

UPDATE

Data Security: WM Morrison Appeal

Update prepared by Carla Benest (Partner, Jersey), Mathew Cook (Partner, Jersey), Rachel Guthrie (Counsel, Guernsey) and Sally French (Senior Associate, Guernsey)

The Morrisons data breach case continues to highlight the message that threats to data security are internal as well as external. Beware the damage which may be done by one malicious employee.

We reported the first instance decision regarding the Morrisons data breach (see [here](#) for our last update). This has since been appealed (full appeal judgment available [here](#)), but the appeal outcome is of little comfort for business.

The Appeal

"The central issue on this appeal is whether, on the facts, an employer is liable in damages to those ...whose personal and confidential information has been misused by being disclosed on the web by the criminal act of another employee, who had a grudge against the employer, in breach of the Data Protection Act 1998 ("the DPA") and in breach of that employee's obligation of confidence."

The three ground of appeal were:

- That the DPA excludes vicarious liability;
- That the DPA excludes the tort of misuse of private information and equitable action for breach of confidence and/or vicarious liability for such breaches; and
- That it had been wrong to conclude that the wrongful acts of the rogue employee occurred during the course of his employment.

The DPA

The first and second grounds of appeal both concern the extent of the DPA.

In respect of the first ground, the Court of Appeal held that:

"...it is clear ... the vicarious liability of an employer for misuse of private information by an employee and for breach of confidence by an employee has not been excluded by the DPA."

In respect of the second ground Morrisons conceded that misuse of private information and breach of confidentiality were not excluded by the DPA in respect of the wrongful processing of data within the ambit of the DPA. There was no provision in the DPA addressing the situation of an employer where an employee data controller breaches the requirements of the DPA. In view of Morrison's concession and absent a relevant statutory provision, it was held that that the common law remedy of vicarious liability of the employer was not expressly or impliedly excluded by the DPA in circumstances where the common law requirements for such liability were otherwise satisfied.

Acts In The Course Of Employment

The leading Supreme Court authority on this point is another Morrisons case, *Mohamud v Wm Morrison Supermarkets plc* [2016] AC 667. That case set a two stage test:

"In the simplest terms, the court has to consider two matters. The first question is what functions or "field of activities" have been entrusted by the employer to the employee, or, in everyday language, what was the nature of his job.

...

Secondly, the court must decide whether there was 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 under the principle of social justice..."

The Court of Appeal found the first question readily satisfied, the rogue employee was regularly entrusted with confidential data, and dealing with the data was a task specifically assigned to him.

On the second question Morrisons' contention was that the close connection test was not satisfied because the harmful act was done by the rogue employee at his home, using his own computer, on a Sunday, several weeks after he had downloaded the data at work onto a personal USB stick. The Court of Appeal found that what fell to be considered was whether the harmful acts fell *"within the field of activities assigned to the employee"*. The Court of Appeal was satisfied that the sending of employee data to third parties was within the field of activities assigned to the rogue employee. The articulation of the first instance Judge, that there had been a seamless and continuous sequence of events providing an unbroken thread linking the criminal acts to the rogue employee's employment, was approved.

Implications

The appeal judgment has not moved matters on a great deal from the first instance decision. Neither judgment was critical of Morrisons' response to the data breach. But nevertheless neither judgment seeks to assist the business.

In a data protection context this is perhaps not surprising. The GDPR has made clear that the interests of data subjects are paramount, regardless of the risks to private enterprise. The Court of Appeal sees insurance as the commercial solution for businesses.

A novel feature of this case in the context of vicarious liability was the rogue employee's clear intention to cause the employer harm. It was submitted to the courts that upholding employer liability risked the courts being complicit in the furtherance of that purpose. However motive was found to be irrelevant in vicarious liability matters.

Nevertheless, the finding that misuse of data, for the clear purpose of harming the employer, formed part of the field of activities assigned to an employer is a difficult one to reconcile.

The case is to be appealed to the Supreme Court. Watch this space for how it is addressed.

Contacts



Carla Benest
Partner, Mourant Ozannes
Jersey
+44 1534 676 076
carla.benest@mourantozannes.com



Mathew Cook
Partner, Mourant Ozannes
Jersey
+44 1534 676 371
mathew.cook@mourantozannes.com



Rachel Guthrie
Counsel
Guernsey
+44 1481 739 395
rachel.guthrie@mourantozannes.com



Sally French
Senior Associate
Guernsey
+44 1481 739 341
sally.french@mourantozannes.com

This update is only intended to give a summary and general overview of the subject matter. It is not intended to be comprehensive and does not constitute, and should not be taken to be, legal advice. If you would like legal advice or further information on any issue raised by this update, please get in touch with one of your usual contacts. © 2018 MOURANT OZANNES ALL RIGHTS RESERVED