Data protection claims: A fragmented future?

Contents

Introduction

Not so long ago, following the Court of Appeal's judgment in the seminal case *of Lloyd v Google LLC* [2019] EWCA Civ 1599, commentators and media outlets predicted an era where organisations would be submerged in a rising tide of US-style 'class-action' data breach claims.

On the contrary, 2021 has given us three recent cases which have decisively reshaped the likely future landscape of these claims. They are:

1. *Darren Lee Warren v DSG Retail Limited* [2021] EWHC 2168 (QB)
2. *Alan Rolfe & Ors v Veale Wasborough Vizards LLP* [2021] EWHC 2809 (QB)
3. *Lloyd v Google LLC* [2021] UKSC 50

The most significant case of the three, of course, is the much-anticipated judgment of the Supreme Court in the *Lloyd v Google* litigation. We discuss them all in this white paper, before concluding with our thoughts on the likely future of data breach claims, including how organisations can prepare for them.

Case one: Warren v DSG Retail
Limited causes of action in a 'cyberattack' case

The background facts:

The cyberattack which hit DSG Retail (known for operating the Currys PC World and Dixons Travel brands) between 24 July 2017 and 25 April 2018 resulted in the infiltration of DSG's systems, including over 5,000 point of sale terminals, by cybercriminals. The Information Commissioner's Office (ICO) investigated the incident and found DSG Retail's data security to be insufficient, issuing a Monetary Penalty Notice (MPN) in the amount of £500,000 (the maximum penalty that could be imposed at the time, as the incident had occurred before the GDPR came into force).

Mr Warren, who had purchased goods from Currys PC World, had his personal data compromised in the incident. He brought a claim for £5,000 for his distress against DSG Retail, raising a number of potential causes of action, including:

- Breach of confidence (BoC)
- Misuse of private information (MoPI)
- Breach of the Data Protection Act 1998 (DPA 1998)
- The common law doctrine of negligence

The decision

In July of this year, the High Court considered a summary judgment and/or strike out application brought by DSG Retail in respect of Mr Warren's claims, save for the claim arising out of the alleged breach of the data security duty (DPP7) under the DPA 1998. DSG Retail argued the BoC, MoPI and negligence claims had no realistic prospects of success and/or were not tenable as a matter of law.

The negligence claim can be dealt with shortly, as there is no tenable claim where there is a specific statutory regime available to the Claimant (as in this case, the DPA 1998 regime). The judgment of the High Court on the BoC and MoPI claims is more interesting.

Mr Justice Saini, handing down the judgment, agreed with DSG Retail. There was no dispute that Mr Warren's claims all arose from the cyberattack itself. The 'wrong' which is said to have happened to the Claimant was a failure of security, allowing the cybercriminals to access his personal data. However, it was not alleged that this failure was a positive act by the Defendant, DSG Retail – which, as the Judge would go on to say, is necessary to found a claim in either BoC or MoPI.

The Judge clarified that neither BoC nor MoPI impose a data security duty on the holders of information [22]. By contrast, both causes of action are concerned with prohibiting actions by the holder of information that are inconsistent with the obligations of confidence or privacy, respectively. Whilst a 'misuse' could include an unintentional use, it would still require a positive action in order for either of these causes of action to be made out [27].

Finally, the Judge noted that the Claimants in the case of *Various Claimants v Wm Morrison Supermarkets plc* [2019] QB 772 had attempted a very similar argument in that case, but the High Court had held that it was the positive actions of the wrongful actor (the aggrieved employee in that case, who had misappropriated the data), not those of Morrisons that could found a claim in BoC or MoPI – after all, it had not been Morrisons who disclosed the information, nor misused it.

Case one: Warren v DSG Retail
Case comment

The effect of this judgment is to narrow the potential causes of action that are available to Claimants in a case where an organisation has suffered from a cyberattack.

This means that in future a claim against the data controller for this sort of attack could only be brought under the new United Kingdom General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). Such a claim would include an alleged breach of Article 32 UK GDPR, which is structurally similar to the data security duty under the DPA 1998, therefore the cases under the 'old law' remain informative.

Although the High Court has not yet determined the question of whether or not DSG Retail breached the data security duty (DPP7), the Claimant may face an uphill struggle. He will need to show that DSG retail failed to implement measures that ensured a level of security appropriate to the nature of the data to be protected and the harm that might result from a data breach, having regard to both the state of technological development and the cost of implementing those measures at the time.

Whilst it assists the Claimant that the ICO has issued an MPN setting out DSG Retail's failures, it is not determinative or binding on the High Court. It is worth remembering that the Claimants in the *Morrisons* case failed to make out any breach by the supermarket chain of DPP7 (save for a minor breach), in spite of the facts in that case involving their internal data security measures and access to data by their own employee, over which they potentially had a greater degree of available control. Here, by contrast, it does not appear to be contested that DSG Retail suffered from a sophisticated external attacker, and they only need to show that their level of security was appropriate in the specific context to protect the Claimant's data, not to have anticipated and fended off a complex cyberattack.

Finally, even if the Claimant is successful in making out their claim, it is worth noting that the awards of damages for 'distress' under the DPA 1998 have a tendency to be far lower than those damages which have been awarded historically in MoPI claims. This will be welcome news for organisations that are 'totting up' the total potential costs and exposure to claims following on from a cyberattack.

Case two: Rolfe v VWV
No claim in a 'trivial' data breach case

The background facts

The Defendant in this case is a law firm which represented a school to which the first two Claimants owed a sum of school fees. The school had instructed the Defendants to write to the Claimants with a demand for payment. The third Claimant was their child.

An email attaching a letter was sent to the Claimants - but due to a one-letter difference in the email address of the mother, the letter went to a person with an identical surname and the same first initial. That person responded promptly to say the email was not intended for them. The Defendants asked the incorrect recipient to delete the message, and she confirmed that she had done so.

The Claimants pleaded BoC, MoPI, and included claims for damages under Article 82 of the GDPR and s169 of the Data Protection Act 2018. The Defendants sought summary judgment on the basis the claim had no real prospect of success.

The decision

Master McCloud referred to the case law in data breach claims (including the High Court decision in *Lloyd v Google*), focusing on the usual rule that there was at least a de minimis threshold, with damage/distress in excess of this threshold needed in order to found a claim in the Courts.

The Master asked herself what, given the nature of the breach, the nature of the information and the steps taken to mitigate the breach, was the actual loss or distress that had been suffered - and was this above a de minimis level? [11]

The Master concluded that the case involved minimally significant information, nothing especially personal such as bank details or medical matters, a rapid set of steps taken to ask the incorrect recipient to delete it and no evidence of further transmission or consequent misuse [12].

In the circumstances, therefore, Master McCloud concluded that the claim for distress was not credible. Commenting that in the modern world it was not appropriate for a party to claim, especially in the High Court, for breaches of this sort which are trivial [13], the Master granted summary judgment and the case was dismissed, with costs.

Case two: Rolfe v VWV
Case comment

Claimants who have experienced very minor data breaches, beware. The effect of this judgment is to reiterate that the Courts will actively consider at an early stage whether the claim falls beneath the threshold of a properly pursuable claim.

If the Claimant has lost nothing other than a trifling amount of information, and 'no harm has credibly been shown or be likely to be shown' (as in the Master's words), then the Claimant is likely to come away without a remedy (and to be punished in costs instead).

The case does also remind organisations how important it is to ensure that the breach is remediated quickly – by contacting the incorrect recipient and ensuring the misaddressed email was destroyed, the Defendants in this case saved themselves from the costs and nuisance of a full data breach claim.

Case three: Lloyd v Google
No easy route for mass data claims

The background facts

The case stems from allegations that between August 2011 and February 2012, Google took advantage of the configuration of software on Apple iPhones, so that if a user of Safari on those iPhones visited a website that contained DoubleClick Ad content, a third-party marketing cookie was installed on the user's device. This was known as the 'Safari Workaround', as it had the effect of bypassing protections in Apple's Safari browser on those devices, which blocked third-party marketing cookies by default. The DoubleClick Ad cookie is alleged to have enabled Google to track the user's activity across websites and to collect considerable amounts of information about their internet usage and advertisement viewing habits. This allegedly enabled Google's distribution of targeted advertising to those users and ultimately fed into Google's commercial profits.

This case concerns Mr Richard Lloyd who, supported by very significant litigation funding, issued a representative claim under CPR 19.6 for damages for breach of the DPA 1998. For the purposes of the representative action, Mr Lloyd issued a claim not only on behalf of himself, but all those potentially affected by the Safari Workaround (the 'Class'). This is a well-established procedure in which a claim can be brought by an individual as a representative of others who have 'the same interest' in the claim. Mr Lloyd argued that this requirement was satisfied, since all members of the Class could claim damages for 'loss of autonomy' or 'loss of control' over their data, for a uniform amount (which court documents stated as being £750 per user), and without the need for individual assessment of damages.

As Google is incorporated in the US, Mr Lloyd required the Court's permission to serve the claim outside the jurisdiction. Google resisted this on the basis that the representative claim had no real prospect of success.

The decision

The judgment of the Supreme Court (Lord Leggatt, with whom the others agreed), allowed Google's appeal, overturning the decision of the Court of Appeal, which would have allowed Mr Lloyd to serve his claim out of the jurisdiction on Google.

There are two key points from the judgment:

1. The impact on Data Protection Law claims
2. The potential impact on Misuse of Private Information (MoPI) claims

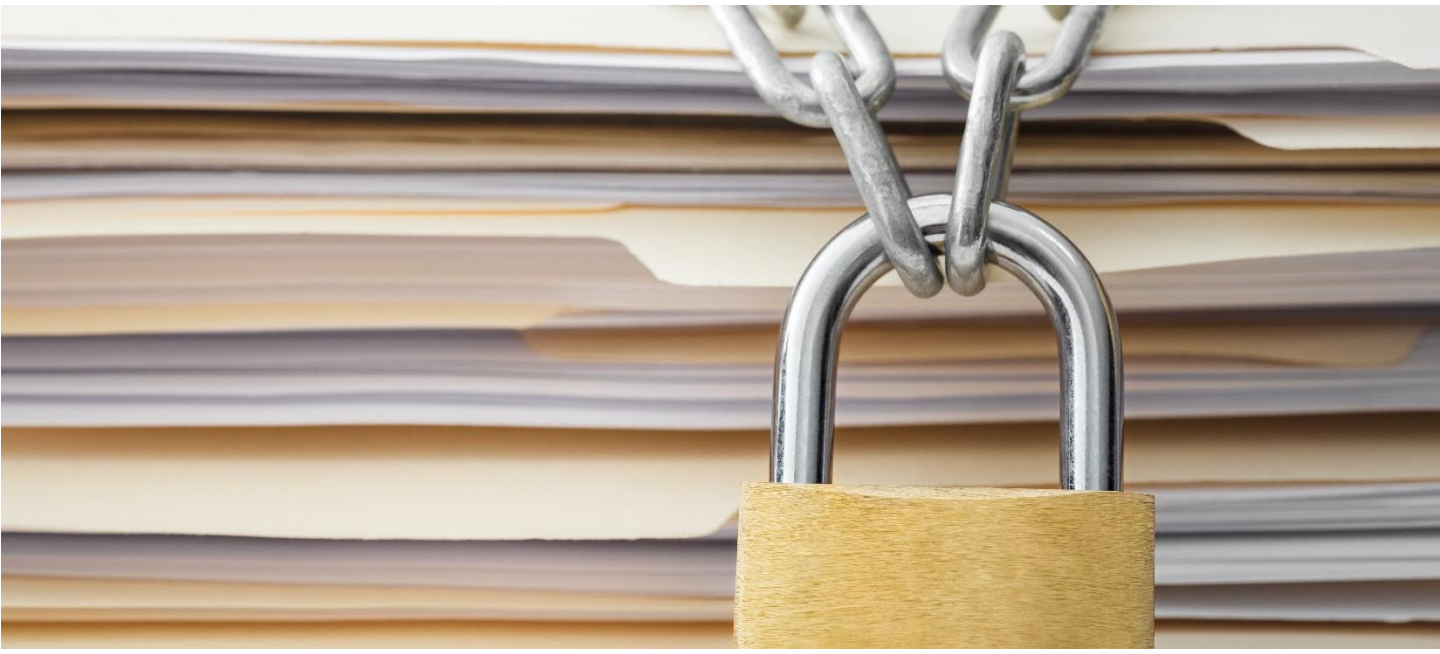
Case three: Lloyd v Google
The impact on Data Protection claims

Mr Lloyd argued that damages could be awarded for 'loss of control' of personal data, stemming from any non–trivial contravention by a data controller of any of the requirements of the DPA 1998.

After exploring, and rejecting, several alternative arguments, the Supreme Court concluded that s13 DPA 1998 could not reasonably be interpreted as conferring on a data subject a right to compensation for any 'contravention' by a data controller of any of the requirements of the DPA 1998, without the need to further and separately prove that the contravention caused material 'damage' or 'distress' to the individual concerned [138].

This, in turn, would require individualised assessment [144]. On the Claimant's own case there was a de minimis threshold that had to be crossed before a breach of the DPA 1998 would give rise to an entitlement to compensation under s13 DPA [153]. The bare minimum to bring someone into the Class (or the 'lowest common denominator') was someone whose internet usage – apart from one visit to a single website, which resulted in the download of the Google DoubleClick Ad cookie – was not illicitly tracked and collated and who received no targeted adverts [151]. This was considered to be below the de minimis threshold and the Supreme Court found it impossible to characterise the damage as more than trivial.

The Supreme Court stated that the Claimant was, in effect, attempting to recover damages without attempting to prove the allegation was true in any individual case or any details of unlawful processing beyond the bare minimum to bring them within the definition of the Class [153]. Accordingly, this case had no prospect of success in meeting the de minimis threshold for an award of damages.



Case three: Lloyd v Google
Distinction between DPA and MoPI claims

Mr Lloyd did not bring a Misuse of Personal Information (MoPI) claim for reasons which are unexplained. However, as Mr Lloyd did attempt to argue that the principles identified in caselaw for MoPI claims at common law also apply to the assessment of compensation under s13 of the DPA 1998, the Supreme Court did go on to comment on the availability of damages claimed on a representative basis for such a claim.

A fundamental element of Mr Lloyd's attempt to bring his claim within the representative action procedure was the assertion that a non-trivial breach of any individual's rights gives rise to an entitlement to damages for 'loss of control' of personal data. Mr Lloyd argued that because the tort of Misuse of Private Information (where 'loss of control' damages are awarded) and data protection legislation are both rooted in the same fundamental right to privacy (Article 8 of the European Convention of Human Rights (ECHR)), the same approach to damages should be adopted for both causes of action.

The Supreme Court rejected this approach. Lord Leggatt observed that there are material differences between the two regimes, including that data protection legislation applied to all personal data with no need to prove that the data is confidential or private in nature or that there is a reasonable expectation of privacy, whereas an action in MoPI protects information only where there is a reasonable expectation of privacy [130]. Furthermore, a Claimant is entitled to damages for contravention of the data protection legislation only where the data controller has failed to exercise reasonable care, whereas an action in MoPI is a tort involving strict liability for deliberate acts, and damages 'can be awarded for commission of the wrong itself' and 'may be awarded without proof of material damage or distress' [133].

Finally, going back to the need for individualised claims, the Supreme Court commented that the Claimant would have been aware that to establish a reasonable expectation of privacy, it would have been necessary to obtain evidence from each individual claimant and this requirement would be 'incompatible' with the nature of his representative claim [106].

Similarly, 'user damages' (i.e. compensation in a hypothetical negotiation with the Defendant for the loss of control of the use of the data), which lend themselves appropriately to MoPI claims, could not be sought in this case because of the inability or unwillingness of the Claimant to prove what, if any, wrongful use was made by Google of the personal data of any particular individual, which again means that any damages awarded would have to be nil [154]. This would require individualised assessment of what unlawful processing by Google of the Claimant's data actually occurred. For the Court to avoid the process of individualised assessment, they would have to consider the only wrongful act in common for the whole Class (i.e. the 'lowest common denominator', as above). This was the individual who had a DoubleClick Ad cookie placed on their phone, but without more, such a 'licence' to Google, would be valueless and the 'user damages' which could reasonably be charged for it would be nil [157].

Case three: Lloyd v Google
Case comment

The judgment offers guidance for future claimants, who now know what hurdles they face in seeking to pursue a representative action for damages in data privacy litigation. It is abundantly clear that claimants in data protection litigation must show the breach that has taken place and the resulting damage of that breach on an individualised basis.

The judgment is unlikely to preclude the possibility of a group of individualised data breach claims where individuals have been tracked for several years and sensitive data has been collected i.e. data concerning health and/or sexuality – in other words, more serious and egregious breaches.

The downsides for Claimants are likely to be practical. MoPI claims may be more attractive than data protection claims due to the availability of 'loss of control' damages, but Claimants must establish the 'reasonable expectation of privacy' (narrower than the availability of DPA claims) and cannot bring these claims where there is no 'wrongful' act by the controller. This will impact a Claimant's efforts to acquire costs protection because ATE insurance premiums are not recoverable from the Defendant for pure data protection claims. Lawyers will of course still be free to run cases on conditional fee (no-win-no-fee) agreements, although that in and of itself presents a substantial risk to firms.

It remains to be seen what, if any impact, the judgment will have on future mass claims founded on a breach of the UK GDPR and/or DPA 2018. The Supreme Court made clear that references to terms of the UK GDPR could not assist any interpretation of the DPA 1998. However, the terminology of Article 82 is similar to the DPA 1998 and the Data Protection Directive, therefore it is reasonable to believe that the case may be decided in a similar manner on the new law.

Conclusions: A fragmented future

The overall effects of the three judgments discussed on the future landscape of data litigation are cumulative, and they are particularly instructive for 'data breach' claims which have involved a cyberattack.

In our view:

- For any case which involves a data breach arising from a 'hacker' or 'cyberattack', whether an internal or external threat, the only realistic cause of action in the future (against the data controller rather than the attacker itself) will be one under data protection law, now the UK GDPR and/or DPA 2018 (contrast that with the situation where the Defendant has misused personal information, which may permit a BoC or MoPI claim).
- A UK GDPR and/or DPA 2018 claim will centre on arguments about whether or not the Defendant has breached the data security requirements (e.g. Article 5(1)(f) and/or Article 32 of the UK GDPR).
- It will be a complete defence for an organisation to show that they implemented all appropriate technical and organisational measures, therefore it is important to ensure your organisation has good cybersecurity governance measures such as a policy framework including an incident response management plan, and a process to regularly assess your technical controls.
- Even if the Claimant(s) are successful, damages will, in most of these cases, be limited to 'distress' (which typically attract lower awards than damages for breach of privacy or loss of control in MoPI claims).
- Damages will not be available in any data litigation cases, whether the cause of action is UK GDPR and/or DPA 2018, BoC or MoPI, where the harm to the Claimant cannot be reasonably substantiated and falls under the de minimis threshold.
- Rapid response by your organisation to contain the data breach and good remediation (as in the *Rolfe* case) may mean that the Claimant struggles to make out a claim above the de minimis threshold.
- A representative action for damages for an undefined large class of potential claimants is not viable, following *Lloyd v Google*, as opposed to numerous claims governed by a group litigation order, or several individual claims relating to the same circumstances. Even if a representative action is brought in future for a declaratory judgment following the 'bifurcated process' described by the Supreme Court, this will need to be followed up by individualised claims for damages. This should mean that your organisation can more easily assess the total potential exposure to claims, and thus make a reserve in your accounts accordingly.

This is not by any means stopping the rising tide of data claims, which will become ever more prevalent in a digital future. However, the overall effect of these judgments is that in future, we would anticipate that claims arising from personal data breaches or other contraventions of data protection law would be limited to claims in respect of the more serious and egregious breaches, properly particularised and with a claim for damages set out to be assessed on an individualised basis.

Get in touch

Tamsin Allen
Partner, Media and Information
+44 20 7833 4433
tamsin.allen@bindmans.com

Monika Sobiecki
Partner, Media and Information
+44 20 7833 4433
monika.sobiecki@bindmans.com

Daniel Shaw
Solicitor, Media and Information
+44 20 7833 4433
daniel.shaw@bindmans.com

Bartosz Kruk
Trainee solicitor, Media and Information
+44 20 7833 4433
bartosz.kruk@bindmans.com

Bindmans

Bindmans LLP is a limited liability partnership, registered in England and Wales. Our registration number is OC335189 and its registered office is 236 Gray's Inn Road, London WC1X 8HB. Our VAT number is GB 234 2718 76. The term partner means either a member of the LLP or a salaried partner. Our services are provided by solicitors of England and Wales. Bindmans LLP is authorised and regulated by the Solicitors Regulation Authority. Our SRA number is 484856.

© Bindmans LLP 2021.