High Court finds Morrisons vicariously liable for data breach

Joseph Jones and **Ruth Scoles Mitchell** of Covington & Burling LLP report on the UK's first successful privacy class action.

On 1 December 2017, the High Court of England and Wales found the fourth-largest supermarket chain in the UK, Wm Morrisons (Morrisons), vicariously liable for a data breach caused by the intentional criminal actions of one of its employees, namely the leaking of payroll information online.

The breach affected almost 100,000 Morrisons employees and the action, brought by 5,518 former and current employees, is considered to be the first of its kind in the United Kingdom. The data compromised in the breach included personal data such as names, addresses, and bank account details.

Facts

In March 2014, payroll data relating to almost 100,000 Morrisons employees was disclosed on a file-sharing website by a disgruntled Morrisons employee Andrew Skelton. Skelton had been entrusted by Morrisons with the data for the purpose of facilitating account auditing. He copied the dataset onto a personal USB drive and posted it to a file-sharing website. He was found to be criminally liable for the breach and was imprisoned for eight years for fraud, securing unauthorised access to data, and disclosing personal data.

A legal action seeking damages on behalf of 5,518 former and current Morrisons employees whose data was leaked was premised on Morrisons being either directly liable or vicariously liable[1] for Skelton's acts. The action alleged that Morrisons had committed a breach of statutory duty under the Data Protection Act 1998, among other things.

Direct liability

The High Court held that Morrisons was not directly liable for the breach. The judgment states that where a corporation "is in no sense responsible for authorising or requiring" the breach and the employee is acting against the employer's wishes in committing the breach, the liability may be vicarious but not direct (para. 49).

Vicarious liability

The High Court ruled that vicarious liability under the Data Protection Act 1998 may be applicable notwithstanding the fact that the Data Protection Act does not expressly refer to it. Citing past case law (*Majrowski* [2006 UKHL 34]), the High Court held that employers can be vicariously liable for the actions of their employees where an employee commits a breach of statutory obligations, while acting in the course of his employment, unless legislation expressly or impliedly indicates otherwise. Moreover, the High Court reasoned that vicarious liability could further the legislative purpose of the Data Protection Act: to protect the rights of data subjects.

On the facts of the case, the High Court found Skelton to have been acting "in the course of employment", adopting a broad interpretation of the scope of employment (consistent with past case law: *Bazely v Curry* [1999 174 D.L.R. 4th 45], *Lister* [2001 UKHL 22] and *Mohamud* [2016 UKSC 11]). Accordingly, Morrisons was held to be vicariously liable.

> The High Court held that employers can be vicariously liable for the actions of their employees.

In addition to the central issue of vicarious liability, the High Court addressed a number of other issues, including:

- **Security standards**. The High Court clarified that the fact that a level of security is available but has not been implemented does not — by itself — amount to a failure to reach an appropriate standard. Applying a balancing test is necessary. The High Court found that Morrisons had violated the security principle of the Data Protection Act 1998 by not having a policy for deletion of data held outside its normal secure repository. However that violation did not cause any loss nor did it enable Skelton's breach. On the facts of the case, therefore, the High Court found that Morrisons did provide "adequate and appropriate [security] controls".
- **Employee monitoring**. The High Court considered routine employee monitoring as needing justification on an individual basis. Active monitoring is not the norm in businesses such as Morrisons and may be deemed unnecessary in the context of its business.

Unhelpfully, the High Court did not resolve the dispute as to the burden of proof. In other words, it remains unclear whether a claimant needs to prove a violation of the Data Protection Act 1998 or whether the defendant needs to prove that its arrangements were appropriate.

Significance

The ruling could have widespread implications for employers and potentially lead to more actions of this kind. The ruling means that employers that may not have directly or actively breached their data protection obligations under UK data protection legislation may nonetheless be held to be vicariously liable for an employee's acts, notwithstanding that the employee acted independently and that it was not unreasonable for the employer to entrust the employee with the data.

Further, this liability is, apparently, not diminished by the fact that the employee's acts were deliberate and specifically intended to cause harm to the employer (as was the case on the facts for Morrisons and Skelton).

Interestingly, and at the end of the judgment, the judge indicated that he was "troubled" by the ruling as it could be interpreted as furthering the criminal aims of Skelton, specifically his aim to hurt his employer, Morrisons. The judge recognised that the issues raised were suitable for consideration by a higher court. Reports indicate that Morrisons will appeal.

This is possibly the UK's first data protection "class action", a trend which may increase from May 2018 when the EU General Data Protection Regulation rules come into force, including those contemplating collective actions for redress in respect of data breaches. The Regulation makes use of the EU concept of "undertaking", which in the competition law context has led to parent companies being held liable for the acts of their wholly owned subsidiaries.

AUTHORS

Joe Jones is an Associate and Ruth Scoles Mitchell is a trainee solicitor at the London office of Covington & Burling.
Email: jjones@cov.com

REFERENCES

1 Refers to a situation where someone is held responsible for the actions or omissions of another person.

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Organisations discuss how to demonstrate GDPR compliance

Companies are well on track with compliance programmes but different approaches to GDPR-readiness emerge. By **Laura Linkomies**.

A *PL&B* Roundtable, hosted by Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network, on 30 November 2017, was organised to facilitate peer-to-peer discussions with a small group on EU GDPR compliance. The next event in this series takes place in London on 31 January (more information at the end of the article).

A "business as usual" approach will not work in organising compliance with the GDPR. It is important to connect with the departmental managers who are responsible for

Continued on p.3

Practical handling of data breaches now and post-GDPR

Organisations need to prepare a response plan and take a joined-up approach when communicating with stakeholders. By **Richard Jeens** and **Mohan Rao** of Slaughter and May.

No one working in the data privacy space will have failed to notice that the number, scale and consequences of data breaches have all increased in recent months. Unsurprisingly this has led to many more "so what are we doing about it" questions from senior executives. The recent Morrisons' decision[1] and arrival in May this year of the GDPR, with its mandatory notification regime and significantly increased monetary sanctions, hardly calm the nerves. However, in our

Continued on p.5

Issue 95 **January 2018**

UNITED KINGDOM
report

ISSUE NO 95 **JANUARY 2018**

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.thomas@privacylaws.com

CONTRIBUTORS

Alison Deighton and Claire Saunders
TLT LLP

Rosalie Hayes
Bristows LLP

Richard Jeens and Mohan Rao
Slaughter and May

Joe Jones and Ruth Scoles Mitchell
Covington & Burling LLP

Patricia Gelabert
PL&B Correspondent

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

What about data transfers after Brexit?

The UK will become a third country after March 2019, the EU Commission stated earlier this month (p.23). The government's view is that adequacy should be easy to achieve as the UK is implementing the GDPR and has a long tradition in data privacy. Whether the EU's reminder is just a political message to get on with things, or implying that the UK regime has pretty strong surveillance powers, which could stand in way of an adequacy decision, is a matter of great interest to any company dealing with EU citizens' data.

Giving evidence to the House of Commons Home Affairs Committee in December, Elizabeth Denham, the Information Commissioner, said that she would favour a transition agreement to cover all personal data. This could be a bespoke agreement as part of the withdrawal negotiations. "The UK stands a very good chance at that kind of mutual recognition agreement in a transitional period, because there is no other country that is as close to the EU when it comes to the law," she said. "You could carve out law enforcement."

The House of Lords has pointed out that the UK Data Protection Bill does not mention data protection as a qualified fundamental right. To include that would also send the right message to the EU. The Lords, who are in favour of this amendment, are moving on to the third reading of the bill as we go to print. Several amendments have been made, see p.10.

For now, organisations are busy organising many aspects of GDPR compliance, for example data breach notification (p.1) and marketing. The future e-privacy regime is still being debated at European level, but organisations can rest assured that not everything will change (p.16).

In this issue we also report on Artificial Intelligence (p.14), and investigate training options for Data Protection Officers (p.19). Join us on 31 January in London for a peer-to-peer discussion on GDPR implementation, see www.privacylaws.com/events

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 1998, 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 future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
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.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

4. Back Issues
Access all the *PL&B UK Report* back issues since the year 2000.

5. Events Documentation
Access UK events documentation such as Roundtables with the UK Information Commissioner and *PL&B Annual International Conferences*, in July, Cambridge.

6. 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.

To Subscribe: www.privacylaws.com/subscribe

"I particularly like the short and concise nature of the *Privacy Laws & Business* Reports. I never leave home without a copy, and value the printed copies, as I like to read them whilst on my daily train journey into work."

Steve Wright, Data Privacy & InfoSec Officer, John Lewis Partnership

Subscription Fees

Single User Access

UK Edition **£440 + VAT***

International Edition **£550 + VAT***

UK & International Combined Edition **£880 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-10 users. Enterprise licence for 11+ users.

Subscription Discounts

Introductory 50% discount. Use code HPSUB (first year only) for DPAs, public sector, charities, academic institutions and small and medium companies.

Discounts for 2-year (10%) and 3-year (15%) subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

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

Privacy Laws & Business also publishes the International Report.

www.privacylaws.com/int