



Google court case ruling broadens business privacy risks

Vanessa Cathie

The UK's Court of Appeal has allowed a representative action against Google, clarifying that individuals can suffer damage by losing control of data while potentially opening the floodgates for privacy class actions in the country. The court fired a warning shot to big businesses, reiterating that individuals' data cannot be used for commercial gain without consent.

The court held that individuals may be entitled to damages when they lose control or autonomy over their personal data without having to prove monetary loss or distress, extending the risk exposure of any company controlling personal data.

The Background

The case was launched by Richard Lloyd, champion of consumer rights and former director of Which?. According to Lloyd, in 2011 and 2012, Google allegedly secretly tracked personal data of more than four million iPhone users, even when users had enabled a "Do not track" option on their phones. Google then used this data ("browser generated information" or BGI) for the purposes of directed advertising. Lloyd is claiming £750 per head in damages, adding up to a total cost of £3.3 billion.

This case arose out of the "Safari Workaround" - essentially Google's use of a technical workaround to bypass the cookie settings on the Safari browser and place tracking cookies without the individual's knowledge or consent. Google was required to pay \$22.5 million by way of fine to US regulators in 2012.

Gauging the Consequences

Lloyd is bringing a "class action" against Google seeking damages for each individual affected. While the High Court (in October 2018) refused to allow the case to proceed, the Court of Appeal decision unanimously allowed the appeal in the first October week, handed down by Sir Geoffrey Vos.

Sir Geoffrey's analysis in the appeal court was that a key feature is the class members' loss of control or loss of autonomy over their personal data. This was the start and finish of it — no evidence of monetary loss or distress needs to be proved.

The Court of Appeal's position was that data is an asset that has value — the fact that a person's BGI has economic value and can be sold, is evidence of this. The class members' loss of control or loss of autonomy was the damage.

The appeal court's decision relies on several case law examples which support the principle that privacy must be protected and compensation provided, regardless of proof of distress or pecuniary loss. In passing, the court noted that General Data Protection Regulation (GDPR) legislation provides that compensation may be available for non-material damage including loss of control.

A key factor is that privacy must be protected and in this case "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."

The court held that failure to allow compensatory damages in this situation could mean that the alleged breaches remain unremedied.



“[T]his case, quite properly if the allegations are proved, seeks to call Google to account for its allegedly wholesale and deliberate misuse of personal data without consent, undertaken with a view to commercial profit.”

Sir Geoffrey opined that while the court resources to deal with the claim may be significant “it will ensure that there is a civil compensatory remedy for what appear, at first sight, to be clear, repeated and widespread breaches of Google’s data processing obligations...”

Google is seeking permission to appeal to the Supreme Court and declared that “protecting the privacy and security of our users has always been our number one priority. This case relates to events that took place nearly a decade ago and that we addressed at the time. We believe it has no merit and should be dismissed.”

The “class action” Component

According to Pinsent Mason, Google’s lawyers, “the court’s findings potentially open the way for representative actions in the context of other data protection claims where numerous data subjects have been affected, regardless of whether those data subjects were distressed by what happened, and regardless of whether they actually want to make a claim.”

Under the relevant law, the persons represented in a claim must have the same interest in the claim. The appeal judgment states that “[t]he represented class are all victims of the same alleged wrong”, namely the loss of control over their BGI. The parties all have a stake in the same interest – a common interest and a common grievance.

The sum awarded to the claimants will not take account of individual circumstances but “will take account, at least, the facts of the tort proved against Google generically, and the effect, in terms of loss of control of personal data, that the breaches would have on any person affected by Google’s unlawful actions.”

The Court of Appeal held that it is theoretically possible to identify the class based on the data in possession of Google and allowed the “opt-out” principle to apply - the claim is made on behalf of all those affected, and those who are not keen to be a part of the class, may opt-out.

Consequences for Businesses

The judgment shows how seriously the Court of Appeal takes the fundamental right to privacy and data protection. The message for businesses is clear...ignore basic privacy rights at your peril.

Loss of control and loss of autonomy are recognised triggers for claims for damages and, with the landscape gradually shifting to support a new wave of representative actions, this decision is likely to increase businesses’ exposure significantly. Consequently, the decision reinforces the need for businesses to be very aware of their corporate cyber hygiene and cyber risk profiles.

A robust cyber policy, if in place, would cover legally insurable compensation awarded by the court, together with associated legal, forensic, crisis management and public relations costs.

For further details please contact:



Lucy Scott | Senior Vice President

E lucy.scott@uk.lockton.com

T **+44 (0) 20 7933 2382**



Vanessa Cathie | Account Executive,
Global Professional & Financial Risks

E vanessa.cathie@uk.lockton.com

T **+44 (0) 20 7933 2478**