UK Court Rejects Class-Action Claim Against Google For Privacy Breaches

Date : October 18, 2018

What is this about?

As we have recently reported, litigation in the form of class-actions/group actions, i.e. where a large number of individuals collectively try and obtain compensation caused by data protection infringements, is on the rise – see our general briefing on this here: http://www.corderycompliance.com/data-protection-breaches-and-compensation-litigation-issues-for-consideration/

A recent case brought against Google concerning several million individuals seeking several billion UK pounds in damages based on the unlawful collection and use of their personal data was thrown out by a judge for two main failings and is very instructive on important issues concerning making such class-action/group action claims.

What is the background to the case?

In this case an individual applicant was asking the court to be allowed to serve his claim on Google in the U.S. The claim alleged that Google had infringed the then existing UK data protection legislation because between June 2011 and February 2012 Google had secretly tracked the internet activity of Apple iPhone users, collating and using the information it obtained by doing so (more commonly known as “the Safari Workaround”) and then selling the accumulated data. This issue was also the basis of other well-known and ground-breaking litigation in the UK called the Vidal-Hall case, which we have written about here: http://www.corderycompliance.com/vidal-hall-data-protection-class-action-appeal-settled/

The applicant was trying to bring the case on behalf of a “class” of other end-users in the UK who it was claimed had also been affected by the Safari Workaround. The applicant sought to bring the claim as a so-called “representative action” on behalf of a class whose members were neither identified nor involved (who were very possibly not even aware of the claim); in contrast, the above-mentioned Vidal-Hall case was brought by three identified individuals.

The claim was for the members of the class to be compensated for “damage” (under the then existing UK data protection legislation). There was however no claim for financial loss or distress. The claim was for an equal, standard, “tariff” award for each member of the class, for infringement of their data protection rights, the commission of the wrong, and loss of control over personal data. Alternatively it was claimed that each class member was entitled to damages reflecting the value of the use to which the data were wrongfully put by Google. It was claimed that on either basis more than so-called “nominal damages” could be obtained by each claimant. No specific figure was put on the tariff, although ranges were put forward and a figure of £750 was put in the “letter of claim”.

On either basis it was claimed that the total damages that Google would have to pay would be calculated by multiplying the fixed sum awarded in respect of each class member by the number of individuals within the class. The class was a large one and estimates of its scale varied. The claimant’s best estimate at one stage was that it comprised as many as 5.4 million people. However, in the proceedings the estimate was reduced as the class was re-defined and refined. Nevertheless this still came to a substantial number at 4.4 million. Google’s estimate of the potential liability, if some of the claimant’s per capita figures for damages were accepted, was between £1 and £3 billion.

It wasn’t disputed that it was arguable that Google’s alleged role in the collection, collation, and use of data obtained via the Safari Workaround was wrongful. The two main issues to be decided were therefore: first, whether there was a basis for claiming compensation; and, second, if so, whether the court should or would permit the claim to continue as a so-called “representative action” (i.e. for the class).

What did the court decide?

The judge roundly rejected the application (calling it "officious litigation") answering these questions in the negative, for the following reasons. First, the facts alleged in the claim did not support the contention that the applicant or any of those whom he represented had suffered "damage" (under the terms of the then existing UK data protection legislation). Second, the members of the class did not have the "same interest" (under the applicable UK civil litigation procedural rules) and/or it was impossible reliably to ascertain the members of the represented class - the number, nature and extent of the breaches, and the impact of these breaches on individual members of such a very large class would have greatly varied (e.g. were the class members infrequent or heavy internet users, or what particular attitudes would they have about protecting their personal data etc.).

On the "damage" issue the judge made the following notable point (at paragraph 74 of the judgment):

"I do not believe that the authorities [caselaw] show that a person whose information has been acquired or used without consent invariably suffers compensatable harm, either by virtue of the wrong itself, or the interference with autonomy that it involves. Not everything that happens to a person without their prior consent causes significant or any distress. Not all such events are even objectionable, or unwelcome. Some people enjoy a surprise party. Not everybody objects to every non-consensual disclosure or use of private information about them. Lasting relationships can be formed on the basis of contact first made via a phone number disclosed by a mutual friend, without asking first. Some are quite happy to have their personal information collected online, and to receive advertising or marketing or other information as a result. Others are indifferent. Neither category suffers from "loss of control" in the same way as someone who objects to such use of their information, and neither in my judgment suffers any, or any material, diminution in the value of their right to control the use of their information. Both classes would have consented if asked. In short, the question of whether or not damage has been sustained by an individual as a result of the non-consensual use of personal data about them must depend on the facts of the case."

Those involved in the claim have apparently said that they will appeal this ruling.

What are the takeaways?

The main takeaway is that compensation claims for privacy breaches cannot claim "damage" in a willy-nilly way – the basis and proof of actual "damage" must be made clear. Such damage doesn't have to be financial or material – it could include emotional harm such as distress. The second takeaway is that there are clearly obstacles in bringing this particular type of class-action/group action. This said, this case might not be such a deterrent to individuals seeking compensation, because, as stated, this case was brought under the previous UK data protection legislation and the heightened awareness of the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 and the number of reported major data security breaches might have sharpened the appetite of affected individuals to seek compensation for data protection infringements. If there is an appeal we will report on it when it is decided, when these takeaways can be reconsidered.

In order to reduce risk, ensure data protection compliance and avoid causing incidents that might give rise to possible compensation claims, organizations are reminded to put in place or review technical measures along with policies and procedures and train individuals accordingly. If incidents do occur and compensation claims are made, both the handling of such claims and any P.R. communications that might be made about such incidents will also need to be thought through very carefully.

The judgement can be found here: https://www.judiciary.uk/judgments/lloyd-v-google/

We report about data protection issues including litigation here: http://www.corderycompliance.com/category/data-protection-privacy/. For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the security aspects of GDPR in paper and on film;
- A template data breach log;
- A template data breach plan; and,
- A template data breach reporting form.
- For more on Navigator please see here: http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/.

For more information please contact André Bywater or Jonathan Armstrong who are commercial lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com