COURT OF APPEAL CONFIRMS MORRISONS VICARIOUSLY LIABLE FOR EMPLOYEE'S DELIBERATE ACTIONS IN FIRST SUCCESSFUL UK CLASS ACTION FOR DATA BREACH

23 October 2018 | London
Legal Briefings – By **Miriam Everett, Julian Copeman, Christine Young, Andrew Moir, Greig Anderson and Lucy McAlister**

The Court of Appeal has today dismissed an appeal against the High Court's decision that Morrisons was vicariously liable for its employee's misuse of data, despite: (i) Morrisons having done as much as it reasonably could to prevent the misuse; and (ii) the employee's intention being to cause reputational or financial damage to Morrisons itself: *Wm Morrisons Supermarkets Plc v Various Claimants [2018] EWCA Civ 2339* (click here for the Court of Appeal's full judgement and click here for our summary of the High Court decision).

SUMMARY IMPLICATIONS FOR BUSINESSES

This case highlights the wide reach of data protection. An organisation can be liable for data breaches even if it has taken appropriate measures to comply with the data protection legislation itself, and even if it is the intended victim of the breach. In this respect, the decision will also concern employers who can now be vicariously liable for the actions taken by a rogue employee even with appropriate safeguards in place to protect employee personal data. In addition to civil liability, organisations may suffer further damage as a result of negative publicity and impact on share price.

The fear for organisations will now be that this decision, combined with the legislative changes made by the EU General Data Protection Legislation ("**GDPR**"), increased public awareness of data protection issues, and the publicity that the case has attracted, could spark a new wave of court cases from workers and customers in the event of a data breach. Whilst individuals may not themselves be entitled to significant sums, if the data breach affects large numbers of individuals, the total potential liability for organisations could become commensurately large. In this regard, it will be interesting to see how the court approaches the issue of quantum in the case against Morrisons.

The Court of Appeal suggested that insurance could be the answer to "Doomsday or Armageddon arguments" about the effect of its decision. Cyber insurance typically covers claims for breaches of confidential information; and in some circumstances coverage may also be found in other classes of liability insurance. However, at this stage the UK cyber insurance market remains in its infancy and claims experience is limited. It therefore remains to be seen how the market will react to this enhanced exposure and whether insurance will be an effective tool to offset the increased risks that organisations now face.

Importantly, this case related to data breaches which occurred prior to 25 May 2018 (i.e. prior to the implementation of the GDPR). In the post-GDPR world where there is an express right for individuals to be compensated for non-material damage (i.e. distress) it could become even easier to bring such actions, particularly where there have been findings of non-compliance by the Information Comissioner's Office ("**ICO**") (the UK's data protection regulator). With multiple data breaches having hit the headlines since 25 May 2018 (including the Conservative Party Conference, Butlin's, British Airways, Dixons Carphone, Facebook and Google+), it will be interesting to see the impact of this decision on future individual compensation claims and whether or not this case opens the floodgates for data breach class action claims in the UK.

BACKGROUND

In July 2015, Andrew Skelton (a former Morrisons' employee) was sentenced to eight years in jail after he was found guilty of stealing and unlawfully sharing the names, addresses, bank account, salary and national insurance details of almost 100,000 of his former colleagues with news outlets and data sharing websites. Mr Skelton had copied the data as part of his job and then used his personal computer to publish it online outside working hours.

According to reports, the ICO investigated the incident at the time and decided no action was required with respect to compliance with the Data Protection Act 1998 ("**DPA**") (the data protection legislation in force in the UK at the time).

However, subsequently around 5,500 employees brought a claim for damages against Morrisons in the courts, despite not having suffered any financial loss. The claim was brought on the basis that Morrisons was liable, directly or vicariously for:

(i) the criminal action of its rogue employee in disclosing personal information of co-employees; and

(ii) the subsequent distress suffered by those employees;

whether in breach of certain data protection principles under the DPA, an action for breach of confidence, or an action for misuse of private information.

HIGH COURT DECISION

In a decision handed down in the High Court on 1 December 2017, Morrisons was cleared of direct liability as it had not breached any of the data protection principles (except in one respect which was not causative of any loss), nor could direct liability be established for misuse of private information or breach of confidentiality. This is because, once Mr Skelton acted autonomously in deciding how to handle the personal data, he became the data controller in respect of the relevant processing. Therefore, the acts that breached the DPA were those of a third party data controller (Mr Skelton), not Morrisons.

However, it was held that the DPA does not exclude vicarious liability, despite not expressly referring to it. As Mr Skelton's disclosure of the data was deemed to be a seamless and continuing series of events, it was held that Mr Skelton acted in the course of his employment and Morrisons was therefore vicariously liable for Mr Skelton's actions. The judgment also stated that this conclusion would be the same regardless of whether the basis of Skelton's liability was seen as a breach of duty under the DPA, a misuse of private information or a breach of confidence.

In giving the judgment, Mr Justice Langstaff stated his concerns that, since the wrongful acts of Skelton were deliberately aimed at Morrisons, by finding Morrisons vicariously liable, the court could be regarded as "an accessory to furthering his criminal aims". As a result, he granted leave to Morrisons to appeal the conclusion on vicarious liability.

COURT OF APPEAL DECISION

On 22 October 2018, the Court of Appeal (the Master of the Rolls, Lord Justice Bean and Lord Justice Flaux) unanimously dismissed the appeal.

There were three grounds of appeal:

(i) The judge ought to have concluded that, on its proper interpretation and having regard to the nature and purposes of the statutory scheme, the DPA excludes the application of vicarious liability.

(ii) The judge ought to have concluded that, on its proper interpretation, the DPA excludes the application of causes of action for misuse of private information and breach of confidence and/or the imposition of vicarious liability for breaches of the same.

(iii) The judge was wrong to conclude that the wrongful acts of Mr Skelton occurred during the course of his employment by Morrisons and, accordingly, that Morrisons was vicariously liable for those wrongful acts.

There was no challenge to the judge's finding that Mr Skelton, and not Morrisons, was the data controller in respect of the relevant processing. Nor was there any appeal against the court's conclusion that Morrisons was not directly liable for the breach of data protection legislation.

First and second grounds of appeal

The court took the first and second grounds together, describing the first as a "stepping stone" to the second.

Morrisons submitted that there were highly significant inconsistencies between the liabilities of employers under the DPA, which are qualified by concepts of appropriateness and reasonableness, and the strict liability imposed at common law by way of vicarious liability for the defaults of employees and others. It contended that the terms of the DPA expressly or impliedly excluded the imposition of vicarious liability under the common law for breach of the statutory duty of an employee data controller to comply with the DPA.

The Court of Appeal rejected these submissions. It said it was clear that, whatever the position on vicarious liability for breach of the DPA (the first ground of appeal), vicarious liability for misuse of private information and breach of confidence had not been excluded by the DPA (the second ground of appeal).

The question was whether the DPA excluded such vicarious liability by necessary implication. If the statutory code covered precisely the same ground as vicarious liability at common law, and the two were inconsistent with each other in substantial respects, then the common law remedy would almost certainly have been excluded by necessary implication. Here, however, there were three major obstacles to Morrisons' proposition that the DPA had excluded such vicarious liability by necessary implication:

(i) If Parliament had intended such a substantial eradication of common law and equitable rights, it might have been expected to say so expressly.

(ii) Morrisons had accepted that the DPA did not impliedly exclude the entire tort of misuse of private information and the cause of action for breach of confidence in relation to the processing of personal data within the ambit of the DPA. It was only vicarious liability for those causes of action that was alleged to be excluded. That was, on its face, a difficult line to tread.

(iii) Rather than being inconsistent with the common law, the DPA simply had nothing to say about the liability of an employer who is not a data controller for wrongful data processing by an employee who is a data controller. That was quite different from the situation in the cases relied on by Morrisons, where the legislation expressly addressed the circumstances which it was alleged gave rise to a common law remedy but there were substantial differences between them.

Further, on the issue of inconsistency, the contrast between the fault based primary liability on an employer data controller under the DPA and the imposition of strict vicarious liability on an employer for the defaults of an employee data controller was no more of an anomaly than the position at common law. The common law imposes strict liability on an employer who is guilty of no fault, where there is a sufficient connection between the employee's default and the running of the employer's business.

Third ground of appeal

The tests for vicarious liability are set out in the most recent Supreme Court decision on this issue, *Mohamud v Wm Morrison Supermarkets plc* [2016] AC 667. The court has to consider two matters: first, what functions or "field of activities" have been entrusted by the employer to the employee, a question which must be addressed broadly; secondly, was there sufficient connection between the position in which he was employed and his wrongful conduct to make it right for the employer to be held liable.

The first question was answered by the judge in terms which the Court of Appeal regarded as plainly correct, namely that Morrisons entrusted Skelton with dealing with the payroll data.

In relation to the second question, Morrisons submitted that the close connection test was not satisfied since the tortious act which caused the harm was done by Mr Skelton at his home, using his own computer, on a Sunday several weeks after he had downloaded the data. The Court of Appeal rejected that submission. Although the time and place at which the relevant acts occurred will always be relevant (though not conclusive), there are numerous cases in which employers have been held vicariously liable for torts committed away from the workplace. Mr Skelton's tortious acts in sending the claimants' data to third parties were, in the Court of Appeal's view, within the field of activities assigned to him by Morrisons. It entirely agreed with the judge's evaluation of those acts as constituting a "seamless and continuous sequence" or "unbroken chain" of events.

The court noted that there is one novel feature to this case, in that the employee's motive was to harm his employer rather than to achieve some benefit for himself or inflict injury on a third party. Morrisons submitted (reflecting the judge's own concern as expressed in his judgment) that to impose vicarious liability on Morrisons in these circumstances would render the court an accessory in furthering Mr Skelton's criminal aims.

The Court of Appeal rejected this submission, noting that it is clearly established that an employer may be vicariously liable for deliberate wrongdoing by an employee. The Supreme Court stated in *Mohamud* that motive was irrelevant. The Court of Appeal did not accept that there is an exception where the motive is to cause financial or reputational damage to the employer.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

MIRIAM EVERETT
PARTNER, LONDON

+44 20 7466 2378
Miriam.Everett@hsf.com

JULIAN COPEMAN
PARTNER, LONDON, NON-RESIDENT PARTNER, HONG KONG, LONDON
+44 20 7466 2168
Julian.Copeman@hsf.com

CHRISTINE YOUNG
PARTNER, LONDON

+44 20 7466 2845
Christine.Young@hsf.com

ANDREW MOIR
PARTNER, INTELLECTUAL PROPERTY AND GLOBAL HEAD OF CYBER & DATA SECURITY, LONDON
+44 20 7466 2773
Andrew.Moir@hsf.com

GREIG ANDERSON
PARTNER, LONDON

+44 20 7466 2229

Greig.Anderson@hsf.com

LEGAL NOTICE