The UK Supreme Court Hands Down Judgment in *Lloyd v Google*

David Cran, Head of IP and Tech, **Olly Bray,** Senior Partner, and **Alex Vakil,** Senior Associate, RPC comment on the recent *Lloyd v Google* judgment.

On 10 November 2021, in a keenly anticipated judgment that has significant ramifications for UK data protection, the Supreme Court overturned the Court of Appeal's decision in *Lloyd v Google* and restored the original order made by the High Court, refusing the claimant's application for permission to serve proceedings on Google outside the jurisdiction.[1]

In this article, we provide a summary of the High Court and Court of Appeal decisions, then delve into the key points arising from the Supreme Court judgment of Lord Leggatt (with whom the other justices agreed).

Background

In May 2017, Mr Richard Lloyd (the **Claimant**), a former executive director of Which, filed a class action against Google for its use of the so called "Safari Workaround" during 2011 and 2012.

The Safari Workaround circumvented the privacy settings in place on the browser and allowed Google to place a third-party cookie on the iPhone of any user that visited a website containing "DoubleClickAd" content. Information on the individual's browsing habits (browser generated information (**BGI**)) would be collected via the cookie. BGI was then sold to third parties, enabling them to target their advertising towards consumers with specific interests or attributes.

Google was fined $22.5m by the United States Federal Trade Commission for its use of the Safari Workaround. Mr Lloyd brought the opt-out class action in the English courts on behalf of approximately 4.4m iPhone users. In order to bring the claim against Delaware-based Google, Mr Lloyd had to obtain permission of the court to serve proceedings out of the jurisdiction.

High Court Decision

At first instance, Warby J of the High Court refused the application. The reasoning for the decision was three-fold:

1. the Claimants in the representative class had not suffered damage within the meaning of s13 of the *Data Protection Act 1998* (**DPA**);
2. the Claimants did not have the "same interest" for the purpose of Civil Practice Rule 19.6(1) because they were likely to have suffered different types of harm (if any at all);
3. Warby J exercised his own discretion under Civil Practice Rule 19.6(2) to prevent the claim from proceeding. He considered it *"officious litigation on behalf of others who have little to gain from it, and have not authorised the pursuit of the claim, nor indicated any concern"*.

Court of Appeal Decision

In 2019, the Court of Appeal unanimously overturned the decision of the High Court.

The Court found that it was possible to award damages for "loss of control" of an individual's data, despite the Claimants not having suffered pecuniary loss or distress. Whilst data was not property, it had economic value as it had been sold to third parties. Following that reasoning, losing control of your data has a value. In reaching its conclusion, the Court looked to previous case law on loss of control of private information.

The Court ruled that the Claimants in the representative class had the same interest. Each had suffered the same harm, as they had experienced loss of control of their data. However, the loss suffered by each in the class was the "lowest common denominator".

In relation to the final point, the Court exercised its discretion and allowed the claim to proceed. The fact that the Claimants had not been specifically identified or authorised the claim did not mean that the claim should be halted.

On 11 March 2020, the Supreme Court granted Google permission to appeal against the Court of Appeal's decision.

Supreme Court Decision

Monetary Compensation

The Claimant's case was that an individual is entitled to recover compensation under section 13 of the DPA without proof of material damage or distress whenever a data controller fails to comply with any of the requirements of the DPA in relation to any of that individual's personal data, provided only that the breach is not trivial or de minimis. This was presented as "loss of control" or "user" damages; a lowest common denominator of loss suffered by each and every individual by reason of the breach.

Reversing the Court of Appeal's decision, the Supreme Court held that, to recover compensation, it is not enough to merely prove a breach by a data controller of its statutory

1 *Lloyd v Google LLC [2021] UKSC 50*

duty under section 4(4) of the DPA: an individual is only entitled to compensation under section 13 where "damage" - or in some circumstances "distress" - is suffered as a consequence of such a breach of duty. It is therefore necessary to prove that the breach of the DPA has caused material damage or distress to the individual concerned. The Claimant's construct of "loss of control" or "user" damages was rejected.

Takeaway: In order to bring a claim for compensation for breach of data protection legislation, it is necessary for a data subject to prove that they suffered "damage" or "distress" – a contravention by a data controller of the requirements of data protection legislation alone is not sufficient.

Representative claim

Lord Leggatt could see no legitimate objection to a representative claim brought to establish whether Google was in breach of the DPA, and, if so, seeking a declaration that any member of the represented class who has suffered damage by reason of the breach is entitled to be paid compensation. However, the Claimant had not proposed such process given that success at the first stage would not itself generate any financial return for the litigation funders or the persons represented. Both courts below accepted that a representative action is the only way the claims could be pursued.

Takeaway: A representative action remains an appropriate mechanism for seeking a declaration that each member of class has suffered damage and could also be used where each member of the class has suffered the same damage (although the latter is likely to be difficult in a data claim).

De minimis threshold

The Claimant accepted that there is a threshold of seriousness which must be crossed before a breach of the DPA will give rise to an entitlement to compensation. The Supreme Court held that the position that the Claimant asserted in each individual case was not sufficient to surmount the threshold and held that it was "impossible to characterise such damages as more than trivial."

Takeaway: The Supreme Court did not provide any further guidance on what constitutes a de minimis or trivial contravention of data protection legislation. There is likely to be further debate as to this threshold when claims are asserted against data controllers, although the mere fact of a breach will not be sufficient.

Relevance of GDPR

The Supreme Court acknowledged that the parties and the interveners had made frequent references to the provisions of the General Data Protection Regulation and the Data Protection Act 2018 in their submissions but given that the meaning and effect of the DPA and the Data Protection Directive could not be affected by the subsequent legislation, it was not considered.

Takeaway: Although GDPR and the Data Protection Act 2018 were not considered capable of helping to resolve the particular issues raised on the appeal, given the wording of the provisions concerning compensation are substantively replicated in Article 82 GDPR, the Supreme Court's judgment will have future application.

Comment

The Supreme Court's judgment will be warmly welcomed by data controllers who, following the Court of Appeal's judgment, were exposed to very significant potential liability arising from data claims, even if no specific damage was shown to have been suffered by any individual.

The judgment has firmly rejected the basis of this class action and many others that were waiting in the wings (some of which had been stayed pending handing down of this judgment). It is likely to have a very significant impact on UK industry across many different sectors that handle customer data, as well as the UK legal market, including claimant firms, litigation funders and ATE insurers.

Although the Supreme Court has left the door open for representative actions to proceed in relation to claims for breaches of data protection legislation, the rejection of the concept of "loss of control" damages and the requirement that individuals must prove they have suffered damage means that a representative action is unlikely to be a financially viable option for legal advisers and funders in most data claims.