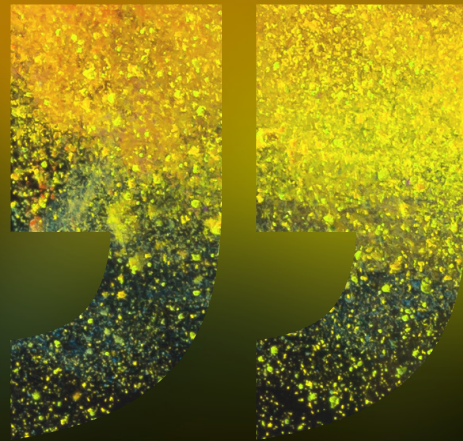


C L I F F O R D
C H A N C E



***LLOYD V GOOGLE:
HOW THE SUPREME
COURT JUDGMENT
CLOSED THE DOOR
ON LLOYD'S £3.3BN
DATA CLAIM***



— THOUGHT LEADERSHIP

NOVEMBER 2021



LLOYD V GOOGLE: HOW THE SUPREME COURT JUDGMENT CLOSED THE DOOR ON LLOYD'S £3.3BN DATA CLAIM

In a landmark case, *Lloyd (Respondent) v Google LLC (Appellant) [2021] UKSC 50 ("Lloyd")*, the Supreme Court has ruled that claimants can only obtain compensation for breaches of their statutory data privacy rights if they can evidence material damage or distress – loss of control of personal data alone is not sufficient. The case is likely to have implications for other class action-style claims against companies accused of breaching data privacy law. However, a focus on claims where actual damage has been suffered is the right outcome for all businesses, and not just for big Tech.

Key takeaways

- Reversing the decision of the Court of Appeal, the Supreme Court found that, to obtain compensation under the Data Protection Act 1998 (the "**DPA 1998**"), data subjects need to demonstrate that breaches of their data privacy rights caused them to suffer material damage or distress. Under the UK GDPR and the Data Protection Act 2018 (the "**DPA 2018**"), the right to claim compensation is likely to be materially the same as under the DPA 1998 (see below).
- Whilst claimants under the DPA 1998 will not be entitled to compensation simply by virtue of a data controller's loss of control over their data, compensation remains available for financial and non-financial loss in connection with data misuse, including distress. We still expect to see a growth in data litigation where there is real, actionable harm.
- The Supreme Court's finding that representative actions are inappropriate for damages claims that necessitate an individualised assessment of harm may mean that claimant solicitors and litigation funders will need to apply for group litigation orders instead. Unlike the representative action process, these are opt-in collective action processes, meaning that claimants will need to be persuaded to engage in the litigation. Claimants and litigation funders will have to either accept that a representative action can be used to obtain a declaration on liability, and then persuade claimants to opt-in to have their damages assessed, or pursue other collective mechanisms, such as group litigation orders. In doing so, they are likely to want to focus on claims where damages are likely to be material.

Background to the case

- In May 2017, Richard Lloyd filed a representative action on behalf of a number of claimants alleging that Google had breached its duties as a data controller under the DPA 1998 to over 4 million Apple iPhone users during some months in 2011 to 2012, by tracking their internet activity using the so-called *Safari Workaround*.
- The *Safari Workaround* allowed Google to identify visits by a relevant device to any website displaying an advertisement in its advertising network, and to collect considerable amounts of information. Among other things, it is alleged that the *Safari Workaround* allowed Google to determine how long a user spent on each relevant website and what advertisements were viewed, and to direct advertising to the user tailored to their interests.
- In the present case, Mr Lloyd seeks to serve the claims on Google in the US, and so was first required to seek permission from the English court to do so. In October 2018, Mr Justice Warby refused permission, explaining that, among other things, the Court could not make an award of "*vindictory*" damages in circumstances where it could not be shown that material damage or distress had been caused. Warby J noted that the representative class did not all have the "*same interest*" and, even if the class could be defined, there were practical

difficulties in establishing who the members were.

- However, in October 2019 Warby J's decision was reversed by the Court of Appeal. The Court (with the leading judgment by Sir Geoffrey Vos) found that an individual's control over their personal data had value, and therefore the loss of control over said data also had value. Therefore, in principle, damages are capable of being awarded in the absence of pecuniary loss or distress.
- It was held that the representative class did have the "*same interest*", namely that they were all victims of the same alleged wrong and suffered the same loss (i.e. loss of control over their personal data).
- Google appealed the Court of Appeal's decision, and this appeal was heard by the Supreme Court in April 2021.

What makes this a landmark judgment?

Two key aspects to the case make *Lloyd* a significant judgment in the emerging English data litigation landscape::

- First, in seeking permission to serve out of the jurisdiction on Google, Mr Lloyd sought the Court's approval of his argument that the DPA 1998 supported compensation for loss of control over data subjects' personal information without the need for the data subjects themselves to identify any specific financial loss, or evidence that they had

suffered material damage or distress. If this had been successful, the effect of such a finding would have been to open the floodgates to claims from data subjects for this new head of loss.

- Second, the case required the Supreme Court to reach a view on whether a representative action under Rule 19.6 of the Civil Procedure Rules (the "**CPR**") could proceed on the basis that the 4.6 million members of the class had the "*same interest*" in the claim, and were identifiable.

The Supreme Court Ruling

The Supreme Court has now allowed Google's appeal, and in a landmark judgment for the emerging English data litigation landscape, has found that:

- **Loss of control** – section 13 of the DPA 1998 requires that, for compensation to be awarded, the claimant must suffer "*damage by reason of any contravention*" (i.e. there must be damage distinct from and caused by the contravention). For the purposes of section 13 of the DPA 1998, "*damage*" is to be interpreted as material damage or distress.
- **Representative actions** – where damages are claimed in a representative action (as they were by Mr Lloyd), they must be calculable on a basis that is common to all persons represented. Alternatively, representative actions may be brought in two stages. The first stage would be to assess liability (i.e. whether the defendant was in breach of data protection legislation and a declaration that any member of the represented class who has suffered damage by reason of the breach is entitled to compensation). Then the second stage would then be to assess, on an opt-in basis, compensation in individual claims. Given that the purpose of awarding damages here is to put the claimants in the same position as if the wrong had not occurred, an individual assessment is generally necessary. Outside the data claims context, the Supreme Court left the door open to representative actions where damages can be calculated on a basis common to all members of a class, such as

where an entire class was wrongly charged the same fee or purchased an item with the same defect which reduces the item's value by the same amount.

The impact of *Lloyd* on liability for loss of control over data

Lloyd is the latest in a line of English jurisprudence through which the English courts have transitioned away from the traditional position (in cases such as *Johnson v Medical Defence Union* [2007] EWCA Civ 262) that "*damage*" for the purposes of section 13(1) of the DPA 1998 did not go beyond "*its root meaning of pecuniary loss*", i.e. monetary or other material loss (such as physical damage).

The judgment in *Vidal-Hall v Google, Inc.* [2015] EWCA Civ 311 radically altered the landscape. In *Vidal-Hall*, the Court of Appeal noted that Article 8 of the Charter of Fundamental Rights of the European Union ("**the Charter**") makes specific provision for the fundamental right to the protection of personal data, and that the type of loss suffered in breaches of privacy rights is generally one of "*moral damage*", i.e. the distressing invasion of privacy, rather than identifiable pecuniary loss. Limiting section 13(1) to pecuniary loss was therefore deemed incompatible with the Charter. Following this reasoning, the Court extended the interpretation of "*damage*" for the purposes of section 13 of the DPA 1998 to encompass a range of material and non-material damage, including any damage suffered as a result of contravention by a data controller of any of the requirements of the DPA 1998.

A landmark judgment in *Gulati v Mirror Group Newspapers* [2015] EWCA Civ 1291, a claim for misuse of private information arising from phone hacking, further altered the English legal landscape. In that case, the Court of Appeal found that misuse of private information *per se* could be compensable (i.e. without the need to show that damage had been caused by the misuse). In her judgment, Arden LJ (as she then was, and who – as Lady Arden – heard the case of *Lloyd* in the Supreme Court) reasoned that privacy is

a fundamental right and, therefore, that loss of control of privacy is in itself a form of damage.

The Court of Appeal in *Lloyd* cited *Gulati* extensively, indicating that it would be contrary to the EU law principle of equivalence – which provides that detailed procedural rules governing actions for safeguarding an individual's rights under EU law must be no less favourable than those governing similar domestic actions – to depart from the approach taken in *Gulati*. Since misuse of private information in *Gulati* and a breach of the DPA 1998 in *Lloyd* were similar domestic actions, "it would be *prima facie* inappropriate for the court to apply differing approaches to the meaning of damage".¹

The judgment of the Court of Appeal in *Lloyd* further extended liability under section 13 of the DPA 1998, applying *Gulati*, to include liability for "loss of control". Importantly, the Court confirmed that claimants did not need to show that they had actually suffered any loss because of the breach. It was not relevant that a claimant may not have objected to the loss of control.

Thus the battleground was set for argument in the Supreme Court over whether, on the one hand, damages only ought to be awarded to claimants in circumstances where their data rights had been breached and they can show that they have suffered pecuniary (i.e. monetary) loss or distress, or on the other hand, as Lady Arden described during the hearing of the appeal, "once you have interfered with someone's rights, there is *per se* an injury" that is compensable.

The Supreme Court judgment resolves the issue:

- Lloyd had sought an order that compensation could be awarded under section 13 of the DPA 1998 for any non-trivial contravention by a data controller of any of the requirements of the Act. The Supreme Court found that this could not succeed for two reasons:
 - under section 13 of the DPA 1998, compensation cannot be awarded for

a contravention *per se*, and can only be awarded where an individual has suffered damage distinct from and caused by the "contravention" (i.e. material damage or distress); and

- in order to assess compensation under s13, it is necessary to prove what unlawful processing of personal data relating to a given individual occurred. So, it was necessary to consider over what period of time Google tracked each individual's browsing history, the nature of the data obtained, the quantity of data that was unlawfully processed, how Google used the data etc.
- The Supreme Court confirmed that claims for damages for misuse of private information are different from claims under section 13 of the DPA 1998: (1) section 13 of the DPA 1998 provides a right for compensation for breaches in respect of personal data (which is not necessarily private), whereas the tort of misuse of private information protects specifically private information; and (2) the right to compensation under section 13 of the DPA 1998 is a qualified right (i.e. is subject to the defence that the defendant took reasonable care), whereas the tort of misuse of private information involves strict liability for deliberate acts. Therefore, claims may be brought for misuse of private information without proof of material damage or distress; this is not the position with claims under section 13.
- "User damages" (i.e. damages assessed by estimating what a reasonable person would have paid for the data rights of the user, typically found in wrongful use of land or property claims) may be available in misuse of private information claims. However, "user damages" are not available for breaches of section 13, as compensation under section 13 is based on material damage or distress having been caused by an infringement of a claimant's right to have his or her personal data processed in accordance with the requirements of the statute, not on the infringement itself.

¹ [2019] EWCA Civ 1599, at paragraph 52.

Lloyd and the future of collective actions in England

Collective actions are often brought with a view to pursuing claims which are, per claimant, of fairly modest value. However, the two available forms of collective action in England and Wales each provide for different challenges:

- Group Litigation Orders (under CPR 19.11) are made by the Court where multiple claims give rise to common or related issues of fact or law. Claimants have to "opt-in" to such actions; and
- Representative actions (under CPR 19.6) do not require individuals in the represented class to opt-in; rather, they are "opt-out" actions. However, representative claimants have to show that those in the class have the "same interest" in the claim.

For claims to proceed under a Group Litigation Order, a significant challenge has been to secure the participation of as many potential claimants as possible, so as to maximise the value of the claim as a whole. This is of particular importance where external litigation funding is sought, with funders often seeking to "build a book" of claimants before funding litigation. Persuading data subjects to opt-in and pursue relatively low value claims has been challenging. Conversely, the opt-out representative process allows the threat of the whole potential class to be leveraged, and for ATE insurance to be obtained in relation to the costs risk.

At first instance, Warby J found that iPhone users did not have the *same interest* as the consequences of Google's actions were not uniform across the entire class. He held that while the consequences may have amounted to some damage for some in the class, that was not necessarily the case for all. In addition, he held that even if the class was appropriately defined, there were insuperable practical difficulties in ascertaining whether any given individual was a member of the class. Ultimately, any compensation would need to be distributed to claimants self-identifying as

entitled to that compensation, and so this also led to serious concerns about how to verify those who came forward.

In reversing Warby J's decision, the Court of Appeal found that the represented class were all victims of the same alleged wrong, namely loss of control over their browser generated information. The fact that the claim did not rely on facts affecting any individual represented claimant did not mean that the represented claimants did not have the *same interest* in the claim. As Sir Geoffrey Vos noted in the judgment, "[t]he wrong is the same, and the loss claimed is the same. The represented parties do, therefore, in the relevant sense have the same interest"². Of Warby J's concern in relation to identifying the class, Sir Geoffrey Vos went on to note that "Google will be able to identify who is, and who is not, in the class"³.

The Supreme Court concluded that:

- Representative actions are a "flexible tool of convenience in the administration of justice". It found that the requirement that all members of the class have the "same interest" must be interpreted purposively and pragmatically on the basis that "it is better to go as far as possible towards justice than to deny it altogether".
- As such, it found that it should be no bar to making a representative claim that each claimant in the class has in law a separate cause of action "so long as advancing the case of class members affected by the issue would not prejudice the position of others", and there is "no true conflict of interest between them". This approach has been adopted by the highest courts in Australia, Canada and New Zealand, and is even more appropriate now given the development of digital technologies that have increased the potential for mass harm.
- However, it also found that, whilst it is no bar to making a representative claim that the relief includes damages, the vehicle of a representative action is inappropriate for damages claims that

² *Ibid*, at 75.

³ *Ibid*, at 80.

necessitate an individualised assessment of harm requiring the participation in the proceedings of the individuals concerned. This could work in circumstances where damages can be calculated on a basis common to all persons represented. However, this was not the case here, as the extent of the damage suffered was not the same for each claimant. We submit this criterion is always likely to be difficult to satisfy in data protection claims.

- The Supreme Court also acknowledged the prospect of representative actions being brought as part of a bifurcated two-stage process. The first stage would be to assess liability (i.e. whether the defendant was in breach of data protection legislation and a declaration that any member of the represented class who has suffered damage by reason of the breach is entitled to compensation). The second stage would then be to assess compensation in individual claims on the basis of the specific facts in each case.

What does this mean for claims under the UK GDPR and the Data Protection Act 2018?

The Supreme Court judgment requires claimants to evidence material loss or distress to bring a claim under section 13 of the DPA 1998, which was interpreted by reference to article 23 of the EU Data Protection Directive. However, as the UK GDPR and DPA 2018 superseded the DPA 1998, how will courts apply *Lloyd* to future claims brought under the UK GDPR and the DPA 2018?

The right to claim compensation under Article 82 of the UK GDPR and sections 168 and 169 of the DPA 2018 is broadly the same as under section 13 of the DPA 1998, albeit the UK GDPR and DPA 2018 include several clarificatory updates. These include Article 82(1) of the UK GDPR, which explicitly provides that compensation may be claimed by persons who suffer "*material or non-material damage*" (rather than mere "*damage*") and extends liability to

"*data processors*" (in addition to "*data controllers*"). Both sections 168 and 169 of the DPA 2018 (which respectively relate to compensation for contraventions of the UK GDPR and of other data protection legislation) specify that "*damage*" includes non-material or non-financial loss, including distress.

Recital 85 of the UK GDPR⁴ was an area of particular focus in the submissions made in the case, as it arguably provides an elucidation as to the types of damage contemplated by the UK GDPR, and in particular includes a reference to "*loss of control over [natural persons'] personal data or limitation of their rights [...]*" as constituting damage that may be suffered by a data subject. However, the Supreme Court judgment did not consider interpretation of UK GDPR to be relevant in this case because "*the meaning and effect of the DPA 1998 and the Data Protection Directive cannot be affected by legislation which has been enacted subsequently*".

Given the Supreme Court's interpretation of "*damage*" relied on the specific construction of section 13 of the DPA 1998 without reference to legislation subsequently enacted, there may be claimants who seek to distinguish themselves from *Lloyd* on the basis that their "loss of control" took place under the current statutory regime, for example, relying on Article 82 and Recital 85 of the UK GDPR. However, as "infringement" under the GDPR is equivalent to "contravention" under the DPA 1998, it seems likely that its decision in *Lloyd* that compensation can only be awarded where an individual has suffered damage distinct from and caused by the "contravention" will be followed in claims brought under current UK legislation.

What remains unanswered by the Supreme Court, and where next for data litigation?

Whilst the Supreme Court's judgment is a detailed analysis of the legal issues arising out of data claims, a number of outstanding issues remain to be resolved:

⁴ The explanatory notes to the European Union (Withdrawal Act) 2018 confirm that the text of the European legislation itself will form part of domestic legislation (the UK GDPR), and recitals will continue to be interpreted as they were prior to the UK's exit from the EU.

- **UK GDPR and the DPA 2018:** as above, it remains to be seen whether courts will follow *Lloyd* under the current UK statutory regime. Our view is that they should do so.
- **Quantification of damages:** Article 82 of the UK GDPR does not prescribe the level of compensation which should be awarded by the national court, and Recital 146 provides only that data subjects should receive "*full and effective compensation for the damage they have suffered*".

As the issues the Supreme Court has been considering in *Lloyd* ultimately arise out of an application for service out of the jurisdiction (rather than the substantive claim for compensation), the Supreme Court's judgment addresses whether loss of control damages are available under section 13 of the DPA 2018 in principle, and leaves open the question of quantum.

Whilst the judgment supports the "user damages" measure for damages in misuse of private information claims, it expressly disavows that measure for statutory claims. As such, it remains unclear the manner in which damages may be calculated for the purpose of providing "full and effective compensation". Far from a "finger in the air" exercise, we consider that the valuation of data will become a hotly contested area of expert debate in the coming years.⁵

- **Collective Actions:** with the Supreme Court rejecting the use of the representative action process for damages claims that necessitate an individualised assessment of harm, it remains to be seen whether potential claimants will engage in the Supreme Court's proposed two-step process, or will seek to bring claims under a group litigation order. Either way, to obtain an order for compensation, they will need to engage in the process of encouraging potential claimants to opt into the process, which can be time-consuming and uncertain.

- **Article 82 of the GDPR:** in reaching its judgment, the Supreme Court noted that "*EU law therefore does not provide a basis for giving a wider meaning to the term "damage" in section 13 of the DPA 1998 than was given to that term by the Court of Appeal in Vidal-Hall*". As to whether this is the case under Article 82 of the GDPR, on 15 April 2021 the Austrian Supreme Court referred certain key questions regarding non-material damages for data protection infringements under Article 82 to the European Court of Justice ("CJEU") for a preliminary ruling. One of the questions for the CJEU to address is whether the mere breach of provisions under the GDPR is in itself sufficient for the award of damages. It will be interesting to see how these matters develop and whether there is a divergence between UK GDPR and EU GDPR.

What are the consequences for businesses going forward?

This landmark judgment will have a range of consequences for businesses going forward:

- The Supreme Court's decision brings the position on data litigation in England and Wales closer to the position in other European jurisdictions, where the Courts have habitually required evidence of material damage or distress / emotional harm when awarding compensation for breaches of data protection rights / unlawful data processing under the GDPR.
- However, given the increasing number of high-profile data breaches in recent months and years, claims from individuals for compensation for breach of their data rights seem likely to continue to pose a serious threat to businesses. TikTok and Marriott are amongst those currently facing representative actions in England, with proceedings stayed pending the Supreme Court's judgment in *Lloyd*. Whilst claimants in such actions will not be entitled to compensation simply by virtue of the loss of control over their data, compensation remains available



⁵ For more, see our *Data Litigation: A Toolkit for Defendants briefing*.

for financial and non-financial loss in connection with data misuse, including distress.

- Moreover, it will be important to determine how (if at all) the decision affects the way in which the ICO operates following data breaches going forward. Gerry Facenna QC (on behalf of the ICO) noted at the Supreme Court hearings that if the Supreme Court were to construe the term "*damage*" in applicable data protection legislation

so narrowly as to exclude loss of control where there had been no material harm or distress, that may have an impact on the considerations the ICO may reasonably be able to take into account in deciding on the regulatory action it may take against businesses in breach (and, indeed, the fines it is able to levy).

Liam Porritt, Rikesh Gandhi and Bláithín Dockery contributed to the writing of this briefing.

AUTHORS



Kate Scott
Partner
London
T: +44 207006 4442
E: kate.scott@cliffordchance.com



Haafiz Suleman
Senior Associate
London
T: +44 207006 4348
E: haafiz.suleman@cliffordchance.com

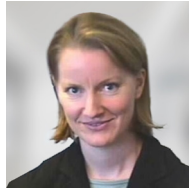
CONTACTS



Maxine Mossman
Partner
London
T: +44 207006 4204
E: maxine.mossman@cliffordchance.com



Samantha Ward
Partner
London
T: +44 207006 8546
E: samantha.ward@cliffordchance.com



Susan Poffley
Knowledge Director
London
T: +44 207006 2758
E: susan.poffley@cliffordchance.com



Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com



Simon Persoff
Partner
London
T: +44 207006 3060
E: simon.persoff@cliffordchance.com



Rita Flakoll
Senior Associate
Knowledge Lawyer
London
T: +44 207006 1826
E: Rita.Flakoll@cliffordchance.com

CLIFFORD CHANCE

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2021

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels
• Bucharest • Casablanca • Delhi • Dubai • Düsseldorf •
Frankfurt • Hong Kong • Istanbul • London • Luxembourg
• Madrid • Milan • Moscow • Munich • Newcastle • New
York • Paris • Perth • Prague • Rome • São Paulo • Shanghai
• Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.