GROUP DATA CLAIMS REMAIN A THREAT AFTER LANDMARK LLOYD V GOOGLE DECISION, SAY HERBERT SMITH FREEHILLS LAWYERS

10 November 2021 | London
News

The UK Supreme Court has given its decision on an appeal by Google against the Judgment of the Court of Appeal in the case of Lloyd v Google, ruling in favour of Google.

In October 2019, the English and Welsh Court of Appeal granted claimant Richard Lloyd permission to serve a ‘US-style’ class action against Google in the English Courts on behalf of an estimated 4.4 million iPhone users. The claim centres around Google’s alleged unlawful gathering and exploitation of browser generated information on Apple’s Safari browser, in breach of the UK Data Protection Act 1998.

This hearing confirmed that the "opt-out" class action representative procedure under Rule 19.6 of the Civil Procedure Rules 1998 cannot be used in a mass claim of this kind to seek damages for alleged data breaches for the whole class, although it could be used to determine liability with the issue of damages to be dealt with in various separate proceedings. A team of Herbert Smith Freehills lawyers give their immediate reaction to the decision today below.

Julian Copeman, Herbert Smith Freehills Partner and a leading expert in data class actions said: "*While this decision means that the threat of 'US style' opt-out litigation in data claims has receded, group litigation is here to stay and there is nothing in this decision which means that such claims won't continue to be brought as 'opt in' group claims. This decision focused on whether claims for loss of control of data could be brought by a single representative on behalf of a class of potentially millions of unknown claimants. It will be a relief to businesses that claimant firms and funders won't simply be able to issue claims for compensation on that basis. However, claims can still be brought by gathering a group of claimants, and in those circumstances it is possible for the claim to reflect the individual circumstances of different sub- groups or classes of claimants. Indeed, the Supreme Court has suggested a US style class action could still be brought to determine liability, but that smaller group claims would then be needed to deal with different issues of compensation. Businesses should still ensure their data and privacy risk management frameworks are fit for purpose – the floodgates have not been opened, but group data claims remain a threat.*"

Herbert Smith Freehills Partner Miriam Everett, who is Global Head of Data and Privacy. said*:* "*This is the outcome that most organisations will have hoped for. It closes the door (at least for now) on compensation under data protection laws for a 'loss of control' of data. However, whilst a small sigh of relief can be expected, organisations will be all too well aware that the GDPR does still grant a right to individuals to claim compensation for data protection breaches, including where there is no financial loss. Whilst 'loss of control' of data has been ruled out, there are many other ways in which organisations may breach their data protection obligations and many more individuals looking to seek compensation as a result of such infringements.*"

Herbert Smith Freehills Partner Andrew Moir, who is Global Head of the firm's Cyber and Data Security practice, said: "*It was already common for data breach class actions to follow any significant data breach, almost by return, and today's judgment doesn't really change that. Today's judgment does mean that there's going to be more work for claimants to do to get the claims off the ground. It's common in data breaches for data subjects to be affected in different ways. Some might only have had their e-mail address compromised for example; others might have more sensitive data affected such as banking details. Claimants therefore often naturally stratify into different classes – there will now be more of an onus on claimant lawyers to identify those, and actually to prove loss, before any claim will be successful. The Supreme Court did leave the door open to two-stage claims – first establishing a breach of the underlying data privacy legislation, but then a subsequent assessment of damages. Such claims will therefore remain viable, most probably using an initial judgment on liability to promote settlement without needing the subsequent inquiry as to damages.*

"For defendants, it therefore remains important to be able to justify the technical and organisational measures in place prior to any cyber incident. It doesn't follow, just because data has been taken, that there is an underlying inadequacy of technical and organisational measures. Being able to tell the story of what happened and why, with supporting expert evidence, is going to be a key aspect of any data breach class action – and vital to the first stage of a two-stage claim. While the Supreme Court did indicate any damages would need to be material to be recovered, further guidance will be necessary on what a data breach which causes distress, but not any financial loss, is "worth" in damages."

Herbert Smith Freehills Consultant Kate Macmillan, who is an expert in cyber and information/data law, said: *"This case was part of a broader debate about how to deliver accountability to consumers in a digital world. The case honed in on "damage" under the pre-GDPR law (the 1998 Data Protection Act). The Supreme Court had to decide whether English law allowed it to award a uniform, lowest common denominator sum in damages for "loss of control" of data under data protection statute. Such a finding would have opened the floodgates to class actions; people would have been held to share the "same interest" in the claim, allowing one individual to sue as a representative of the whole group.*

"The UK courts have previously recognised that loss of control is a harm to people's personal autonomy and dignity in misuse of private information (the Gulati phone hacking case). In this case the Supreme Court decided that the facts didn't warrant compensation for everyone. To achieve an award of damages the court made clear you have to prove facts and show that they caused financial harm or mental distress. Loss of control by itself was not enough to warrant compensation.

The GDPR provides that every individual has the right to "an effective judicial remedy" (Article 79) as well as a specific statutory right to receive compensation for damage (Article 82.1), which survive in UK law post Brexit in UK GDPR. It also refers expressly to material and non-material harm

People are concerned about what is being done with their information. Businesses should expect to see the points run again in the future in relation to different facts – and under the new law. The use of a two stage process (as has been adopted in other causes of action based upon Article 8 such as defamation for example) may be adopted in data protection litigation.

Make sure your data protection and cyber and data security meets the standard the law requires – or risk being sued is still the message."

Herbert Smith Freehills Partner Greig Anderson, who focuses on insurance disputes, said: "*One of the first questions a business will ask is whether my claim is insured – costs alone of a data class action may be eye watering and, while group data claims remain a threat, a judgment for the claimants would have marked a sea-change in exposure for insurers. The cyber insurance market typically covers data related claims but is already a very challenging environment for policyholders and is hardening quickly, making it a seller's market. Whilst the door has been left open, it is unclear how the market would have reacted to yet further enhanced exposure had the floodgates been opened, whether by putting up price further, reducing limits or even excluding or withdrawing cover, which has tended to be the approach of the insurance market more generally to emerging risks such as cyber and COVID-19. It is to be hoped that the cyber market will now have the opportunity to stabilise pricing and cover, and thus remain a realistic risk transfer option for policyholders, with a wait and see approach to whether claimants will seek to bring representative actions to establish liability as part of two stage process: just now, that possible exposure will be hard to project.*

"*We should not forget too that the potentially insurable impact is not just about the data class actions. For example, if the events resulting in a data class action were also to result in knock on regulatory action, securities claims or derivative claims against directors, D&O coverage will be implicated; as may PI cover for firms or companies that are considered by their customers or clients to be responsible for a data class action against them. The difficulty is that the insurance market is already seeking to affirm or exclude cover for cyber risks, which is leaving gaps in cover and the impact of a serious new exposure would have had the potential to widen these gaps, although the issue still remains.*"

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

JULIAN COPEMAN
PARTNER, LONDON, NON-RESIDENT PARTNER, HONG KONG, LONDON
+44 20 7466 2168
Julian.Copeman@hsf.com

MIRIAM EVERETT
PARTNER, LONDON
+44 20 7466 2378
Miriam.Everett@hsf.com

ANDREW MOIR
PARTNER, INTELLECTUAL PROPERTY AND GLOBAL HEAD OF CYBER & DATA SECURITY, LONDON

KATE MACMILLAN
CONSULTANT, LONDON
+44 20 7466 3737
kate.macmillan@hsf.com

+44 20 7466 2773
Andrew.Moir@hsf.com

GREIG ANDERSON
PARTNER, LONDON

+44 20 7466 2229
Greig.Anderson@hsf.com

MEDIA CONTACT

For further information on this news article, please contact:

CORINNE MCPARTLAND, COMMUNICATIONS LEAD

LONDON
Tel: +44 20 7466 2057
Mob: +44 7912 394 304
Email: corinne.mcpartland@hsf.com