KEY POINTS

- Morrisons were held to be vicariously liable for the actions of a disgruntled employee who was deliberately, and criminally, seeking to cause them harm through the disclosure of employee data in circumstances where there was no suggestion that Morrisons had failed to act promptly to take down all the data from the internet once the leak had been discovered.
- The case thus provides a clear warning to financial institutions that they must have robust training and procedures in place for those who deal with data and, most importantly, have specific insurance in place to cover any such liability.
- Financial institutions should, however, take comfort from the fact that the High Court held that liability under the Data Protection Act 1998 is not strict but, rather, requires fault, a conclusion not challenged on appeal. Thus, by having robust training and procedures in place, a financial institution should be able to minimise the prospects of being found in breach and should, as a result, be able to reduce their insurance premiums.

Feature

Authors Sir Richard Aikens and Andrew Dinsmore

Financial institutions beware: cybersecurity lessons from the *Wm Morrisons Supermarket* case

In *Various Claimants v Wm Morrisons Supermarket Plc* [2017] EWHC 3113 (QB); [2018] 3 W.L.R. 691 the High Court held that an employer could be vicariously, but on the facts of this case, not primarily, liable for the deliberate and criminal actions of a rogue employee in the context of a group action for breach of the Data Protection Act 1998 (DPA), misuse of private information and breach of confidence. The Court of Appeal, [2018] EWCA Civ 2339, upheld the first instance decision. The case provides a clear warning for financial institutions who control large amounts of data.

FACTS

The defendant operates a chain of well-known supermarkets. Its external auditor requested a copy of its payroll data, which included personal and bank data of nearly 100,000 personnel. One of the defendant's internal auditor team, a disgruntled employee who had been the subject of internal disciplinary action by the defendant (the Employee), lawfully had this data on his work computer to facilitate its transfer to the external auditor.

However, he then unlawfully copied this data to his own computer and posted it on a file-sharing website to which links were published elsewhere on the internet. He later posted it to three newspapers with the intention of harming the defendant. The defendant learned of the publication and immediately took steps to take the website down. The Employee was subsequently convicted under the Computer Misuse Act 1990 and s 55 of the DPA and sentenced to eight years imprisonment.

The claimants were a number of employees that brought an action for breach of s 4(4) of the DPA, arguing that the defendant was, at all times, the "data controller" and that the payroll data had been misused by reference to the "data protection principles" set out in Sch 1, para.1, 2, 3, 5 and 7. The key issues were therefore whether:

- The DPA imposed primary liability on the defendant, where it is a corporate entity and the misuse had been the actions of its employee.
- Liability for a breach of one or more of the principles set out in Sch 1, para 1, 2, 3, 5 and 7 was strict or required fault.
- If there was no primary liability, the defendant was vicariously liable for the wrongful actions of the internal auditor.
- The defendant was liable for misuse of private information and breach of confidence.

THE FIRST INSTANCE JUDGMENT

The High Court held that:

- The "data controller" was the person who made decisions about how and why personal data were processed (§§45-46).
- A company could be only primarily responsible for those who processed such data on its behalf where the company had authorised or facilitated their actions (§§49-51).
- Schedule 1, para 1, 2, 3 and 5 of the DPA did not create strict liability but rather required fault on the part of the "data controller" (§§63-64).
- However, on the facts there was no primary liability in relation to Sch 1, para 1, 2, 3 and 5 of the DPA for the actions of the Employee because his actions (copying the data and then uploading it etc) were unauthorised and the defendant had not facilitated his actions; his actions were therefore not the primary actions of the defendant in its capacity as the "data controller" (§65).
- Similarly, there could be no primary liability for misuse of private information nor for breach of confidence because the defendant had not been the party responsible; rather, it was the Employee acting without authority and criminally (§66).
- Schedule 1, para 7 was, however, different because it required that the

"appropriate technical and organisational measures shall be taken [by the data controller] against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

- In this context, the word "appropriate" in Sch 1, para 7 was intended to set a minimum standard as to the security to be achieved. However, what is "appropriate" would be influenced by technological developments available and the costs of implementation; in this regard, the simple fact that some technology was available was not enough to require it to be used, because it may be prohibitively expensive (§68).
- Further, whilst the term "reasonable care" was not used in Sch 1, para 7 of the DPA, the standard of care in negligence would be "indicative of the standard which should apply" (§69).
- The defendant was "undoubtedly" the "data controller" at the time when the duty imposed by Sch 1, para 7 fell to be discharged (§71).
- The defendant had taken precautions against people misprocessing, mishandling or disclosing information without authority through limiting access to a few trusted people (§80).
- Further, the simple fact that the Employee had previously been the subject of a disciplinary procedure (which resulted in a "verbal" warning only), did not indicate to the defendant that the Employee was likely to criminally disclose data entrusted to him (§§91-96); nor that there should have been monitoring or mentoring to prevent the specific individual from dealing with the data (§97).
- However, the defendant had failed in its duty under Sch 1 para 7 because there was no organised system for checking that data such as the payroll, which had been legitimately transferred to a work computer, had been subsequently and safely deleted; there was no failsafe system in respect of safe deletion (§118).
- Nevertheless, in the circumstances of this case, by the time that it would have been appropriate to make a check that the data had been deleted, the data would already have been unlawfully copied, such that any breach of the duty under Sch 1, para 7 by the defendant neither caused nor contributed to the Employee's criminal misuse of the payroll data (§121, §125).
- Although the court absolved the defendant of any primary liability under the DPA and at common law, the defendant was vicariously liable for the unlawful and unauthorised actions of the Employee. The DPA did not exclude the possibility of vicarious liability of a corporate employer where the employee had become the "data controller" of the information and where he is in breach of statutory obligations that rest on him alone, while acting in the course of his employment (§154). There could be vicarious liability on the employer even when it is not the "data controller" and had no statutory duties itself at the time that the Employee wrongfully disclosed the data (§155 and §156).
- The unlawful disclosure was committed whilst the Employee was the "data controller" and in the course of his employment because: the actions were sufficiently closely connected to his role as an internal auditor in time, place and nature (§184); the defendant deliberately entrusted the Employee with payroll data (§185); his role in respect of the payroll data was to receive and store it, and to disclose it to a third party who was authorised to receive it (§186); it was irrelevant that the defendant was not, also, a "data controller" (§188); the fact that the Employee's motive was to deliberately harm the defendant was irrelevant, relying on the recent Supreme Court case of *Mohamud v WM Morrison Supermarkets Plc* [2016] UKSC 11, [2016] A.C. 677 (§190); and, it was important to note that the defendant was not the only victim and the issue was not so much at whom the conduct was aimed, but rather upon whose shoulders it is just for the loss to fall (§193).

> Although the court absolved the defendant of any primary liability ... the defendant was vicariously liable for the unlawful and unauthorised actions of the Employee.

THE COURT OF APPEAL JUDGMENT

The Appellants argued that Langstaff J erred in three respects, noted at §33 of the judgment of the court:

- First, the judge should have held that the DPA excluded the application of vicarious liability.
- Second, he should have held that the DPA excluded a cause of action for misuse of private information and breach of confidence and/or the imposition of vicarious liability for breaches of the same.
- Third, the judge should have held the wrongful acts did not occur during the course of the Employee's employment by Morrisons and thus should have held that Morrisons were not vicariously liable for his actions.

Interestingly, neither party challenged his Lordship's dismissal of the claims for breach of statutory duty nor his conclusion that the Employee had become the 'data controller' for the purposes of the DPA at the time that he wrongfully copied the data onto his personal USB stick and then disclosed it on the internet (§35).

The Court of Appeal held that:

- The first and second grounds could be dealt with together and held that the DPA does not exclude vicarious liability for causes of action outside the ambit of the DPA. The court made three points:
  - First, if Parliament intended such a substantial eradication of common law and equitable rights, it might have been expected to say so expressly (§§51-52).

- Second, Morrisons accepted that primary liability for causes of action at common law and in equity operated in parallel with the DPA (which accords with what the courts had stated in *Campbell v MGN Ltd* [2004] 2 A.C. 457) and noted that it was a "difficult line to tread" also to contend that there could not be vicarious liability as it "may be said to present an 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" (§§53-56).
- Third, the DPA says nothing at all about the liability of an employer, who is not a "data controller", for breaches of the DPA by an employee who is a "data controller". This rendered the present case quite different from the case law cited by Morrisons because the legislation in those cases expressly and specifically addressed the circumstances which, it was contended, also gave rise to a common law remedy and the court in those cases held, as a matter of statutory interpretation, that the statutory remedy was exclusive (§§57-60). The legislation in the present case did not do so.

As to the third ground of appeal, the Court of Appeal upheld Langstaff J and held that:

- The time and place where the acts are committed will always be relevant, but not conclusive, and noted that there are several instances where employees have been held liable for acts away from the workplace, citing *Bellman v Northampton Recruitment Ltd* [2016] EWHC 3104, QB (§71).
- On the (unchallenged) facts, the Employee's actions formed part of a "seamless and continuous sequence" or "unbroken chain" (§74).
- The novel point in this case was that the Employee's actions were directed at harming the defendant rather than to achieve some benefit for himself or inflict injury on a third party. The Court of Appeal held that it was clearly established that an employer could be held vicariously liable for an employee's actions that intended to cause harm (citing the seminal case of *Lloyd v Grace Smith* [1912] A.C. 716 and the more recent sexual abuse cases of *Lister v Hesley Hall Ltd* [2002] A.C. 215 and the *Catholic Child Welfare Society* case [2013] 2 A.C. 1). The Court of Appeal noted Lord Toulson's conclusion in *Mohamud v William Morrison Supermarket plc* [2016] A.C. 677 that motive was irrelevant and held that there is no exception where the motive is to cause harm to the employer (§§75-76).
- The fact that there were a potentially large number of claimants was an "unconvincing" argument to hold that Morrisons were not liable (§77) and the Court of Appeal noted that:

> "There have been many instances reported in the media in recent years of data breaches on a massive scale caused by either corporate system failures or negligence by individuals acting in the course of their employment. These might, depending on the facts, lead to a large number of claims against the relevant company for potentially ruinous amounts. The solution is to insure against such catastrophes ... the availability of insurance is a valid answer to the Doomsday or Armageddon arguments put forward by ... Morrisons." (§78).

COMMENTS

This article builds on our series of articles on liability for Cybersecurity breaches (see [2017] 11 JIBFL 676 and [2018] 8 JIBFL 505). It is the first case where an action has been brought pursuant to a Group Litigation Order for data breaches and provides a clear warning for financial institutions who control large amounts of data, especially because there was no suggestion that the defendant had not acted promptly in taking down all the data from the internet once the leak had been discovered.

The interesting points to note are that:

- The statutory duties in Sch 1 paras 1 to 7 are placed on the "data controller" only, by virtue of s 4(4), and only for as long as that person (natural or legal) remains the "data controller" (High Court, §51) . If a person or entity ceases to be a "data controller", that person (natural or legal) is no longer personally bound by those duties. Although it is possible for there to be two "data controllers" at any one time, in this case the defendant ceased to be the "data controller" once the Employee started to use the data for his own ends, at which point the Employee became the "data controller" (High Court §51). For the defendant to be primarily liable (as opposed to vicariously liable for the wrongdoing of the Employee) there had to be a breach of one of the duties in Sch 1 paras, 2, 3, 5 or 7 at the time the defendant was "data controller", ie before the Employee misused the data.
- Schedule 1, paras 2, 3 and 5 of the DPA, which concern the obtaining, keeping and processing of personal data, are of a different character to Sch 1, para 7 of the DPA, which concerns the technical and organisational safeguards that are required specifically to avoid unauthorised or unlawful processing or accidental loss, destruction or damage to personal data. The former relates to the nature of the personal data and how it is to be dealt with, whereas the latter concerns the systems that a data controller should have in place to guard against unauthorised or unlawful processing or accidental loss, destruction of or damage to the personal data.
- The circumstances in which Langstaff J held that the defendant was vicariously liable for the wrongful acts of the Employee are, perhaps, unusual.
  - First, the court held that the defendant was vicariously liable for the Employee's breaches of Sch 1, para 1, 2, 3 and 5 despite holding that the defendant did not, itself, owe

Feature

Biog box

Sir Richard Aikens is based at Brick Court Chambers and is a former Lord Justice of Appeal who now works as an arbitrator in international commercial disputes. He is also a Visiting Professor at King's College London and Queen Mary University of London and one of the editors of Dicey, Morris & Collins Conflict of Laws. Email: richard.aikens@brickcourt.co.uk

any duties under these paragraphs because it was not the "data controller" at that time. Langstaff J applied the well-known statement of Lord MacDermott in *Harrison v National Coal Board* [1951] AC 639 at 671 to the effect that an employer can be vicariously liable for the breach of statutory duty placed on an employee (so long as the breach is committed during the course of his employment), even if, at the time of the employee's breach, the employer does not owe the same or a similar statutory duty to the claimant.

- Second, it may be said that Langstaff J took a broad view of what constituted "the course of employment" on the facts. However, because the process of deciding whether an action is within the course of employment is one that is "broad and evaluative", if a judge finds that the act was within the course of employment it will be difficult to reverse that factual conclusion on appeal. That was made clear on appeal in this case where no attempt was made by the Appellants to challenge these factual conclusions with which the Court of Appeal noted their agreement. Langstaff J accepted (High Court, §199) that it might seem curious to hold a party vicariously liable for acts that (in the submission of the defendant) were deliberately aimed at that same party. Normally, the acts for which a defendant is held vicariously liable, whether negligent or deliberate, are directed at a third party. Whilst it was, therefore, perhaps not surprising that Langstaff J gave permission to appeal to the Court of Appeal on this point, it was not an argument that impressed the Court of Appeal at all. Its robust conclusion was that the motive of the employee who committed a wrong towards third parties was wholly irrelevant even in these circumstances where the motive was to do damage to the employer and even when, at the time the tortious acts of the employee were committed, the employer owed no statutory duties under the DPA to its employees because it had ceased by then to be the "data controller".
- Third, although Langstaff J did not spell it out in the section of the judgment on vicarious liability, it would appear that he concluded that the Employee, as "data controller" at the time he wrongfully misused the data, was guilty of breaches of the duties imposed by Sch 1 paras 2, 3 and 5. Therefore, his Lordship held that the defendant was vicariously liable for those breaches of statutory duty by the Employee when he became "data controller". This is implicit in the Court of Appeal's reasoning as well.

- The case is a good example of the efficacy of Group Litigation Orders in the context of a cyber-security and data breaches. Whilst the judgments do not give much insight into the operation of the GLO itself, it is nevertheless interesting to see that it is possible successfully to manage a GLO so as to reach a substantive judgment on liability issues whose resolution would enable quantum issues to be determined at a later date. GLOs can be particularly useful when combined with voluntary redress schemes (like, for example, the redress schemes established by banks to address the mis-sale of interest rate hedging products): the GLO can provide a useful vehicle through which key issues can be determined judicially with the litigation then stayed in favour of a redress scheme to resolve each individual dispute.
- The judgments are both silent on how much litigants can be expected to receive by way of quantum in circumstances where the defendant was not directly in breach of the DPA statutory duties, but only vicariously liable for the wrongful acts of the Employee when the employee was the "data controller". In the US, the maximum sum claimable is US$1,000 (provided for by statute) and it is for that amount that the 70 million litigants have brought an action in the Cambridge-Analytica Class Action. There are indications in the English Courts that serious breaches could lead to a liability for £10,000 (see *Gulati v MGN Ltd* [2015] EWHC 1482).
- The Court of Appeal has made clear that misuse of private information and breach of confidence exist alongside an action for breach of the DPA; it will be interesting to see, in practice, when, if at all, a court finds a breach of the former without finding a breach of the latter.
- The Court of Appeal also made clear that organisations that deal with a large quantity of personal data should have extensive cyber-security insurance in place. The court specifically noted that without such insurance, a data breach would potentially be ruinous. It is thus clear that future defendants will not be able to gain any sympathy from the courts through arguing that a successful action will potentially destroy them; the simple answer is that they should have insured against such a risk. Whilst financial institutions have perhaps been a little slow to take out specific cyber-security insurance, this judgment makes clear that such insurance is now essential.

These cases come at a critical time in the regulation of data:

- The General Data Protection Regulation (679/2016/EU) (GDPR), which came into effect in May 2018, places more stringent requirements on "data controllers" and provides a right to damages for "material and non-material damages" in Art 82 (which is likely to include emotional distress as *Vidal-Hall et al v Google* [2016] Q.B. 1003 held when construing s 13 of the DPA that incorporated the Directive preceding the GDPR and as noted in s 168 of the Data Protection Act 2018).
- Further, Art 80 of the GDPR provides

Biog box

Andrew Dinsmore, based at 20 Essex Street, is a barrister practising in International Commercial Litigation and Arbitration. He regularly acts in banking and financial matters and cybersecurity cases; his recent work includes: (i) acting in two cases for a large number of claimants in a group litigation action following high-profile data failures of major airlines; and (ii) obtaining a number of urgent freezing injunctions and Norwich Pharmacal Orders in the context of cyber-fraud. Email: adinsmore@20essexst.com

that a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a member state, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data, can lodge a complaint on behalf of a complainant thereby making group litigation even easier than the traditional CPR Pt 19 route.

- Regulators are becoming increasingly likely to impose substantial fines on financial institutions where they fail to properly protect data; for example:
  - the Financial Conduct Authority recently fined Tesco Personal Finance Bank PLC £16.4m for failures in a 2016 cyber-attack; and
  - the Information Commission recently fined Bupa Insurance Services Ltd £175,000 for failing to have effective security measures in place to protect customers' personal information.

It is thus clear that the English legal and regulatory system has woken up to the importance of data and hence why some say that "data is the new oil". It is important that, in order to avoid potential liability to many possible claimants, financial institutions have robust training and procedures in place for those who deal with data and it is now crucial that they have adequate insurance in place. ■

Further Reading:

- The legal implications of cybersecurity breaches for financial institutions (2017) 11 JIBFL 676.
- Cybersecurity litigation: jurisdiction, applicable law and class actions (2018) 8 JIBFL 505.
- LexisPSL: Financial Services: Information and cyber security for financial services firms – overview.