

Vicarious Liability – The Gap is Closing Absent Data Breaches by Employer

Related Lawyers:

Related Practice Areas: **Commercial Disputes**

The Court of Appeal, in *WM Morrison Supermarkets Plc v. Various Claimants*, has upheld a ruling by the High Court that allowed a compensation claim by thousands of current and former employees at supermarket chain, Morrisons. The Court of Appeal held that Morrisons should be found vicariously liable for the actions of a former disgruntled employee who stole employees' personal data, before posting that confidential data online.

Background

The case follows a security breach in 2014 when Mr Skelton, then a senior internal auditor at Morrisons' Bradford headquarters, leaked payroll data after copying it to his personal USB.

In response to a claim by 5,518 Morrisons employees, Langstaff J concluded at first instance that Morrisons was vicariously liable for the actions of the ex-employee, despite not being directly liable in respect of any data breach. The Judge dismissed claims against Morrisons for primary liability, in equity, for breach of confidence and, at common law, for misuse of personal information. Langstaff J found that Morrisons did not know, and that it ought not reasonably to have known, that Skelton posed a threat to the employee database. The supermarket had applied all required control mechanisms in respect of the disgruntled employee. The trial was only concerned with the supermarket's liability, with the compensation to be awarded for the breach to be assessed later.

By upholding the lower court's decision, the Court of Appeal paves the way for future compensation claims by employees who have been victims of a data breach within their company even though their employer is not primarily liable for the breach.

The judgement

The judgement handed down on 22 October 2018 contains a useful summary of the leading authorities and principles at common law to establish vicarious liability.

In terms of the required 'sufficient connection' between the function entrusted by the employer and the employee's wrongful act, the Court endorsed the broad test in *Mohamud* that the employee's tortious act must be 'within the field of activities' assigned to the employee by the employer. The fact that an employee 'grossly abuses its position' is irrelevant in establishing vicarious liability. The disclosure of the employees' payroll data to third parties was clearly within the field of activities assigned to Skelton.

The Court agreed that, in principle, the time and place at which the wrongful acts occur will be relevant but not decisive in proving vicarious liability. The Court plainly refuted the idea that an employee should be 'on the job' when the wrongful act is committed. Of more significant importance was the clear evidence that the leaking of the data was closely connected to Skelton's employment, and the two were linked by a 'seamless and uninterrupted' sequence of events.

The case raises a number of interesting issues on vicarious liability.

By way of example, *Morrisons'* counsel attempted to argue that the motive of Skelton was to harm his employer rather than inflict harm on third-party employees such that imposing vicarious liability on *Morrisons* would render the court, in the circumstances, an accessory in furthering Skelton's criminal aims. The Court of Appeal, like the first instance judge, was not convinced by this point.

Some might find it surprising that employers could be liable for the criminal or malicious acts of a disgruntled employee. However, the three appeal judges made it clear that the employee's motive was irrelevant, including where the motive is, by causing harm to third parties, to deliberately cause financial and reputational damage to the employer.

The fact that an employer can be vicariously liable for an act which involved a criminal offence was established long ago. The solution to this 'moral' point is probably, as suggested by the Court, for employers to reduce their exposure by insuring against losses caused by malicious employees, and in the context of data protection, putting in place measures to monitor staff handling personal data more closely.

Potential compensation for data breach

Morrisons has announced that it will appeal to the Supreme Court. If this appeal fails, employees affected by the data breach will be able to claim compensation, and legal proceedings will take place to determine the nature of their loss and quantum.

There are 5,518 employees who are claimants in the present case, but the total number of employees whose confidential information was leaked is estimated at almost 100,000, so the compensation claim will be significant.