ALERT MEMORANDUM

Relief for Employers as Supreme Court Rules no Liability for Morrisons in Data Breach Case

April 16, 2020

The UK Supreme Court, in a unanimous decision delivered on April 1,[1] has overturned the decision of the Court of Appeal which had found that Morrisons Supermarkets plc ("Morrisons") could be held vicariously liable for the unauthorised actions of an employee who had deliberately leaked the personal data of thousands of Morrisons' employees online. In its judgment, the Supreme Court explained that the Court of Appeal had "*misunderstood the principles governing vicarious liability*".[2] The full text of the judgment can be read here.

As the threat of class action lawsuits for personal data breaches increases, the Supreme Court's ruling should be welcomed by employers. The EU General Data Protection Regulation sets a low bar for data subject compensation, with "non-material" damage being sufficient to warrant a pay-out. Data subjects do not need to demonstrate actual financial loss and may be able to claim compensation for distress associated with an unauthorised disclosure of their personal data. The Supreme Court judgement, therefore, brings welcomed clarity on the extent to which an employer could be on the hook for the actions of a rogue employee.

I. Background and breach in the Morrisons case:

In November 2013, in preparation for an internal audit, Andrew Skelton (a former senior auditor employed by Morrisons, "Skelton") was provided access to employee payroll data and was put in charge of collating and

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

PARIS

Emmanuel Ronco
+331 4074 6906
eronco@cgsh.com

LONDON

Natalie Farmer
+4420 2309 7614
nfarmer@cgsh.com

[1] *WM Morrisons Supermarkets PLC (Appellant) v Various Claimants (Respondents)* [2020] UKSC 12, see paragraphs 2 – 8.
[2] *Ibid.*, paragraph 31.

transmitting the relevant data to Morrisons' external auditors, KPMG. Following transmission of the data to KPMG, as instructed, Skelton made a copy of the data from his work laptop to a personal USB stick. In January 2014 Skelton released the harvested personal data relating to 98,998 Morrisons employees to a publically accessible file sharing website. The data packet contained details of employees' national insurance numbers, bank account information and contact details.

Skelton's actions followed internal disciplinary proceedings against him, which the Supreme Court's judgment characterised as having caused Skelton's "*irrational grudge against Morrisons, which led him to make the disclosures in question*".[3]

II. High Court and Court of Appeal cases:

In 2017, an action brought by a group of approximately 5,500 affected Morrisons employees was heard by the High Court.[4] The claimants argued that Morrisons had both primary and vicarious liability to compensate the employees for the breach of its statutory duty under section 4(4) Data Protection Act 1998 ("DPA"), breach of confidence and misuse of private information.

The High Court found that Morrisons "*did not directly misuse any information personal to the data subjects. Nor did they authorise its misuse, nor permit it by any carelessness on their part. If Morrisons are liable it must be vicariously or not at all*."[5] However, the High Court did determine that a sufficient connection existed between Skelton's actions and the course of his employment for vicarious liability to arise. In particular, the High Court found that Skelton's actions were part of an "*unbroken chain*" of events which began when he was granted access to the data by Morrisons in the course of his duties.[6]

The High Court did, however, clearly state its discomfort in making its judgment in light of the fact that the wrongful acts of Skelton were deliberately aimed at Morrisons, such that the High Court's conclusion "*may seem to render the court an accessory in furthering [Skelton's] criminal aims*".[7] As part of the judgment, the High Court granted leave for the decision to be appealed.

Morrisons appealed the High Court's decision in 2018 on three grounds: (1) that the DPA excludes vicarious liability, (2) that the DPA excludes causes of action for misuse of private information and breach of confidence, and (3) Skelton's actions in any event occurred outside of the course of his employment, precluding the vicarious liability of Morrisons. The Court of Appeal considered (1) and (2) together, ultimately finding that the DPA did not exclude either vicarious liability or actions for misuse of private information or breach of confidence. Morrisons' arguments had focused on the idea that the DPA was intended to provide a comprehensive data protection framework, to the exclusion of other causes of action related to the wrongful use of personal data and that where statute was inconsistent with common law, common law should not be applied (as would have been Parliament's intention). The Court of Appeal however found three "*major obstacles*"[8] to Morrisons' proposition:

- First, the Court of Appeal found that if Parliament had intended such an eradication of common law and equitable rights, it would have done so expressly.
- Second, in oral submissions Morrisons had conceded that the DPA did not impliedly exclude primary liability for misuse of private information and breach of confidence, arguing instead that only vicarious liability was excluded. The acceptance by Morrisons that the causes of action at common law and in equity operate in parallel

[3] *Ibid.*, paragraph 3.
[4] *Various Claimants v WM Morrisons Supermarket PLC* [2017] EWHC 3113 (QB)
[5] *Ibid*., paragraph 123.
[6] *Ibid.*, see paragraphs 183 – 186.
[7] *Ibid.*, paragraph 198.
[8] *WM Morrison Supermarkets PLC v Various Claimants* [2018] EWCA Civ 2339, paragraph 50.

with the DPA in respect of primary liability, while at the same time contending that vicarious liability for the same causes of action are excluded, was according to the Court of Appeal "*a difficult line to tread*", not least due to the "*inconsistency in the application of one of the principal objects of the Directive and of the DPA, namely the protection of privacy and the provision of an effective remedy for its infringement (including by an employee of limited means), rather than their curtailment*."[9]

— Third, the Court of Appeal found that the DPA was silent on the liability of an employer who was not a data controller for breaches of the DPA by an employee that is the data controller. There was no inconsistency with the common law because the DPA was simply silent. This is unlike the examples on which Morrisons relied (where statute allegedly provided for a common law remedy, in manner inconsistent with the common law practice).

With respect to Morrisons' third ground of appeal, the Court of Appeal also affirmed the High Court's judgment that Morrisons was vicariously liable for the actions of its employee, noting that the High Court's characterization of Skelton's actions as a "seamless and continuous sequence" or "unbroken chain" of events commencing with his employment duties, "*is one with which we entirely agree*".[10]

III. UKSC judgment:

The Supreme Court's decision delivered on April 1, 2020 again considered the question of whether Morrisons could be held vicariously liable for Skelton's conduct. The Supreme Court found that the lower courts had misunderstood the principles governing vicarious liability in four key respects:

1. Skelton's public disclosure of the personal data of Morrisons' employees on the internet was neither part of the function of Skelton's employment, nor was it within his field of activities;
2. The fact that the five factors for vicarious liability established in *Various Claimants v Catholic Child Welfare Society*[11] were present, was not decisive. The factors were designed to be applicable to the scenario of establishing vicarious liability between parties where the wrongdoer and the defendant had a bond that was *akin* to an employment relationship, rather than an actual relationship of employment as between Morrisons and Skelton;
3. Although there exists a close temporal link and an unbroken chain of causation between the provision of the data to Skelton for the purpose of transmitting it to KPMG and his subsequent disclosure of the data online, a temporal link or causal connection does not alone satisfy the required "close connection" test required to establish vicarious liability; and
4. Skelton's motivations should not be considered irrelevant. Whether Skelton "*was acting on his employer's business or for purely personal reasons*" should be considered highly material.[12]

The question of Morrisons' vicariously liable for Skelton's wrongdoing was therefore considered "afresh" by the Supreme Court, applying the test laid down by Lord Nicholls in para 23 of *Dubai Aluminium*[13]: was Skelton's disclosure of the data so closely connected with acts he was authorized to do that, for the purposes of the liability of his employer to third parties, his wrongful disclosure may fairly and properly be regarded as done by him while acting in the ordinary course of his employment?[14]

The only connection between Skelton's authorized actions and his decision to disclose the data online was that he had been tasked with collating the data and transmitting it to KPMG. The Supreme Court,

[9] *Ibid.*, paragraph 56.
[10] *Ibid.*, paragraph 74.
[11] *Various Claimants v Catholic Child Welfare Society* [2013] 2 AC 1, paragraph 35.
[12] *WM Morrison Supermarkets plc (Appellant) v Various Claimants (Respondents)* [2020] UKSC 12, paragraph 31.
[13] *Dubai Aluminium Co Ltd v Salaam* [2002] UKHL 48, paragraph 23.
[14] *WM Morrison Supermarkets plc (Appellant) v Various Claimants (Respondents)* [2020] UKSC 12, paragraph 32.

however, found that the "*mere fact that Skelton's employment gave him the opportunity to commit the wrongful act would not be sufficient to warrant the imposition of vicarious liability*".[15] In applying the "close connection" test and taking into account previous case law, the Supreme Court distinguished the actions of an employee (whether or not misguided) in furtherance of his employer's business, and actions of an employee which are solely motivated by the furtherance of the employee's own interests. The Supreme Court found that in the present case:

> "*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. In those circumstances, applying the test laid down by Lord Nicholls in Dubai Aluminium in the light of the circumstances of the case and the relevant precedents, Skelton's wrongful conduct was not so closely connected with acts which he was authorised to do that, for the purposes of Morrisons' liability to third parties, it can fairly and properly be regarded as done by him while acting in the ordinary course of his employment.*"[16]

Having established that the conditions for vicarious liability did not exist in the present case, it was not necessary for the Supreme Court to consider whether the DPA excludes such liability. However, as the relevant points had been fully argued, the Supreme Court considered it desirable to express a view. On this question, the Supreme Court agreed with the High Court and Court of Appeal, finding that the DPA did not exclude the possibility of common law vicarious liability being established against an employer who had otherwise complied with its data security obligations under the DPA.

It was argued by Morrisons that: (i) Morrisons performed the obligations incumbent upon it as a data controller; (ii) Skelton was a data controller in his own right in relation to the data disclosed; (iii) the DPA was clear that liability should only be imposed on data controllers where such data controllers had failed to act with reasonable care; and (iv) therefore, the statutory scheme under the DPA could not be reconciled with the imposition of strict liability on Morrisons, the employer of a data controller, for its employee's breach of the DPA or its own breach of duties arising at common law or in equity. However, the Supreme Court found such argument to be unpersuasive noting that: (a) since the DPA is silent on the position of a data controller's employer, there can be no inconsistency; and (b) that this position is not affected by the fact that the DPA is a fault-based liability regime (imposing liability on the data controller, including for the action of an employee, for failing to take reasonable care) whereas vicarious liability is not based on fault.

IV. Takeaways for employers:

As the threat of class action lawsuits for personal data breaches increases, the Supreme Court's ruling should be welcomed by employers. The EU General Data Protection Regulation ("GDPR") sets a low bar for data subject compensation, with "non-material" damage being sufficient to warrant a pay-out.[17] Data subjects do not need to demonstrate actual financial loss and may be able to claim compensation for distress associated with an unauthorized disclosure of their personal data.

The Supreme Court judgement, therefore, brings welcomed clarity on the extent to which an employer could be on the hook for the actions of a rogue employee. Helpfully, the Supreme Court determined that:

— An employer will not be liable for the actions of an employee in deliberately causing a data breach while acting beyond the ordinary scope of their employment, provided the employer can demonstrate the necessary standard of care

[15] *Ibid.*, paragraphs 34 and 35.
[16] *Ibid.*, paragraph 47.
[17] Article 82(1), GDPR.

imposed by data protection law has been met, thus avoiding any primary liability.

— When assessing what is within the ordinary scope of employment, more than a temporal or causal link between the authorized acts of the employee and the wrongful disclosure of personal data, will be needed. It is not enough that the employee has the opportunity to cause a breach during the course of his employment.

— Motivations of an employee will be a relevant part of the assessment. Where an employee is not motivated to further his employer's business, but instead is driven by a personal vendetta, this will be taken into account.

However, the Supreme Court's judgment is not all good news for employers. The UK's highest judicial authority did not exclude the possibility of vicarious liability for data breaches altogether. Therefore, in principle, an employer could be vicariously liable to compensate data subjects for the actions of an employee which, for example, amount to a breach of the GDPR, a breach of confidence or a misuse of private information, where such actions are *within* the ordinary scope of his employment.

However, whether an employer can ever be vicariously liable for a breach of the GDPR by virtue of its employee's actions which take place *within* the scope of its employment is debatable. While not specifically considered by the Supreme Court, it is generally understood that where an employee is processing personal data in the context of their employment, their processing activities are considered to be those of their employer (i.e., the data controller). An employer would not therefore be vicariously liable for such employee's actions, but instead would be directly liable under the GDPR as the controller of such processing. This is distinct from the situation where the employee acts *outside* of the scope of their employment, in which case they would be deemed to be an independent data controller and at the same time vicarious liability would be precluded.

While vicarious liability at common law or in equity may still arise, the distinction with the position under statutory data protection law has important implications for potential damages claims (in light of the very low threshold for compensation set by the GDPR). Primarily therefore, employers should take all steps necessary to avoid a breach of the GDPR as a result of its employees' actions within the course of employment.

Going forward, it will be crucial for employers to:

— Carefully select employees to be tasked with sensitive or high volume data handling and to ensure that they have the requisite skills to perform their functions without error. This should include appropriate training on internal systems, technologies, procedures and policies.

— Ensure that appropriate technical and organizational measures are in place to secure data, such that direct liability for data breaches can be avoided.

— Implement effective disaster recovery plans to mitigate the financial and reputational fallout from any accidental or deliberate personal data breaches that employee actions may give rise to.

— Document data processing instructions and the delegation of data handling responsibilities to employees (whether in connection with human resources, information technology, client relationship management, or the execution of internal audits) and ensure that clear and accessible internal policies provide for the appropriate parameters of such responsibilities.

…

CLEARY GOTTLIEB