SUMMARY

2019/19 – Employer liable for wrongful disclosure of data by 'rogue' employee (UK)

While an internal auditor who disclosed payroll data on the internet was sentenced to eight years in prison, his employer was found to be vicariously liable for the data breach.

Summary

The supermarket chain Morrisons had an internal auditor who went rogue. Aggrieved at an internal disciplinary process, he disclosed payroll data on the internet relating to about 100,000 of his colleagues. He was tracked down, charged and sentenced to eight years in prison. Morrisons were found to be vicariously liable for the data breach, though they have indicated they will be appealing the judgment.

Background

Andrew S was an internal auditor employed by Morrisons. Mr S copied Morrison's master payroll file and went on to release the data of over 100,000 employees online. Mr S was subsequently convicted for criminal misuse of the payroll data and sent to prison. During his trial, it was revealed that Mr S's actions were an elaborate revenge campaign against Morrisons after he was subject to internal disciplinary proceedings in early 2013.

Over 5,500 employees took group action against Morrisons seeking damages for the distress arising from the disclosure of their personal data. The action included claims for direct liability for the disclosure (under the Data Protection Act 1998, common law principles and equity); alternatively on the basis that Morrisons was liable under common law vicarious liability principles.

Legal background

Privacy

This case was decided under the Data Protection Act 1998 ('DPA 1998') which was applicable at the time. The DPA 1998 implemented the Data Protection Directive 95/46/EC. Section 4(4) of the DPA 1998 states: "*it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller*".

The seventh data protection principle states: "*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*".

Section 13(1) of the DPA 1998 states that individuals do not need to have suffered financial loss in order to make a compensation claim for distress they have suffered.

Data subjects can also enforce their privacy rights by claiming breach of confidence in equity. To establish this claim, the relevant information must be confidential; imparted 'in circumstances importing an obligation of confidence'; and disclosed in a way that is detrimental to the person that imparted it.

A claim can also be brought in tort for misuse of private information where there has been misuse of information that was obviously private.

Vicarious liability

Employers will be liable for an employee's actions where there is sufficient connection between the employment and the wrongdoing. In order for vicarious liability to be established, it must be determined that there is a relationship between the employee and the employer which is capable of giving rise to vicarious liability, and that the connection between the employment and the wrongful act or omission is so close that it is just and reasonable to impose liability (this second part established in *Lister – v – Hesley Hall Ltd* [2001] UKHL 22 as the 'sufficient connection' test).

High Court judgment

The High Court held that Morrisons had no direct liability but that, even though it had done nothing wrong, it was indirectly or 'vicariously' liable for the leak because the auditor was acting in the course of his employment. Although 'only' 5,500 employees had brought a claim, there was potential liability to all 100,000 employees. Even if an individual employee might recover only a small amount for the distress caused, the overall financial impact on Morrisons might be enormous.

In reaching his judgment, the judge expressed his concern that, as Mr S's intention was to cause harm to Morrisons, the decision might have the unintended effect of furthering Mr S's aims. Accordingly the judge granted Morrisons permission to appeal his decision on vicarious liability.

Morrisons appealed to the Court of Appeal, on two main grounds. First, it argued that vicarious liability had no place in data protection law and did not apply. Secondly, it said that the auditor was not acting in the course of his employment.

Judgment

The Court of Appeal rejected the appeal.

On the first ground, it could see no reason why vicarious liability should not apply. If Parliament had intended to eradicate an individual's normal common law rights, it would have said so.

The Court of Appeal then turned to the second ground and whether or not the auditor was acting in the course of his employment. Previous cases on vicarious liability had established a two-step test:

Identify the function or field of activity entrusted by the employer to the employee.
Consider whether there was sufficient connection between the individual's position and his wrongful conduct to make it 'right' for the employer to be held liable.

The first step was simple – the employee had clearly been entrusted with payroll data. But was there sufficient connection between his position and leaking the data? The leak had occurred some weeks after he had taken the data, at his home, using his own computer. In addition, his aim was to cause harm to his employer. If Morrisons were found liable, the result – albeit indirectly – would be to help him achieve that aim.

After looking at various previous cases, the Court of Appeal concluded that the employee was acting in the course of his employment. The employee's removal of the data and subsequent publication constituted a 'seamless and continuous sequence' or 'unbroken chain' of events. In addition, the Court of Appeal concluded that the motive of the employee (i.e. to cause Morrisons harm) was irrelevant to the analysis of whether Morrisons were vicariously liable. The appeal was therefore not upheld.

Commentary

Normally, the law will only impose liability on an individual who is blameworthy, but vicarious liability is an exception to this. In essence, vicarious liability is about loss distribution and achieving fairness and justice, imposing liability on the person most able to pay. Since the late 1990s, however, the courts have extended the scope of vicarious liability, taking a flexible and expansive approach.

One can argue over whether it is right that an employer should be responsible for, say, the actions of a racist employee who attacks a customer, but normally the imposition of liability causes little difficulty. Claims are limited in number – for example, even cases about allegations of sustained sexual abuse rarely involve more than 100 claims against one institution. The costs of meeting such claims are generally manageable, and may be insured.

The Morrisons case breaks new ground – although at least it was limited to an identifiable, albeit very large group. Facebook has recently admitted that up to 50 million users were affected by a data breach. Will they bring claims for the distress caused?

Although Morrisons has said it will seek to appeal to the Supreme Court, the issues raised by the case go well beyond its specific facts. Ultimately, Parliament may need to decide on the extent of liability. Pending that, employers should dig out their insurance policies and check the scope of their cover.

Comments from other jurisdictions

Finland (Janne Nurminen, Roschier, Attorneys Ltd.): If taking place now, the situation would be resolved under the General Data Protection Regulation (EU) 2016/679 (the GDPR). According to Article 82 of the GDPR, any person who has suffered material or non-material loss as a result of an infringement of the GDPR has the right to receive compensation from the controller or processor for the loss suffered. Here the employer is a controller under the GDPR. In the case of personal data breach, the controller must without undue delay and, where feasible, not later than 72 hours notify the supervisory authority about the breach (Article 33). The controller must also inform the data subject, when the data breach is likely to result in a high risk to the rights and freedoms of natural persons. When it comes to the award of damages under national law, the employer is vicariously liable for the loss caused by an employee through an error in work performance or omission at work (Chapter 4, Section 3 of the Finnish Tort Liability Act, 412/1974 as amended). The grounds for the employer's liability is the employee's negligence and liability is limited to breaches made in the course of employment. Therefore, the employer's vicarious liability actualizes only if the loss arises in the employee's performance of work. Under Article 83 of the GDPR, an administrative fine might also be imposed on the controller, i.e. the employer.

The employee is, under Chapter 4, Section 1 of the Tort Liability Act, liable for the loss they cause in the performance of work, up to an amount that is considered reasonable. If the employee causes the loss willfully, the employee is liable for the damages under joint liability. In addition, the main rule is that for willfully caused loss full compensation is payable by the employee unless there are special reasons to reduce the damages. (In practice, the employee's liability is directed to the employer who is liable for the loss under vicarious liability and thus has the right to recover the paid damages from the employee.)

As we have understood, the internal auditor worked on an employee status and there was a sufficient connection between the employee's position and the wrongful conduct. Therefore, the employer would, in Finland also, be vicariously liable for the data breach. The other employees could under vicarious liability claim compensation from the employer, i.e. the company, but also from the employee since the employee's actions were willful. If the employer pays full compensation, the employer has the right of recovery, i.e. the right to claim compensation from the employee. The degree of the employee's negligence needs to be taken into account when assessing their liability for the damages. In this case, however, the employee acted willfully so it is likely that full recovery would be available, unless the employee was able to invoke special reasons.

For the sake of clarity, a Finnish court would similarly need to assess whether the employee acted in the course of employment or whether the actions of the employee were so unexpected that the employer could not be held liable. According to the legislative preworks of the Tort Liability Act, it is difficult to assess whether the employee's action in this case took place in the performance of work but the provision should be interpreted broadly rather than narrowly (as it is for third party protection).

Subject: Privacy

Parties: Various Claimants – *v* – Wm Morrisons Supermarket plc

Court: Court of Appeal

Date: 22 October 2018

Case Number: [2018] EWCA Civ 2339

Internet Publication: https://www.bailii.org/ew/cases/EWCA/Civ/2018/2339.html

EELA EUROPEAN EMPLOYMENT LAWYERS ASSOCIATION

Creator: Court of Appeal
Verdict at: 2018-10-22
Case number: [2018] EWCA Civ 2339