Morrisons not to blame for actions of an employee with a grudge

Carrying the can: What does the UK Supreme Court's decision in Morrisons tell us about liability under data protection law? By **Victoria Hordern** of Bates Wells.

In what circumstances should an employer be vicariously liable for the actions of an employee where those actions have an impact on other individuals' data protection rights? This was the core question that the UK courts considered as part of the series of decisions which culminated in the Supreme Court's judgment published in early April[1]. Many employers were concerned by the implications of the lower court rulings which held that an innocent employer was vicariously liable for the criminal actions of an employee.

Data protection authorities that investigate complaints determine liability when deciding whether to take any enforcement action (and in this case for Morrisons, the Information Commissioner (ICO) took no enforcement action). With the advent of the General Data Protection Regulation 2016/679 (GDPR), there are increasing attempts by individuals (through class or individual actions) to seek compensation through the courts. Working out who bears liability is essential.

Under the Data Protection Act 1998 (DP Act) there were a number of court decisions where controllers were held liable for damages; but the sums awarded were low. The stakes have now increased due to the advent of the GDPR and Data Protection Act 2018 (DP Act 2018).

The final outcome in Morrisons

The circumstances related to a Morrisons' employee (Mr Skelton) maliciously uploading payroll data of Morrisons onto the Internet where his actions were motivated by a grudge against his employer following an incident where he was disciplined. As part of his authorised activities as an auditor, Skelton was permitted to receive payroll data. But his activities to (i) copy the payroll data onto a USB stick, (ii) remove the copy from Morrisons' control, and (iii) upload it onto a file sharing website, were not authorised.

A group of Morrisons' former and current employees brought a claim for compensation against Morrisons under the DP Act (since the incident occurred pre-GDPR) and common law. The claim of direct liability was dismissed in the High Court as Mr Justice Langstaff (Langstaff J) determined that Morrisons could not be primarily liable for the actions of Skelton since Morrisons was not the controller at the time. But the claim for vicarious liability was upheld in the High Court and Court of Appeal.

Ultimately the Supreme Court ruled that it was abundantly clear that Skelton had not been engaged in furthering Morrisons' business when he committed the wrongdoing. Therefore the employee'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 (the victims), it could fairly and properly be regarded as done by Skelton while acting in the ordinary course of his employment. Consequently, Morrisons was not vicariously liable.

Controllers, employers and employees

Data protection law revolves around the concept of a controller – it is the controller who is primarily responsible under the GDPR and who was solely responsible for compliance under the DP Act (as per the EU Data Protection Directive 95/46 (Directive)). A controller can be an individual (e.g. an employee); it can be a company (e.g. an employer). It is whoever or whatever is determining the purposes and means of processing personal data.

But employees are not separate controllers if they are under the direct authority of a controller or processor. Employees can become "third parties" if they engage in activities which are not authorised by the employer[2]. Of course in reality it is employees that overwhelmingly make decisions about processing personal data. A tension therefore exists between the decisions made by an individual employee (at what point do these become decisions made as an independent controller?) and decisions attributed to the legal entity as controller.

Employers and employees

The common law development of vicarious liability in the UK has long established that an employer may be vicariously liable for deliberate wrongdoing by an employee. But the DP Act says nothing at all about the liability of an employer, who is not a controller, for breaches of the DP Act by an employee who is a controller. Morrisons argued therefore that the DP Act was only concerned with primary liability.

The claimants' legal team argued in the High Court that if a controller is only held liable if it has contravened its DP Act statutory obligations, a controller could comply with the DP Act through the actions of its employees but never be in breach of its obligations should an employee misuse data. In their view, the statutory scheme should impute to an employer controller the processing (good or bad) of its employees. Langstaff J disagreed since it would mean a controller would be liable not only for breaches it had authorised but also for those it had not authorised[3]. Imputing direct liability in such circumstances would be wrong. However, Langstaff J considered liability could be established vicariously since there was an unbroken thread linking Skelton's work as an auditor to his criminal disclosure[4].

Under the DP Act security principle (DPP 7) a controller was required to take reasonable steps to ensure the reliability of employees who access

personal data. This was not a requirement originating from the Directive and is not language we see in the GDPR[5]. The claimants argued that Skelton was not a trusted employee and by giving him access to payroll data, Morrisons failed to comply with DPP 7. Langstaff J disagreed since the level of warning given to Skelton following his disciplinary did not mean that he could not be trusted to do his job[6]. In other words, it is not reasonable to expect employers to be able to predict that an employee will act in a criminal manner. Would further training have prevented the criminal disclosure by Skelton? Highly unlikely. Would additional monitoring by Morrisons have prevented the disclosure? Possibly, but Langstaff J considered that implementing broad surveillance measures to find out if an employee had behaved thoughtlessly with data would be disproportionate. This should provide reassurance to employers that there's no expectation of close (and constant) employee monitoring.

The importance of harm?

Amidst the legal arguments in the Morrisons litigation, it can be easy to overlook the fact that, on the face of it, the affected individuals suffered little harm. While the personal details of 100,000 Morrisons employees were available on a file sharing website for a couple of months, as soon as Skelton alerted newspapers to the fact that the details were available publicly, access to the data file was disabled. There is no record of any proven harm suffered by individuals as a result of the disclosure. However, dealing with the implications of Skelton's actions cost Morrisons at least £2.26m. Much of this sum had been spent on identity protection measures for victims to help reduce the likelihood of harm. Was it fair for Morrisons to be expected to pay compensation as well when there seemed to be little harm?

Unresolved aspects

Morrisons argued that making an employer vicariously liable in all circumstances would be disproportionate and not in the public interest. Langstaff J thought this was overstating the case and referred to the availability of insurance. The Supreme Court insisted that vicarious liability could still apply for employers where employees act as independent controllers since nothing in the DP Act excluded this possibility (and we should expect the same interpretation under the GDPR/DP Act 2018). What is not entirely clear is in what (presumably quite narrow) circumstances this rule would apply and an employer would be vicariously liable for an employee who acts as an independent controller.

The High Court and Court of Appeal signalled that implementing insurance was how employers should deal with the potentially enormous burden of dealing with compensation claims from individuals brought under a vicarious liability action. No real consideration was given to the practical likelihood of employers procuring such insurance and the Supreme Court declined to comment further on this aspect.

Remedies and social justice

One of the factors influencing the lower courts' rulings was the desire to achieve the purposes of the Directive including providing affected individuals with a judicial remedy[7]. While Langstaff J conceded that it would be unjust to expose controllers who are without fault to "enormously burdensome group litigation and claims out of all proportion to the value of the claims of the…" individuals affected[8], the incident required consideration of upon whose shoulders it is just for the loss to fall[9]. Langstaff J concluded that it was right for Morrisons to be liable vicariously "under the principle of social justice"[10].

The GDPR also states that every individual has a right to an effective judicial remedy where his rights have been infringed as a result of non-compliance[11]. Furthermore, any person who has suffered material or non-material damage as a result of a GDPR infringement has the right to receive compensation for damage suffered[12]. A controller involved in processing is liable for the damage caused by the infringing processing but is exempt from liability if it can prove that it is not responsible for the event giving rise to the damage[13]. Where more than one controller are involved in the same processing and where they are responsible for any damage caused by processing, each controller shall be held liable for the entire damage in order to ensure effective compensation[14]. If this incident had occurred under the GDPR, presumably Morrisons would have argued successfully that it was not responsible. But what if the incident had comprised slightly different facts? So Morrisons had implemented Data Loss Prevention technology that detected that Skelton was copying the payroll onto a third party USB, triggered an alert to an IT supervisor, but failed to stop the copying or the resulting disclosure. While that may have amounted to a contravention of Article 32, would this also have meant Morrisons was "involved" in the criminal disclosure and therefore responsible for any

REFERENCES

1 *WM Morrison Supermarkets plc v Various Claimants* [2020] UKSC 12
2 Article 29 Working Party, Opinion on Controllers and Processors, WP 169, 16 February 2010, p. 31 and see Article 4 (10) GDPR
3 *Various Claimants v WM Morrisons*, [2017] EWHC 3113 (QB), 49
4 *Ibid*, 183
5 The closest we get to it is in Article 28 where a processor must contractually commit to ensure that persons authorised to process personal data have committed to confidentiality.
6 *Various Claimants v WM Morrisons*, 91
7 Directive, Article 22
8 *Various Claimants v WM Morrisons*, 146
9 *Ibid*, 192
10 *Ibid*, 194
11 Article 79
12 Article 82 (1)
13 Article 82 (2) and (3)
14 Article 82 (4)
15 *Fleming, Law of Torts*, 9th edition (1998) quoted in *Majrowski v Guy's and St Thomas' NHS Trust* [2005] EWCA Civ 251

damage caused?

While the Supreme Court's ruling may well have reassured many employers, is there a danger that individuals who suffer damage due to data protection contraventions are left exposed where an employee acts in a way that their employer is not vicariously liable for? What if, as a consequence of the disclosure, there were substantial financial losses for the victims. Morrisons clearly has deeper pockets than Skelton. Will the courts in the future, for social justice purposes, impute liability to an employer in such circumstances to ensure that individuals receive a judicial remedy and compensation?

Vicarious liability is a compromise between two conflicting policies – firstly, the social interest in furnishing an innocent tort victim with recourse against a financially responsible defendant, and secondly, a hesitation to foist any undue burden on a business[15]. Since we are likely to see an increase in data protection claims, what lengths do employers have to go to in order to demonstrate that employee actions do not give rise to vicarious liability? The Supreme Court's decision may allow employers to breathe easier in the short term but there's no guarantee that employers would never face vicarious liability for data protection breaches in the future.

AUTHOR

Victoria Hordern is a Partner and Head of Data Privacy at Bates Wells.
Email: V.Hordern@bateswells.co.uk

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Returning to work: Covid-19 and the UK data protection perspective

Nicola Fulford and **Hannah Jackson** of Hogan Lovells report on the data protection aspects organisations should consider with regard to coronavirus testing and processing of health data.

Individually, many of us use data to track our progress – from fitness gains to home energy consumption; we watch information about our lives and use it to inform our activities. On a larger scale, numerous organisations have made significant investments in data analytics capabilities, and at a state level, a vast quantity of information about populations is used to direct public policy. It is not unreasonable,

Continued on p.3

Winner of the ICO's Data Practitioner Award: Barry Moult

The regulator's annual award recognises a long career in NHS Information Governance and innovative thinking. **Laura Linkomies** talked to Barry Moult about his work.

The 2020 ICO Practitioner Award for Excellence in Data Protection was awarded to Barry Moult, Information Governance and Privacy Consultant, and former Head of Information Governance and Health Records at the Colchester Hospital University NHS Foundation Trust. Recently retired from his role at Colchester, which he held from 2014 to 2018, Barry is now utilising his decades-

Continued on p.5

Issue 109 **MAY 2020**

UNITED KINGDOM
report

ISSUE NO 109 **MAY 2020**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Nicola Fulford and Hannah Jackson
Hogan Lovells

Josephine Jay and Christopher Foo
Wilson Sonsini Goodrich & Rosati

Victoria Hordern
Bates Wells

Emma Erskine-Fox and Gareth Oldale
TLT

Rebecca Cousin and Cindy Knott
Slaughter & May

Jonathan Armstrong
Cordery

David Barnard-Wills
Trilateral Research

Camilla Ravazzolo
UK Market Research Society

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

Stay alert to Covid-19 data protection issues

There is unfortunately still much uncertainty about when we are back to "normal" life in the UK. The 'new normal' will most definitely include new rules and procedures at the workplace when offices start to reopen. Read on p.1 our correspondent's analysis of the data protection implications at the workplace.

We recently carried out a survey to find out about the challenges that DPOs encounter due to the pandemic. There are implications across the board: for remote working, data security, processing employee data etc. Read on p.12 how organisations are tackling these issues. Normal compliance work, for example processing Subject Access Requests has not gone away – in fact some organisations are seeing an influx of requests relating to furloughing and employee health records (p.9). While employers may ask staff whether they have Coronavirus symptoms, they should not ask unrelated questions, for example about underlying medical conditions, or symptoms not associated with Covid-19. The NHSX contact tracing app may help to control the virus but has privacy implications (p.8).

If home working and social distancing continues for the rest of the year for many, it will undoubtedly create a new work culture in some organisations. DPOs may become more reliant on webinars and online team meetings to exchange information. *Privacy Laws & Business* will soon launch a value-added way for you to connect with our expert consultants to address your specific questions during an initial half-an-hour consultation.

In this issue, to keep you well-informed, we bring you updates on AI legislative developments (p.16), how to choose your legal basis for adtech (p.22), the implications of the Supreme Court's Morrisons vicarious liability decision (p.24), top tips on managing data breaches (p.27), data protection issues for SMEs (p.20), DP issues in scientific research (p.29) and an interview with the ICO award winner (p.1).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access UK events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

> *PL&B UK Report* offers excellent guidance for Information Management professionals on the latest changes in data regulation, as well as useful advice on improving data security and protecting privacy.
>
> **Simon Baker, Nursing and Midwifery Council**

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 33rd year. Comprehensive global news, currently on 165+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.