CYBERSECURITY, DATA PRIVACY & INFORMATION MANAGEMENT ALERT: MORRISONS NOT LIABLE FOR EMPLOYEE'S WRONGFUL DISCLOSURE OF PERSONAL DATA

APRIL 2020

By Barry Fishley and George Mole

A sigh of relief for employers?

In its recent landmark decision, the UK Supreme Court found that Morrisons (the UK supermarket) was not vicariously liable for the actions of Mr Skelton, an employee who unlawfully disclosed personal data of close to 100,000 other Morrisons' employees and former employees on the internet and to three UK newspapers (the "unauthorised disclosure").[1]

The judgment overturns the ruling of the Court of Appeal (and the High Court before that) by restating the law on vicarious liability, which the Supreme Court (the "Court") argued had been misapplied. So does this mean employers can breathe a sigh of relief when considering the risks of their employees mishandling personal data and , if not, what steps should employers be taking to mitigate their risk of an employee doing the same?

What are the facts surrounding the case?

Morrisons employed Mr Skelton as a senior auditor in its internal audit team. In July 2013, Morrisons disciplined Mr Skelton for misconduct, however, the incident left Mr Skelton harbouring an "irrational grudge" against the supermarket. In November 2014, Mr Skelton was instructed to collate certain payroll information relating to Morrisons' employees (the "payroll information"), and transmit it to KPMG for the purpose of their annual audit. The payroll information included the name, address, gender, date of birth, phone numbers, national insurance number, bank details and salary of each employee.

In light of his personal grievance, once given access to the payroll information, Mr Skelton unlawfully copied the data onto a USB drive and, using his personal computer, uploaded it to a publicly accessible file-sharing website and anonymously sent CD copies to three UK newspapers. After being notified by one of the newspapers, Morrisons immediately contacted the police and set about taking steps to mitigate the impact of the unauthorised disclosure spending more than £2.26m in the process, much of it on measures to help protect the identities of affected employees. In separate criminal proceedings, Mr Skelton was sentenced to an eight year prison sentence.

What did the case decide?

The issues for the Court to determine were (1) whether Morrisons could be held vicariously liable for Mr Skelton's actions; and, if so (2) whether the Data Protection Act 1998 ("DPA 1998") excluded the imposition of vicarious liability for statutory torts committed by an employee data controller (under the DPA 1998), the misuse of private information and breach of confidence.

On the first issue, the Court ultimately found Morrisons free of vicarious liability for Mr Skelton's wrongful acts on the basis that, on the facts, Mr Skelton was not acting (or purporting to act) on behalf of Morrisons when he made the unauthorised disclosure but was instead on a "frolic of his own". Therefore, there was not a sufficiently close connection between the unauthorised disclosure and the instruction Morrisons gave Mr Skelton to collate and transmit the payroll information to KPMG for their independent audit. The fact that his employment gave Mr Skelton the opportunity to make the unauthorised disclosure was not sufficient to impose vicarious liability on Morrisons.

On the second issue, the Court found that because there is no express or implied exclusion under the DPA 1998 for vicarious liability of an employer, an employer could in principle be liable for a breach by an employee of the DPA 1998 where they act as a separate data controller. The judgment did not examine the underlying data protection legislation per se.

Does this mean that employers can breathe a sigh of relief as they are no longer at risk of vicarious liability where their employees mishandle personal data?

In short, no. Even though Mr Skelton's wrongful acts were committed when the DPA 1998 was in force, the principles of the Court's judgment will apply in future when determining vicarious liability for breaches of the General Data Protection Regulation (EU) 2016/679 ("GDPR") and the Data Protection Act 2018 ("DPA 2018") (as well as for the common law torts of misusing private information and breaching confidence). This means that unless an express or implied exclusion for vicarious liability is found

1 WM Morrison Supermarkets plc (Appellant) v Various Claimants (Respondents) [2020] UKSC 12

CYBERSECURITY, DATA PRIVACY & INFORMATION MANAGEMENT ALERT: MORRISONS NOT LIABLE FOR EMPLOYEE'S WRONGFUL DISCLOSURE OF PERSONAL DATA

APRIL 2020

> *Employers, first and foremost, need to make sure that they comply with their obligations under the GDPR and DPA 2018*

under the DPA 2018 or the GDPR, employers can be vicariously liable for breaches of the GDPR and/or DPA 2018 by employees.

How can employers mitigate the risk of vicarious liability where employees mishandle personal data?

Employers, first and foremost, need to make sure that they comply with their obligations under the GDPR and DPA 2018. This will not only help the employer mitigate the risks of vicarious liability but primary liability too.

To start with, employers should ensure they implement appropriate technical and organisational measures to ensure a level of security which is appropriate to the risk associated with that personal data. In practice, this might mean keeping a record of who accesses personal data and when, setting up a notification system to alert the employer when unusual activity of an employee is detected or imposing technical restrictions on the copying and/or downloading of large databases of personal data from work systems (e.g. preventing USB drives being used on work computers).

Employers should put robust, written data protection and IT security policies and procedures in place which set out how and when employees are able to access certain personal data (and this should be on a strictly need-to-know basis). Employers should also make sure they regularly provide appropriate training to employees on what they need to do to comply with the organisation's policies and procedures as well as the law more generally. Carrying out these steps will also assist the employer in demonstrating its own compliance with the GDPR and DPA 2018 as to avoid any primary liability.

Employers should consider whether they can obtain and maintain appropriate cybersecurity insurance policies. Insurance will probably not allow the employer to pass liability for regulatory fines but will allow the employer to recover first- and third-party losses arising from the disclosure of personal information in a data breach or cyber incident. In terms of liability claims, anyone who suffers material or non-material damage as a result of a data breach (including distress), will have the right to receive compensation from the company involved. The cybersecurity insurance policy will cover the defence costs and liability claims resulting from a breach of confidential information and can protect against malicious data breaches. Employers need to take a holistic approach so as to ensure that these policies are wide enough to cover the acts of all individuals for whom the organisation may be vicariously liable.

Key takeaways

- Where a single employee is given wide access to a database of personal data, there should be appropriate checks and balances on their access, such as keeping a log of how the data is accessed or used and having this log reviewed regularly. There should also be mechanisms in place to alert the employer of unusual activity by the employee.
- Employers should impose restrictions on the copying and/or downloading of large databases of personal data from work computers, such as by preventing the use of USB drives with work computers.
- Employers should impose measures to detect the unauthorised copying or downloading of personal data.
- Employers should obtain cybersecurity insurance to cover vicarious liability or ensure that any existing policy covers the risk.

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any of the authors listed below.

Barry Fishley	View Bio	barry.fishley@weil.com	+44 20 7903 1410
George Mole	View Bio	george.mole@weil.com	+44 20 7903 1367