DATA CLASS ACTIONS
THE OUTLOOK AFTER *MORRISON*

Tim Leaver and Kate Macmillan of Herbert Smith Freehills LLP discuss the legal implications of the Supreme Court's decision in *Morrison* and the outlook for data class actions in the UK.

The first class action to be heard in the English courts following a cyber and data security incident came to its final conclusion on 1 April 2020, with the Supreme Court's ruling in *Various Claimants v WM Morrison Supermarkets Plc ([2020] UKSC 12; see News brief "Rogue employee's data breach: employers not vicariously liable in data class action", www.practicallaw.com/w-025-1936*).

Morrison has brought far greater clarity to the circumstances in which vicarious liability may apply in data protection class actions. It brings into sharp relief the highly topical challenge of striking a fair balance between the right to private and family life under Article 8 of the European Convention on Human Rights (Article 8) and an employer's right to engage in monitoring in order to ensure the smooth running of a company. *Morrison* also makes clear that data claims will continue to be pleaded in multiple causes of action, such as data protection, misuse of private information and breach of confidence, until this issue is addressed again either by legislators or the courts.

This article discusses the practical implications of *Morrison* in relation to vicarious liability, primary liability under data protection legislation and the questions that remain to be answered in terms of the future development of data protection class actions.

MORRISON DECISION

Morrison concerned a data breach by Mr Skelton, an aggrieved former employee of WM Morrison Supermarkets Plc, who copied and published the personal data of nearly 100,000 employees (*see box "The dispute in Morrison"*). A group of employees whose data were disclosed brought proceedings against Morrison claiming that it had primary liability for failing to protect their data and was vicariously liable for Mr Skelton's actions.

By the time the proceedings reached the Supreme Court, the questions that remained to be determined were whether Morrison was vicariously liable for Mr Skelton's actions and whether the Data Protection Act 1998 (DPA 1998) excluded vicarious liability in the circumstances of the case.

The court held that Morrison was not vicariously liable for Mr Skelton's actions of transferring his colleagues' private information onto his own private USB stick, removing it from the business and putting it into the public domain from home in order to cause his colleagues and employer harm. In reaching this conclusion, the court appeared to endorse the commonsense approach advocated by Morrison at the hearing; that is, that the case was analogous to an

The dispute in *Morrison*

Mr Andrew Skelton worked as an internal auditor at WM Morrison Supermarkets Plc. In 2013, he was given a verbal warning for minor misconduct, after which he was reported to harbour an irrational grudge against Morrison. In preparation for an external audit, Mr Skelton was given access to the payroll data of the whole of Morrison's workforce. This comprised employees' personal data, including their name, address, gender, date of birth, home telephone number, mobile telephone number, National Insurance number, bank account number and sort code, and salary.

On 18 November 2013, Mr Skelton copied the data onto an encrypted USB stick. On 12 January 2014, Skelton uploaded the data onto a publicly accessible file-sharing website. On 13 March 2014, Mr Skelton sent the data to local and national newspapers.

In July 2015, Skelton was found guilty at Bradford Crown Court of fraud offences under the Computer Misuse Act 1990 and under section 55 of the Data Protection Act 1998 (DPA 1998) and was jailed for eight years.

The Information Commissioner's Office (ICO) investigated and found no enforcement action was required with respect to Morrison's compliance with the DPA 1998. It was crucial to its decision that Mr Skelton had been trying to harm his former colleagues and employer in taking the information and putting it into the public domain. The ICO regarded Morrison as a victim.

Around 5,518 of Morrison's employees, 5.5% of those affected, brought a claim for damages. The claim was pleaded as a breach of statutory duty under the DPA 1998, misuse of private information and breach of confidence.

The High Court held that Morrison was not directly liable for the breach, either under the DPA 1998, for misuse of private information or for breach of confidence; however it was vicariously liable for Mr Skelton's actions (*[2017] EWHC 3113; see News brief "Vicarious liability for data breach: going rogue", www.practicallaw.com/w-012-8826*). The Court of Appeal dismissed Morrison's appeal (*[2018] EWCA Civ 2339; see News brief "Morrisons' liability for rogue employee: an apple of discord", www.practicallaw.com/w-017-7358*).

The Supreme Court upheld Morrison's further appeal, holding that Morrison was not vicariously liable for Mr Skelton's actions (*see News brief "Rogue employee's data breach: employers not vicariously liable in data class action", www.practicallaw.com/w-025-1936*).

employee on the meat counter stealing a knife and using it to commit the criminal act of murder outside the workplace. Just as no one would hold Morrison responsible in those circumstances, it should not be held responsible for its employee's misuse of data to cause harm.

The court rejected Morrison's contention that the DPA 1998 excludes the imposition of vicarious liability for data breaches under the DPA 1998 and for the misuse of private information or breach of confidence. The court stated that the imposition of a statutory liability on a data controller is not inconsistent with the imposition of a common law vicarious liability on their employer. This is the case both for the breach of duties imposed by the DPA 1998 and for the breach of duties arising under the common law or in equity. Since the DPA 1998 is silent on the position of a data controller's employer, there is no inconsistency between the two regimes (*see box "Interplay between statute and common law"*).

VICARIOUS LIABILITY

The Supreme Court's judgment in *Morrison* was handed down on the same day that it handed down another decision on vicarious liability in *Barclays Bank plc v Various Claimants (*[2020] UKSC 13; *www.practicallaw.com/w-025-1830*). In *Barclays*, the court upheld an appeal from the Court of Appeal, finding that Barclays was not vicariously liable for the actions of a doctor whom it had engaged to carry out medical examinations on new employees and who had allegedly sexually assaulted those employees.

Both decisions could be seen as a handbrake turn in the law on vicarious liability. The lower courts' rulings seemed to indicate a clear direction of travel down a rocky road for employers, with somewhat smoother sailing for claimants. That journey has seemingly now reached a dead-end.

Legal origins

The original 17th century concept of a master being responsible for the acts of their servant changed over the subsequent centuries to embrace developing concepts of companies having their own legal personality. With that came an acceptance that, because the commercial success of a company can largely be attributable to the acts of its employees, companies should take the risk when things go wrong in the course of employment.

From these concepts were born the main themes on which the modern law of vicarious liability was developed. Firstly, that an entity that commercially benefits from the acts of its employees can, and should, also generally be strictly liable for their wrongdoing at work. Secondly, that in certain cases, liability should be displaced where the individual was not carrying out the relevant act in the furtherance of their employer's business; in other words when they went off "on a frolic of their own".

Over time, case law established a two-stage test to determine vicarious liability; that is, whether:

- The relationship between the wrongdoer and the employer is capable of giving rise to vicarious liability.
- The connection between the employment or other relationship and the wrongful conduct makes it just and reasonable to hold the employer legally responsible for the consequences of the wrongdoer's conduct.

Expansion of the test

Cases over the past 20 years appeared to suggest the court's increasing willingness to expand the application of both limbs of the test, perhaps in part due to the fact that many of the cases that came before the courts concerned sexual assault or physical violence where the desire to compensate the victim was entirely understandable.

Interplay between statute and common law

The second issue before the Supreme Court in *Various Claimants v WM Morrison Supermarkets Plc* was whether the Data Protection Act 1998 (DPA 1998) excludes vicarious liability (*[2020] UKSC 12*). Morrison argued that the DPA 1998 imposes direct liability only where an organisation has failed to take reasonable care, and therefore it would be unfair to impose vicarious liability on the facts in *Morrison*. The court found this argument unpersuasive. Noting that it was not strictly necessary to consider the point, given the court's decision on vicarious liability, the court felt that it was desirable for it to express a view as full argument on the topic was heard.

The court noted that the DPA 1998 is silent on the position of a data controller's employer. In light of this, imposing statutory liability on a data controller like Mr Skelton was not inconsistent with the co-existence of vicarious liability at common law, whether for breach of the DPA 1998 or for a common law or equitable wrong. This confirms that if primary liability is not available in a data protection case, vicarious liability may still be available. The position is the same as in negligence, for example, where there is a fault-based test for primary liability and a strict liability test in vicarious liability.

There is likely to be a period of time where claimants continue to bring claims in multiple causes of action, as was the case in *Morrison*, and where the courts seek to align various causes of action protecting the right under Article 8 of the European Convention on Human Rights to respect for one's private and family life, home and correspondence.

Furthermore, *Morrison* was decided under the DPA 1998 so it is unknown if the decision would be the same under the General Data Protection Regulation (*2016/679/EU*) (GDPR). At some point in the future, a claimant may run the argument that the GDPR and the Data Protection Act 2018 exclude vicarious liability on the basis that the GDPR is a more exhaustive code than the Data Protection Directive (*1995/46/EC*), which underpins the DPA 1998. A counter argument could be that vicarious liability is not incompatible with the GDPR and supports the GDPR's aim of bolstering enforcement of the rights contained in it: there is no explicit exclusion of vicarious liability under the GDPR. Either way, it still leaves the issue that vicarious liability could exist under a parallel cause of action.

The first limb. In many of these cases, the wrongdoer had a different type of relationship from that of a simple employment, yet vicarious liability was established on the basis that it was sufficiently akin to employment. For example, in *Cox v Ministry of Justice* the Supreme Court held that the prison service was vicariously liable for the negligence of a prisoner who had accidentally injured an employee while working in the prison kitchens, given that the prisoner worked as an integral part of the prison service's catering business and the risk of the accident was created by assigning those activities to him (*[2016] UKSC 10*).

In *Various Claimants v Catholic Child Welfare Society and others* (also known as *Christian Brothers*), the Supreme Court set out five factors that are relevant in determining whether an employer should be liable for the acts of individuals who are not employees (*[2012] UKSC 56*). These are whether:

- The employer was more likely to have the means to compensate the victim than the wrongdoer, and could therefore be expected to insure against liability.
- The conduct was committed as a result of activity undertaken on behalf of the employer.
- The conduct was likely to be part of the employer's business activity.
- The employer created the risk of the wrongful act being committed by engaging the wrongdoer.
- The wrongdoer was under the control of the employer.

In setting out these factors, the court stated that the law of vicarious liability "is on the move", which the Court of Appeal in *Barclays* took as an invitation to expand this first limb yet further. It rejected the idea that there is a "bright line" test prohibiting vicarious liability for the acts of an independent contractor, holding instead that there can be liability where a consideration of the identified factors makes this appropriate.

The second limb. The second limb of the test was formulated in Salmond on Torts (1907) as applying vicarious liability for either:

- A wrongful act authorised by a master.
- A wrongful and unauthorised mode of doing some act authorised by a master where the unauthorised act is so connected with authorised acts that it should be viewed as an improper mode of doing an authorised act.

However, it was too much of a stretch to view deliberate acts of misconduct as improper modes of carrying out authorised duties so, in order to accommodate these cases, the focus changed to whether the wrongful conduct was so closely connected with authorised acts that it could fairly and properly be regarded as done in the ordinary course of employment (*Lister v Hesley Hall Ltd [2001] UKHL 22; Dubai Aluminium Co Ltd v Salaam [2002] UKHL 48, www.practicallaw.com/4-102-2674*). As the Supreme Court explained in *Mohamud v William Morrison Supermarkets plc*, this requires an analysis of the field of activities that the employee was employed to do and the degree of connection between the employee's role and their wrongful conduct (*[2016] UKSC 11; see News brief "Vicarious liability in the workplace: Supreme Court delivers a blow for workers", www.practicallaw.com/2-625-0789*).

However, this still leaves the courts with considerable discretion in determining how broadly to construe the field of activities and what constitutes a sufficient degree of connection between those activities and the wrongful conduct. In *Mohamud*, the Supreme Court held that Morrison was liable when its sales assistant at a petrol station, Mr Khan, left the sales kiosk and subjected Mr Mohamud to a violent physical attack and racist abuse while on the forecourt. As Mr Khan's conduct arose from his position serving customers, Morrison was held vicariously liable even though Mr Khan's role

did not encompass dealing with customers away from the kiosk or using any level of force. The court commented that:

- The connection between the field of activities and the wrongful conduct must be sufficiently close to make it right for the employer to be held liable under the principle of social justice.
- The assault was part of an unbroken sequence of events, starting at the sales kiosk.
- It was irrelevant that Mr Khan was motivated by personal racism rather than a desire to benefit Morrison's business.

The Court of Appeal in *Morrison* relied heavily on these comments in *Mohamud* as establishing that the motive of the wrongdoer is irrelevant and that social justice is a driving force in determining where the boundaries of the test should be set.

Following the Court of Appeal judgments in *Morrison* and *Barclays*, employers found themselves in a situation where they could potentially be liable for the acts not only of their employees, but also for the acts of independent contractors whom they had engaged. Further, they seemingly were on the hook even where an individual was deliberately doing something to harm someone, as long as there was a sufficient connection to the part of the job that they were paid to do and even where the sole intention of the wrongdoer was to harm the employer.

Key principles from *Morrison* and *Barclays*

Five key principles can be extracted from *Various Claimants v WM Morrison Supermarkets Plc* and *Barclays Bank plc v Various Claimants* (*[2020] UKSC 12; [2020] UKSC 13*).

Independent contractors. Following *Barclays*, there is no vicarious liability for the acts of an independent contractor carrying on business on their own account. The *Christian Brothers* factors will be relevant only in doubtful cases to decide whether those who are neither in business on their own account nor employees are effectively part and parcel of the employer's business so as to make it fair, just and reasonable to impose vicarious liability (*[2012] UKSC 56*).

Close connection. Following *Morrison*, the act of the wrongdoer needs to be so closely connected to acts that they were authorised to do that, for the purposes of vicarious liability, their actions may fairly and properly be regarded as being done while acting in the ordinary course of their employment. Within this concept must come a further consideration of whether the employee was engaged in furthering their employer's business.

Motive. The employee's motive is highly relevant. If their motive is to harm the employer, the employer will not be vicariously liable. If the employee is motivated by something other than furthering their employer's business, this may exempt the employer from liability. The Supreme Court in *Morrison* suggested that a more tailored version of the close connection test may be applicable for sexual abuse cases, where the employer's conferral of authority on the wrongdoer over the victims will be more relevant.

Social justice. Social justice should play little or no part in the determination of whether an employer should be held vicariously liable for the acts of an employee. However, the Supreme Court in *Morrison* noted that, from a social justice perspective, Morrison had reacted extremely quickly in shutting down access to the data and had spent around £2 million in ensuring that it did everything it reasonably could to rectify the situation, including spending significant sums on measures for the prevention of identity theft for its affected employees.

Timing. Temporal proximity of the wrongful actions to a properly authorised act is not sufficient to establish vicarious liability.

All change

In *Morrison* and *Barclays*, the Supreme Court gave a somewhat damning critique of the Court of Appeal and lower courts, saying that they had misunderstood the principles of vicarious liability and misinterpreted the earlier precedents, including the Supreme Court's decision in *Mohamud* (*see box "Key principles from Morrison and Barclays"*).

In *Morrison*, the Supreme Court explained that its comment in *Mohamud* in relation to motive was simply addressing the point that it was irrelevant why the wrongdoer, Mr Khan, had become violent while acting on his employer's business. Equally, the comment on the unbroken chain of events was a relevant factor in determining whether Mr Khan was still acting in the course of employment, and is not a touchstone for liability. The allusion to principles of social justice was simply an allusion to the reason for developing the general vicarious liability doctrine in the 17th and 18th centuries, and it was the principles as elucidated by subsequent case law that should guide the courts rather than their own instincts for social justice.

Likewise, in *Barclays*, the Supreme Court held that the Court of Appeal had erred in considering the *Christian Brothers* factors in order to decide that Barclays was vicariously liable for sexual assaults carried out by the doctor whom it had engaged as an independent contractor.

Future challenges

One of the challenges in the future will be how to distinguish between an employee acting in order to harm their employer or with some other personal motive, in which case there would be no vicarious liability, and an employee who is hugely misguided about an appropriate way to act but who is still acting to further the interests of their employer, in which case there would be vicarious liability. Furthermore, an employee might have a joint motive of wanting to harm their employer and something more benign. Often, there will be few clues about an employee's state of mind. The fact that motive may be the distinguishing factor as to whether a victim can successfully claim against an employer presents real practical difficulties. It seems too uncertain to be satisfactory.

It is also a moot point whether *Morrison* means that *Mohamud*, in which it was suggested that the wrongdoing was racially motivated, would be decided differently today. This will depend on how broadly the concept of motive

is interpreted and whether discriminatory attitudes can be viewed as separate from an underlying purpose of actions. The Supreme Court in *Morrison* viewed the wrongdoer in *Mohamud* as still going about his employer's business, rather than pursuing private ends, suggesting that racism is not in itself to be viewed as a personal purpose. The racist nature of the abuse did not change the fact that the purpose of dealing with the customer was for the employer's business.

PRIMARY LIABILITY

The underlying events of the dispute in *Morrison* arose when the DPA 1998 was in force. The DPA 1998 was superseded by the DPA 2018 on 23 May 2018. Under data protection principle 7 of the DPA 1998, organisations were required to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The question of whether measures were appropriate related to the state of technological development and the cost of implementing any measures, as well as the harm that might result from any unauthorised or unlawful processing, or accidental loss, destruction or damage, and the nature of the data that were protected. This obligation included taking reasonable steps to ensure the reliability of any employees who had access to personal data.

As the High Court in *Morrison* held that Morrison was not primarily liable, the hearings in the Court of Appeal and Supreme Court focused only on vicarious liability.

High court decision

In *Morrison*, the High Court held that Morrison had not failed to provide appropriate controls, save in respect of deletion. In short, it had taken the reasonable care expected of it. The court considered specifically whether Morrison could have stopped Mr Skelton's wrongdoing if it had noticed that he was researching the "Tor" database in order to access the internet with a concealed identity or that he was removing the data from the internal system to a laptop.

Internet searches. The court held that the fact that Morrison did not routinely scrutinise employees' internet searches did not mean that it fell short of the expected standards. The court noted that firewalls blocked undesirable material and an automatic filter restricted access to dubious websites. It also noted that most companies allow employees to access the internet for personal reasons, within reason, provided that it does not conflict with their duties. The resources that would be needed to conduct routine active monitoring would be disproportionate (*see box "Employee monitoring"*).

Data removal. The court held that Morrison did not fall short of the standard expected by allowing the data to be removed from its

Employee monitoring

Given that employers may be held strictly liable for an employee's wrongful actions, the temptation may be to increase levels of monitoring of employee activity both to detect and dissuade misconduct. A fair balance must be struck between individuals' rights to privacy and family life under Article 8 of the European Convention on Human Rights, which courts and tribunals must respect when applying domestic law, and an employer's right to take steps to ensure the smooth running of its business and supervise its employees' use of technology (*Barbulescu v Romania [2017] ECHR 754; see News brief "Workplace privacy: striking a balance", www.practicallaw.com/w-010-4936*).

In Europe, the UK comes in at the more permissive end of the employee monitoring spectrum (*see feature article "Employee monitoring: the value of being prepared", www.practicallaw.com/3-629-9945*). Broadly, monitoring is largely defensible provided that appropriate policies and training are in place, and that the monitoring is undertaken: on a proportionate basis; by restricted personnel; and in ways and for reasons that have clearly been spelled out to employees in advance. In contrast, a number of other European jurisdictions strictly prohibit monitoring of any kind and, indeed, make it a criminal act.

The High Court ruling in *Morrison* is helpful on how employers should treat employees who are sanctioned following a disciplinary process (*[2017] EWHC 3113*). The court rejected robustly the suggestion that someone should be supervised to a greater degree following disciplinary sanction. The court took the view that Mr Skelton's sending of personal items (a white powder, which caused alarm when it leaked through the packaging) through the business's post room showed no more than that he was, on one occasion, thoughtless. The court said that this did not provide a basis on which it could be supposed that Mr Skelton could not be trusted.

However, prevention is better than cure and employers will want to take reasonable steps to reduce the instances of employee misconduct; for example, by:

- Providing workforce education and training on proper data handling and the potential criminal consequences of any wrongdoing.
- Informing employees that the employer has systems and controls in place to both detect wrongdoing and to prevent it.
- Investing in tools and technologies to ensure that appropriate restrictions are in place, for example to: prevent the downloading, uploading or emailing of quantities of data or particular data types; and capture emails using data loss prevention technologies before transmission where the data being sent, or the recipient, appear unusual.
- Putting in place absolute prohibitions and blocks in terms of the use of USB sticks and hard drives, as well as restrictions on access to webmail and cloud storage from work systems.
- Water-marking documents to ensure that any data that are disseminated when they should not have been are name and time-stamped.

database and put onto a laptop. The court accepted Morrison's evidence that this left the data no less secure than they had been while in its database. However, the court recognised that where data are held outside the usual secure repository, there may be an unnecessary risk of inadvertent disclosure.

Deletion. The court found that Morrison had fallen below the standard expected in relation to deletion. Although the failure did not cause harm in this instance and therefore did not lead to an adverse finding on primary liability, the case provides useful guidance on deletion. After *Morrison*, it seems clear that the court will expect employers to have a failsafe and organised system for the deletion of data in similar circumstances.

The court's decision that deletion should have occurred is likely to be the same under the General Data Protection Regulation (*2016/679/EU*) (GDPR), which requires data to be:

- Processed in a manner that ensures appropriate security, including against unauthorised or unlawful processing (*Article 5.1(f)*).
- Kept for no longer than is necessary for the purposes for which the personal data are processed (*Article 5(1)(e)*).

GDPR implications

Morrison demonstrates the operation of an exemption from primary liability in the DPA 1998 regime. Under Article 23(2) of the Data Protection Directive (*1995/46/EC*) (the Directive), a data controller may be exempt from liability if it can prove that it was not responsible for the event giving rise to the damage. The High Court in *Morrison* accepted that Morrison fell within this exemption and so it was not primarily liable.

The provisions on liability in the GDPR broadly mirror the provisions under the Directive. Article 82(3) of the GDPR (Article 82) provides that a controller or processor will be exempt from liability if it can prove that it is not in any way responsible for the event giving rise to the damage.

An important question is where the burden of proof lies in cases about primary liability. In *Morrison*, the claimants argued that the burden was on Morrison to prove that its arrangements were appropriate. Morrison argued that it was for claimants to prove any breach of the data protection principles. Sadly, the High Court declined to resolve the issue, saying that it had not needed to depend on the burden of proof in making its decision.

At first sight, the burden of proof being on the claimant presents considerable difficulties. If many entities are involved in processing data, it may be hard to show who is responsible for any unlawful act and to prove causation. However, reliance on common design might provide the answer in practice. Indeed, the GDPR already contemplates this in the context of controller and processor relationships. Article 82 deals with which entity should pay compensation in any case in which primary liability is established. Broadly, controllers and processors will be jointly and severally liable where they are both responsible for damage caused by their processing. Where one party pays all the compensation for the damage, it can claim back relevant amounts from the other party or parties.

Causation is still an issue in many data protection cases as the data protection legislation does not follow a model like the one in EU and UK competition law which allows for follow-on litigation after an adverse finding by a regulator. This means that anyone bringing a competition claim based on an adverse regulatory finding does not have to establish liability and can move straight to issues of causation and loss in court.

Under the accountability principle in Article 5(2) of the GDPR, controllers are required to demonstrate compliance with Article 5(1), which provides that data must be processed in a manner that ensures the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Article 32 of the GDPR requires controllers and processors to implement appropriate technical measures to ensure a level of security appropriate to the risk.

It could be argued that, as a result of these provisions, the GDPR shifts the burden of proof in data claims from the data subject to the data processor. In practice, this means that it is prudent for organisations to be prepared to demonstrate that they have met the requirements of Article 32 of the GDPR in relation to security of processing. This is a requirement under the accountability principle in any event. There will be considerable debate and expert evidence about what was or was not appropriate to the risk in any particular case, as well as what constituted the state of the art at the time.

It would also be prudent to put considerable effort into avoiding adverse findings by regulators as even though the regulators' decisions are not binding, in practice they will be relied on heavily in any litigation following a cyber or data security incident. There has been a recent increase in legal challenges to the Information Commissioner's Office (ICO). In March 2020, it was reported that around 60 cases were due to be heard by the First-tier Tribunal under the DPA 2018 and the Freedom of Information Act 2000. The data protection appeal cases included Doorstep Dispensaree's appeal against the ICO's first GDPR fine of £275,000 and Heathrow Airport Limited's appeal against a £120,000 fine. Another marker of increased contentious activity in relation to regulatory activity is that, in late 2019, the ICO reported that it had been forced to get a £600,000 bail out from the Treasury to meet increased legal and professional services expenditure (*www.decisionmarketing.co.uk/news/senior-judge-suspends-all-appeals-against-ico-rulings*).

THE FUTURE

Unfortunately, *Morrison* sheds little light on how data class actions will develop in the future and many questions remain to be answered; in particular, how issues of quantum will be decided and how data class actions will be managed.

Quantum

Any person who has suffered material or non-material damage as a result of an infringement of the GDPR has the right to receive compensation from the controller or processor (*Article 82(1)*). Given that so much of the GDPR is as yet untested, particularly with respect to large class action claims resulting from GDPR non-compliance, there is little case law regarding the issue of quantum for Article 82 compensation. Only a handful of cases across the EU have so far considered the issue, and none of those have been in the context of a class action style claim. The very limited successful claims have been in the region of only a few hundred euros.

In considering how quantum will be measured, including with respect to a GDPR compensation claim, the big questions are around non-material damage; for example,

whether mere loss of control of data constitutes damage and whether loss of control is separate from distress. From the EU cases to date, the German and Austrian approach has seemed to suggest that mere data protection non-compliance may not be enough to justify compensation unless it also intervenes in the emotional sphere of the data subject. The Dutch courts, in contrast, seem to have adopted a more liberal approach to non-material damage, although the quantum of the awards has been quite low.

The recitals to the GDPR point to loss of control as a non-material damage. Recital 85 to the GDPR seems to identify it as a separate type of damage, although it was drafted with breach notification in mind. It states that a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons, such as loss of control over their personal data. While recitals do not comprise legal obligations, the European Court of Justice (and presumably the UK courts after the Brexit transition period has ended) will use them to establish what the GDPR means in the context of a particular case.

The best guidance on loss of control and distress comes from the jurisprudence on the closely related cause of action of misuse of private information. Broadly, data protection legislation protects against the unauthorised or unlawful processing of data while the tort of misuse of private information protects: the right to control the dissemination of information about one's private life; and human autonomy and dignity.

In 2015, the Court of Appeal specifically considered loss of control in the telephone hacking case, *Representative Claimants v MGN Limited* (*[2015] EWCA Civ 1291*) (also known as *Gulati*). The court noted that privacy is a fundamental right, citing the House of Lords in *Campbell v MGN*, which emphasised that privacy "lies at the heart of liberty in a modern state" (*[2004] UKHL 22; see News brief "Breach of confidence: Naomi Campbell appeal", www.practicallaw.com/3-102-8134*).

The Court of Appeal in *Gulati* noted that the jurisprudence of the European Court of Human Rights had not limited damages to only damages for distress on the basis that protection for the right to respect for private life had to be practical and effective, and that to confine damages to damages for distress would be inconsistent with this (*[2002] EWCA Civ 1372*). It also noted that, in *AAA v Associated Newspapers Ltd*, the High Court awarded substantial damages for photographing a child even though the child was considered to be too young to be able to suffer distress (*[2012] EWHC 2103 QB*).

The Court of Appeal in *Gulati* rejected the argument that in a case of breach of privacy rights, the court should award damages only for distress and injury to feelings, and not for the fact of intrusion into a person's privacy, autonomy or dignity. It held that by misusing private information, MGN had deprived the respondents of their right to control the use of private information and they were entitled to be compensated for this in addition to any distress.

Misuse of private information has built-in safeguards in relation to claims for damages in respect of minor misuses of private information, in the form of the threshold requirement of seriousness and the balancing exercise. The concept of a threshold of seriousness is common to other laws protecting the Article 8 right; for example, the Defamation Act 2012 provides a statutory bar to cases where the threshold of seriousness is not met.

On this basis, the English courts may award damages for loss of control in data protection cases by analogy, although quantum may not be very high, particularly if the information was available to the public elsewhere. It has been noted that some of the information removed from systems in large data breach cases was on sale on the dark web before the personal data breach.

The Court of Appeal in *Lloyd v Google LLC* considered the issue of damages for loss of control of data with reference to the DPA 1998 (*[2019] EWCA Civ 1599; see News brief "Data protection claims: a green light for representative actions", www.practicallaw.com/w-022-5323*). The High Court had held that none of the represented class had suffered damage under section 13 of the DPA 1998 and, even if they had, neither the breach of duty nor the impact of it was uniform across the entire class. However, the Court of Appeal held that, in principle, damages are capable of being awarded for loss of control of data even if there is no financial loss and no distress.

The practical effect of this is that damages for loss of control will be the lowest common denominator. They will not factor in the volume of data or level of distress involved, which may create difficulties for claimants attempting to recover additional losses.

In reaching its decision in *Lloyd*, the Court of Appeal referred back to *Gulati*. While acknowledging that *Gulati* was not strictly binding on the court as it was not a decision on the DPA 1998, it said that it was applicable by analogy, for three main reasons:

- Both the misuse of private information and section 13 of the DPA 1998 derive from the same core rights to privacy.
- Since loss of control over telephone data was held to be damage for which compensation could be awarded in *Gulati*, it would be wrong in principle if the representative class's loss of control over browser-generated information could not likewise be compensated for the purposes of the DPA 1998.
- The EU law principles of equivalence and effectiveness pointed to the same approach being adopted to the legal definition of damage in the two torts, which both derive from a common EU right to privacy.

On 1 March 2020, the Supreme Court granted permission to appeal *Lloyd* on the issue of whether a uniform per capita amount of compensation can be awarded for a non-trivial breach of the DPA 1998 even if the breach causes no material damage or distress. This reference to "non-trivial" in the grounds of appeal is extremely important. It is trite law that the de minimis threshold applies to loss of control damages claims in data protection and this was accepted by both parties in the case. This means that if the infringement was trivial or de minimis the court would not make an award of loss of control damages.

It is likely to be argued that breaches which are accidental, one off and quickly remedied should fall into the trivial category. In addition, claims for trivial breaches may be vulnerable to be struck out as an abuse of process. For example, in *Jameel (Yousef) v Dow Jones & Co Inc*, the Court of Appeal stayed a defamation claim as an abuse of process on the basis that the damage caused was minimal, so any vindication would be minimal and the costs of obtaining it disproportionate (*[2005] EWCA Civ 75; www.practicallaw.com/4-200-5517*).

Related information

This article is at practicallaw.com/w-026-2617

Other links from uk.practicallaw.com/

Topics

Compliance: data protection	topic/1-616-6178
Data protection: general	topic/1-616-6550
Data security	topic/8-616-6189
Employee data and monitoring	topic/5-200-0623
Privacy	topic/6-383-8687
Rights of data subjects	topic/6-616-6190

Practice notes

Data Protection Act 2018: overview	w-014-5998
Data security under the GDPR	w-013-5138
Data subject rights under the GDPR	w-024-3178
Demonstrating compliance with the GDPR	w-005-2644
GDPR and DPA 2018: claims for compensation	w-018-4325
GDPR and DPA 2018: derogations and exemptions	w-014-6104
GDPR and DPA 2018: enforcement, sanctions and remedies	w-005-2487
Monitoring employees	3-200-4245
Overview of privacy law	1-507-0879
Privacy law: alternative causes of action to claim for misuse of private information	2-507-2571
The GDPR and Data Protection Act 2018: data subject rights in the workplace	w-011-1458
The GDPR and Data Protection Act 2018: employer obligations	w-010-3418
Vicarious liability	3-521-4527

Previous articles

GDPR in the context of litigation: the jury's still out (2019)	w-021-5280
GDPR one year on: taking stock (2019)	w-020-0982
Class actions in England and Wales: key practical challenges (2018)	w-015-9333
Data use: protecting a critical resource (2018)	w-012-5424
Employee monitoring: the value of being prepared (2016)	3-629-9945
Cyber security: top ten tips for businesses (2016)	3-621-9152
General Data Protection Regulation: a game-changer (2016)	2-632-5285

For subscription enquiries to Practical Law web materials please call +44 0345 600 9355

Class action process

Another question, which is linked closely to the issue of damages, is how data class actions will be managed in the future. Generally, they have been brought under the group litigation order (GLO) procedure, as was the case in *Morrison*.

The court will make a GLO under Part 19.11 of the Civil Procedure Rules (CPR) (Part 19) to provide for the case management of claims that give rise to common or related issues of fact or law. A judgment or order in relation to one or more GLO issues is binding on the parties to all other claims that are on the group register at the time unless the court orders otherwise.

The downside of GLOs is that damages are assessed for each individual. However, in reality, once damages for certain types of claims have been established, many claims settle within the bracket that has been seen in similar types of cases.

To bring a claim under the representative action procedure, which is set out at Part 19.6, it must be demonstrated that the whole class has the "same interest" in the claim, which case law has shown means at all stages of the proceedings and not just at the date of judgment at the end.

In *Lloyd*, the courts considered whether data class actions can be brought using the representative action procedure. The High Court held that the members of the class did not have the same interest within Part 19.6(1) to justify allowing the claim to proceed as a representative action. As well as being troubled by the damages point (*see "Quantum" above*), it was concerned about the practical difficulties of identifying the individuals. The court said that the class definition must be workable and conceptually sound, and did not think much of Mr Lloyd's proposal to identify the individuals through disclosure from Google or self-certification.

The Court of Appeal disagreed. It took the view that the High Court had applied too stringent a test of "same interest", partly because of its determination as to the meaning of "damage". The court held that the members of the class did have the same interest under Part 19.6 (1) and were identifiable. They had the same interest as the wrong was the same and the loss claimed was the same.

As with the loss of control point, the issue of whether the High Court was right to hold that the members of the class did not have the same interest under Part 19.6(1) and were not identifiable is now going to the Supreme Court in *Lloyd*.

Viability of data class actions

The issues that come with data class actions inevitably lead to the question of whether it is worth bringing them before the court.

Judicial views. The High Court in *Lloyd* seemed keen to discourage data class actions, with the CPR overriding objective seemingly uppermost in its consideration. As the Court of Appeal in *Lloyd* noted, the High Court took into account the likely costs, the court time required and that the compensation that individuals were likely to recover would be modest at best. The High Court noted that the main beneficiaries of any award would be the litigation funders and the lawyers. The judge in the High Court was Mr Justice Warby, who was appointed Judge in Charge of the Media and Communications List in 2017. Given Mr Justice Warby's position and his extensive experience in information law at the bar, this view must carry weight.

Litigation funding. An important factor in whether this type of class action will take off is litigation funding. The number of individuals who may be eligible for loss of control damages will be key. Funders will be looking for a reasonable sum at the end of the litigation to make the pursuit of claims worthwhile. This is likely to be available only where liability is established and millions of individuals can claim damages for loss of control.

Insurance. After-the-event (ATE) insurance is a particularly tricky issue since claimants are likely to be reluctant to proceed without ATE insurance. Since 2013, when the Legal Aid, Sentencing and Punishment of Offenders Act 2012 ended the recovery of so-called additional liabilities in civil litigation generally, including ATE insurance premiums and conditional fee agreement uplifts, it has not been possible to recover ATE insurance premiums in data protection claims. If damages are insufficient to cover ATE premiums, ATE insurance is unlikely to be forthcoming.

Type of damages. Article 79 of the GDPR gives data subjects the right to an effective judicial remedy where their rights under the regulation have been infringed. If damages for loss of control damages do not deliver that remedy, other types of damages may do so. Some claims will be obviously worthwhile, for example, incidents that have led to more tangible harms such as discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage. In *TLT and others v Secretary of State for the Home Department*, when a spreadsheet was published online containing the data of individuals who had failed in their asylum applications, six claimants were awarded £39,500 for breaches of the DPA 1998 and misuse of private information (*[2016] EWHC 2217 (QB)*). That breach led to some individuals having genuine fears either for their own safety or the safety of family members in their country of origin.

***Lloyd* appeal.** There may be a pause in data class action activity pending the Supreme Court decision in *Lloyd*, which is expected to be heard late in 2020 or early 2021. The third ground of appeal that the Supreme Court will be considering, in addition to the loss of control and same interest points outlined above, is whether the Court of Appeal was wrong to interfere with the High Court's discretion in ruling that the claim should not be permitted to proceed under Part 19.6 as a representative action.

The withdrawal of the *Atkinson v Equifax Ltd* representative class action after the service of the defence hints at a change in confidence levels on the part of those on the claimant side (*Claim Number QB-2019-003524*). That claim was commenced by Mr Atkinson days after the judgment in *Lloyd* on the representative action basis under Part 19.6, claiming damages for loss of control of his personal data caused by Equifax's alleged failure to maintain appropriate security. Mr Atkinson's solicitors said that the claim was brought on behalf of 15 million people affected by the September 2017 cyber attack on Equifax US.

Looking ahead

In terms of the future of data class actions, there is still a lot to play for. A number of questions remain, including: whether damages will be available for mere loss of control and, if so, how quantum will be measured; how quantum in damages for distress may develop; and whether representative action data claims will take off. It is clear that the Supreme Court has important public policy issues to consider.

Tim Leaver is a partner, and Kate Macmillan is a consultant, at Herbert Smith Freehills LLP. *The authors would like to thank other members of the data class actions team, partners Andrew Moir, Miriam Everett and Julian Copeman, for their assistance with this article.*