COVINGTON

Landmark Case Opens the Door to UK Data Protection Consumer Class Actions

October 10, 2019

Data Privacy and Cybersecurity

On October 2, 2019, the English Court of Appeal handed down a landmark judgment in *Lloyd v Google LLC [2019] EWCA Civ 1599* ("*Lloyd*") concerning Google's alleged misuse of the personal data of over 4 million iPhone users via cookies placed on the Safari browser. Although this issue has previously been the subject of litigation in the English courts (*see* our Inside Privacy blogpost on the decision in *Google Inc. v Vidal-Hall & Ors [2015] EWCA Civ 311*), this judgment is particularly noteworthy because:

- the Court of Appeal held that even though the claimants are not claiming for financial loss or distress, they are nonetheless entitled to damages for loss of control of their personal data (the amount of damages is yet to be determined); and
- it is the first time the English courts have been asked to consider this in the context of a class action and, in allowing the claim to proceed, the Court of Appeal has revived the mechanism of representative actions, which was thought to be largely ineffective for bringing substantial consumer collective claims in the UK. This may have ramifications beyond the data protection context.

Background and summary

Google is accused of harvesting personal data – more specifically, browser-generated information ("BGI") from Safari browsers – by placing a "DoubleClick Ad Cookie" on users' iPhones without their knowledge or consent during 2011-2012. This enabled Google to extract data about the websites that users visited and derive information about users' personal interests, opinions and habits for the purpose of profiling and sending targeted advertising.

The case arose following an application by the claimant, Mr Lloyd, who is seeking to represent the entire class of iPhone users, for permission to serve Google in the U.S. The High Court (first instance) judge denied the application on the bases that (1) none of the class of claimants had suffered damage under the UK's Data Protection Act 1998 ("DPA 1998") -- the predecessor law to the EU's General Data Protection Regulation 2016/679 ("GDPR") and the UK's Data Protection Act 2018 ("DPA 2018"); and (2) the members of the proposed class of iPhone users did not have the "same interest" in bringing a case, which is a necessary condition under the UK civil procedure rules ("CPR") for bringing representative actions (a form of opt-out class action). The first instance judge also exercised the discretion available to him under the CPR to prevent the claim from proceeding.

The Court of Appeal has reversed the High Court's decision on all grounds, thus granting Mr Lloyd permission to serve Google and continue the claim on behalf of the represented class. The basis for the Court of Appeal's reversal is significant for two reasons:

- The Court found that although the iPhone users are not claiming for financial loss or distress as a result of Google's mishandling of their personal data, they have all suffered damage under UK data protection law as a result of "*clear, repeated and widespread breaches of Google's data processing obligations*" (paragraph 86) and Google's violation of their respective fundamental rights to privacy. The Court found that loss of control over personal data is in itself damage for which compensation must be paid.
- The Court also held that the proposed class of claimants do have the "same interest" in a claim against Google, permitting the representative action to proceed.

The Court of Appeal's decision in more detail

Loss of control

The first issue that the Court considered was whether a claimant may recover damages for infringement of their data protection rights without demonstrating that they have suffered financial loss or distress. In short, the Court of Appeal held that the answer to this question is "yes".

The answer turned on the meaning of "damage" in this context. The Court considered relevant sections of the UK's and EU's previous data protection legislation[1], noting that they were designed to protect individuals' rights to privacy under human rights rules[2]. The Court determined that the individuals to be represented in the class suffered damage at the hands of Google as a result of the loss of control or loss of autonomy over their personal data. Control of data was deemed to have an economic value and thus loss of that control should be compensated. The Court described it as follows (paragraphs 46-47):

> "*Even if data is not technically regarded as property in English law, its protection under EU law is clear. It is also clear that a person's BGI has economic value: for example, it can be sold. . . . The underlying reality of this case is that Google was able to sell BGI collected from numerous individuals to advertisers who wished to target them with their advertising. That confirms that such data, and consent to its use, has an economic value.*
>
> *Accordingly, in my judgment, a person's control over data or over their BGI does have a value, so that the loss of that control must also have a value.*"

The Court went on to consider whether loss of control of data can properly be considered "damage" by reference to the 2015 Court of Appeal judgment in *Gulati v MGN Limited [2015]*

[1] Section 13 of the DPA 1998 and Article 23 of the EU Data Protection Directive 95/48 (precursor to the GDPR).

[2] Article 8 of the European Convention on Human Rights and Article 8 of the EU Charter of Fundamental Rights.

EWHC 1482 (Ch), [2015] EWCA Civ 1291 (CA) ("*Gulati*"). *Gulati* concerned the infamous phone-hacking scandal, in which multiple claimants sought damages for misuse of their private information by various UK newspaper groups. Together, the claimants were awarded compensation in the order of £1.2 million for the loss of control of their private information.

Although compensation in *Gulati* was awarded on the basis that the defendants had committed the tort of misuse of private information ("MPI"), as opposed to a breach of data protection legislation, the Court of Appeal in *Lloyd* drew an analogy between these two types of claims. Specifically, the Court determined (paragraph 53) that: "*The actions in tort for MPI and breach of the DPA [1998] both protect the individual's fundamental right to privacy; although they have different derivations, they are, in effect, two parts of the same European privacy protection regime.*" Thus in the same way that the Court awarded damages in *Gulati* "*to compensate for the loss or diminution of a right to control formerly private information*," the Court in *Lloyd* held that "*it would be wrong in principle if the represented claimants' loss of control over BGI data could not, likewise, for the purposes of the DPA [1998], also be compensated*" (paragraphs 54-56).

Relatedly, the Court commented that, while not determinative to this case, it was "helpful" to consider how the GDPR deals with the notion of damage in Article 82(1), which gives individuals the right to receive compensation for material or non-material damage suffered as a result of infringement of the GDPR. Looking also at recital 85 to the GDPR, they found that the notion of material or non-material damage includes situations where individuals lose control over their personal data.

The Court also noted that claims of this nature must exceed a "triviality" threshold. This threshold would "*undoubtedly exclude, for example, a claim for damages for an accidental one-off data breach that was quickly remedied"* (paragraph 55). The *Lloyd* case, however, was not deemed to be trivial; instead, here, "*every member of the represented class has had their data deliberately and unlawfully misused, for Google's commercial purposes, without their consent and in violation of their established right to privacy*" (paragraph 55). Accordingly, the claimants are, in principle, entitled to damages for loss of control of their personal data even if there is no financial loss and no distress. The level at which those damages will be set remains to be seen.

"Same interest"

The second key issue that the Court considered was whether members of the represented class of claimants have the "same interest" in bringing a claim. Again, the short answer from the Court of Appeal is "yes".

Mr Lloyd's claim is brought on behalf of potentially all iPhone users who used the Safari browser in England and Wales during the relevant period. Mr Lloyd relies on Rule 19.6 of the CPR, which permits one or more persons to bring a claim as a representative of all other individuals who have the "same interest" in that claim. Unless the "same interest" is established, the representative claim cannot proceed.

The High Court ruled that the represented claimants had either suffered no damage at all or had suffered damage that was inherently fact-specific and therefore could not be considered the "same". This accorded with cases applying the "same interest" requirement strictly in other contexts, such as antitrust litigation. The Court of Appeal's finding that loss of control of data can properly be considered "damage" allowed it to reverse the High Court's earlier

decision. The Court of Appeal held that *"the represented class are all victims of the same alleged wrong, and have all sustained the same loss, namely loss of control over their BGI"* (paragraph 75). The Court found that it was impossible to imagine that Google could raise a defence to one represented claimant that did not also apply to all the others. On this basis, the Court allowed the claim to proceed with Mr Lloyd representing the entire class of potential claimants.

Implications for future representative data protection claims

Claimants are likely to feel emboldened by the *Lloyd* ruling to bring group actions against organisations that have suffered data breaches or otherwise failed adequately to protect personal data. Indeed, claimants may seek to apply the same reasoning to bring putative class actions in other contexts, such as claims based on broader consumer protection violations, antitrust damages, or securities claims. However, the *Lloyd* claim was unusual in finding a mechanism by which all members of the class could feasibly be said to have suffered the same harm. That would be harder in many other contexts.

The decision in *Lloyd* comes at the same time as the English courts are hearing another data protection collective action claim, this time against British Airways, which suffered a security breach in 2018 affecting personal data of thousands of customers. In addition to facing fines of over £180 million imposed by the UK privacy regulator, the Information Commissioner's Office, the airline is defending a collective action in which claimants are seeking compensation for non-material damage caused by the breach. On 4 October 2019, the High Court approved an application for a "Group Litigation Order", which will enable the collective action to proceed (on an opt-in basis).

An important point to note about a representative action, such as that in *Lloyd*, as opposed to a Group Litigation Order in the British Airways case, is that representative actions operate on an opt-out basis, i.e., the claim is brought on behalf of everyone who is a member of the potential class of claimant unless they actively opt out. There is no limit to the number of persons that can be within the class; neither the class size nor the identities of affected individuals need be known in order to bring a claim.

As such, even though the damages award for each individual claimant is likely to be relatively low (much lower than if each claimant was seeking damages for distress or financial harm), the fact that the potential claimant pool can run to millions of individuals means that the financial exposure under a representative action is expansive: Mr Lloyd estimates that as many as 4 million affected individuals could be entitled to approximately £750 compensation each, meaning a total liability sum of £3 billion.

Assuming that the Court of Appeal's decision is not overturned, English courts are now bound to apply the ruling in *Lloyd* on the meaning of "damage" under data protection law generally (not just in respect of class actions) -- even where claimants have not suffered financial loss or distress. Additionally, the Court's comments on the interpretation of "damage" in the GDPR are likely to encourage claimants in the future (in some cases backed by claimant firms and third party litigation funders) to bring claims of this nature under the GDPR.

Covington's team of data protection regulatory lawyers and litigators are closely monitoring this case and similar consumer class actions. If you have any questions concerning the material discussed in this client alert or related developments, please contact any of the following members of our team:

Daniel Cooper	+44 20 7067 2020	dcooper@cov.com
Mark Young	+44 20 7067 2101	myoung@cov.com
Louise Freeman	+44 20 7067 2129	lfreeman@cov.com
Gregory Lascelles	+44 20 7067 2142	glascelles@cov.com
Fredericka Argent	+44 20 7067 2281	fargent@cov.com
Rosie Klement	+44 20 7067 2140	rklement@cov.com