Browne Jacobson

Lloyd v Google – what next?

The Supreme Court's pending decision could potentially open the floodgates for data privacy litigation going forward.

28 June 2021

On 28 and 29 April 2021 the Supreme Court heard the much-anticipated appeal by Google against the 2019 Court of Appeal decision, which granted Mr Lloyd permission to serve a representative action on Google in the US on behalf approximately 4.4 million iPhone users. Whilst we still await the outcome, the Supreme Court's decision could potentially open the floodgates in terms of data privacy litigation going forward.

The facts

The action brought by Mr Lloyd relates to Google's so-called "Safari Workaround" method used during 2011 and 2012, whereby Google allegedly set its DoubleAd Click cookie to track and collect information about iPhone users' internet activity (known as "browser generated information") without their knowledge or consent, in breach of the Data Protection Act 1998. It is alleged that Google aggregated the browser generated information in order to classify users into groups such as "current affairs enthusiasts" or "football lovers" and then sold their data to advertisers who wanted to target specific groups of people.

The notable point is that Mr Lloyd is not alleging that he (nor any of the claimants that he is seeking to represent) have suffered financial loss or distress; merely that they should be compensated for the loss of control of their personal data.

The claim is brought under Civil Procedure Rule ("CPR") 19.6 which allows an individual to act as a representative on behalf of a defined class of claimants, provided that all claimants have the "same interest".

Court of Appeal decision

In granting permission to Mr Lloyd to serve his claim on Google, the Court of Appeal made two key findings:

1. that damages are capable of being awarded for loss of control of personal data without the claimant having to prove financial loss or distress; and
2. that, on that basis of the above finding, a claim could be brought under CPR 19.6 because each of the individuals that Mr Lloyd is seeking to represent are identifiable and have the "same interest".

The Court of Appeal stated "*it is impossible to imagine that Google could raise any defence to one represented claimant that did not apply to all others. The wrong is the same, and the loss claimed is the same*". The Court of Appeal found that it could exercise its discretion to allow the claim to proceed under CPR 19.6.

Impacts of the Supreme Court decision

Should the Supreme Court take the same view as the Court of Appeal, this will represent a seismic shift in the data privacy litigation landscape, impacting on both the ease with which representative actions can be brought (signifying a move to US style "opt out" actions), and lowering the bar in terms of the type of damage that can be claimed (i.e. loss of control of personal data without having to show financial loss or distress). This combined with:

- individuals becoming increasingly aware of their rights in relation to their personal data, aided in part by claimant law firms advertising for claimants in respect of mass data breaches (e.g. British Airways and Easyjet); and

- an increase in litigation funds backing data privacy class actions,

is bound to open the floodgates to a wide range of claims for breaches of data protection legislation.

Whilst this is a case heard under the Data Protection Act 1998, the principles apply to compensation claims made under the EU and UK GDPRs. Indeed, it may serve to clarify the position in Recital 85 which suggests that loss of control of personal data is a type of damage in relation to personal data breaches.

What should you do now?

Here are some practical steps you can take now to protect your organisation against the types of claims described above.

- **Review your cookie practices**; in particular your cookie consent mechanism and the information you provide about your cookies (and other similar technologies). It is easy for individual claimants to go on to your website and immediately identify if you are complying with relevant laws and guidance from regulators. We are already seeing letters before action being sent from individual claimants, who have spotted that organisations are not complying with the relevant obligations, seeking a settlement sum or threatening legal claims.
- **Review your other external facing privacy documentation**, such as privacy policies, to ensure that they are up to date. In particular, there may be changes that are required following Brexit.
- **Review your electronic marketing practices** to ensure compliance with relevant legislation. In particular, ensure that individuals are provide with an opportunity to opt out of direct marketing. Where an individual does opt out of electronic marketing, ensure that you have robust processes in place to ensure those individuals do not continue to be sent direct marketing communications.
- **Review your information security practices and procedures** and ensure that you have robust procedures in place to immediately detect and mitigate the impacts of personal data breaches. This includes training all staff to be able to identify a personal data breach and take appropriate steps.

Contact

Mark Hickson

Head of Business Development

onlineteaminbox@brownejacobson.com

+44 (0)370 270 6000

Related expertise

Data protection and privacy

Dispute resolution and litigation