MORRISON: IT MAY NOT BE OVER YET*.*
VICARIOUS LIABILITY EXPLAINED BY THE SUPREME COURT
(LIABILITY OF JOINT CONTROLLERS UNAFFECTED)

WM Morrison Supermarkets plc (appellant) v Various Claimants (respondents) [2020] UKSC 12

1. In *Morrison* the Supreme Court was at pains to re-state and explain a previous judgment on an employer's vicarious liability for employees that had been misinterpreted and misapplied both at trial and in the Court of Appeal. What was not examined at any level was the primary liability of joint data controllers, as regulated by the General Data Protection Regulation. This article looks at what the Supreme Court said about vicarious liability and the position of joint controllers.

Common Law Vicarious Liability

2. Lord Reed (for the court) took to task those courts that had misunderstood Lord Toulson's characterisation, in *Mohamud v WM Morrison Supermarkets* [2016] UKSC 11, of the connection between the employee's conduct and his employment as "an unbroken sequence of events" or "a seamless episode" together with the statement that the employee's motives were irrelevant.

3. Lord Reed described their mistake: "[A] few phrases … were treated as establishing legal principles: principles which would represent a departure from the precedents which Lord Toulson was expressly following."

4. The facts were simple. Skelton was a senior auditor in Morrisons' internal audit team. After disciplinary proceedings for minor misconduct, he harboured an "irrational grudge" against his employer. He was thereafter instructed to collate

and transmit payroll data to Morrisons' external auditors. He did so but later, and while seeking to conceal his actions, posted this data to a file-sharing website and sent CDs containing the file to three UK newspapers. The trial judge found that Morrisons had provided him with the data and what happened thereafter was part of a "seamless and continuous sequence of events… an unbroken chain" and its disclosure to outside parties, while not authorised, was "closely related" to what he had been instructed to do. It was in formulating the problem and answer thus, that the Supreme Court held the courts below to have misconceived Lord Toulson's judgment in *Mohamud*.

5. Lord Reed therefore started with an analysis of what Lord Toulson's judgment in *Mohamud* really meant. First, it "was not intended to effect a change in the law of vicarious liability." The court, in *Mohamud*, had rejected an invitation to broaden the test, holding that the established test needed no further refinement. This had developed beyond a wrongful act authorised by the employer to, early this century, unauthorised acts so closely connected to what had been authorised "that they may properly be regarded as being within the scope of his employment". This is what Lord Nicholls of Birkenhead had identified in the *Dubai Aluminium* case[1] as "the general principle", and this remained the correct approach.

6. Lord Toulson, Lord Reed said in this case, then summarised the present law. There were two matters to be considered: (1) what function had been entrusted to the errant employee (the question of authority); and (2) was there sufficient connection between this and the employee's wrongful conduct to render the employer liable. However, Lord Toulson had not suggested any departure from recent cases. The issue was not limited to timing or causation and was not a matter for individual judges' sense of social justice. There had also been a misunderstanding that Lord Toulson had found that motive was irrelevant: the context of that finding was that Lord Toulson had already found that the employee in the 2016 case was going about his employer's business. Only in that sense was motive ever irrelevant.

[1] [2002] UKHL 48.

7. Returning to the position of Skelton in this case, Lord Reed found that the only connecting factor between what Skelton was authorised to do and his disclosure of personal data was that he could not have made the disclosure had he not been given the task of collating the data and sending it to the external auditors. But opportunity was not sufficient because, as held in earlier cases, the employee "may so clearly depart from the scope of his employment" that the employer will not be vicariously liable. This leads back to a far earlier limitation on the principle of vicarious liability: when the employer is engaged in "a frolic of his own" the employer is not liable; or, as Lord Nicholls put it in *Dubai Aluminium*, "where the employee is engaged only in furthering his own interests". Here, of course, Skelton was not engaged in Morrisons' interests in making the disclosures – he was simply wreaking his own revenge on Morrisons.

8. This must be correct. If the test were not so limited, then any employee would maliciously be able to create huge liabilities for employers – perhaps to the point of bankruptcy of even very large companies – as acts of revenge for slights, such as the relatively minor disciplinary proceedings that had so incensed Skelton in this matter.

GDPR Joint Controllers

9. The final issue was whether the Data Protection Act, 1998 (now replaced by the Data Protection Act, 2018) excluded vicarious liability not only for breaches of its own provisions committed by an employee as data controller, but also for misuse of public information and for breach of confidence. This was a simple question of statutory interpretation and, although not necessary because of its earlier finding that Morrisons was not liable, the Supreme Court held that the Data Protection Act was silent on the position of a data controller's (such as Skelton's) employer. Vicarious liability was therefore neither expressly nor impliedly excluded by the statute.

10. What then is the remedy for the aggrieved data subject who is wrongfully and materially harmed by an unauthorised disclosure in a *Morrison*-type scenario. The judgment does not provide an answer.

11. It may be a significant fact that Skelton was independently registered as a data controller, even though he was employed by Morrisons to process the data of its employees. Certainly this might start a pattern to require individual employees - including perhaps data protection officers - to register as data controllers. However, employers might think again taking into account the analysis that follows.

12. We know so far that following *Morrison*, and similar to it, liability is borne by the errant employee who is a data controller in his own right - and receives that data from another controller and with the informed consent of the data subject. Also following *Morrison*, within the rules of vicarious liability at common law, liability would not pass to the employer of an errant employee who is not a registered controller in his own right, but has access to personal data within the course of his employment, if the unauthorised disclosure was an irrational act of revenge on the employer. In either case, the level of supervision and control over the data must be adequate. This leaves employees who are not properly trained and who do not carry out an irrational act that makes the employer liable in the conditions set by *Mohamud*.

13. However vicarious liability is not excluded from the DPA. The Supreme Court observes that it is silent, which is true in the case of the 1998 Act, but this different in the case of the GDPR which specially deals with joint controllers and joint liability, but not in all circumstances.

14. In the DPA, "data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed (S.1(1))

15. That definition is retained in in the GDPR, but it does not end there. A more practicable approach is taken, per Art. 26: Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. It directs joint controllers to act in a transparent manner in determining their *respective* responsibilities. The article recognises that this transparency is required most of all "as regards the exercising of the rights of the data subject and their *respective* duties".

16. However, notwithstanding a discretion to determine their respective responsibilities, "*the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers*."

17. Now, in *Morrison* it was common case that Morrison had discharged its duties as a data controller, and from then on it was only a question of vicarious liability within an employment context. There was some discussion at first instance about joint tortfeasors but only to test the premise of vicarious liability.

18. Simply put there has been no discussion concerning the liability of joint controllers by virtue of the GDPR, and specifically the right to an effective judicial remedy (Art. 79) where rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation, including compensation for material or non-material damage. Note, the counterpart to Art. 26 (joint and several responsibility of joint controllers) is that any controller involved in processing shall be liable for the damage caused by processing that infringes the Regulations (Art. 82) and where there are more than one controller responsible for any damage caused by processing, each controller is liable for the entire damage

19. That scope of liability is trimmed by the proportionately principle, which is written into Art. 82: A controller that is not in any way responsible for the event giving rise to the damage is exempt from liability. Thus, whether as controller or employer, it is not one of strict vicarious liability.

20. It is possible therefore that the same result would transpire in a *Morrison*-type scenario under the GDPR as it did under the common law if Morrisons is not held to be responsible for the event giving rise to the damage. Some examination is therefore required of the irrational act of disclosure by a rogue employee, or does some responsibility fall on the employer for not keeping the data more securely at all times so as to prevent its download on to a USB memory stick. The burden appears to be on the employer to prove that it was not responsible.

John Campbell SC

Joseph Dalby SC

36 Commercial

https://36group.co.uk/commercial