Morrisons that a finding of vicarious liability could place an enormous burden on "innocent employers" in future cases given the potential for huge numbers of data subjects to be affected. The Court acknowledged the "potentially ruinous" impact that such data breaches may have on employers. It took the view that companies should "insure against such catastrophes" and against "losses caused by dishonest or malicious employees."

What next?

This case is one of the first data privacy disputes to be heard by the English courts using a collective action mechanism. It is also the second major UK decision on data privacy this month, alongside Lloyd v Google LLC. The DPA in the UK has been replaced with GDPR legislation, as has been the case in Ireland. In fact, in the post-GDPR world, such cases are likely to be more common with potentially even more serious consequences . This is a high profile case that has received much coverage in the media. It is likely to prompt organisations to ensure they have the appropriate insurance, processes and policies in place regarding similar data breaches.

Morrisons expressed disappointment with the ruling, highlighting the fact that the company had "not been blamed by the courts for the way it protected colleagues' data" and that it "worked to get the data taken down quickly, provide protection for those colleagues and reassure them that they would not be financially disadvantaged." Morrisons reacted strongly immediately after the decision was handed down, stating its belief that it "should not be held responsible" and accordingly has confirmed that it will appeal the decision to the Supreme Court.

About the Authors

Aoife Bradley
Partner

Aoife is Head of Employment, Pensions and Employee Benefits.
T: + 353 1 637 1583 **E:** abradley@lkshields.ie