Representative Actions in Data Breach Claims: An Update

Alex Platts

Barrister

St John's Buildings

Representative actions in data breach claims have featured in the media multiple times in recent weeks, underlining the significance of the upcoming appeal to the Supreme Court in Lloyd v Google.

On 28 February 2021, the Mail Online reported that a representative claimant, Ms Liz Williams, has filed for damages against credit firm Experian for selling the personal data of individuals for financial gain.[1] The claim follows the ICO publishing an enforcement notice in October 2020 after their finding that Experian were giving the data of individuals to third parties without consent, and threatening a £20 million fine unless Experian are able to satisfy the ICO that it has improved its practices sufficiently. Experian have appealed against this finding.

Ms Williams is seeking £750 in damages (this being equivalent to the award in *Halliday v Creation Consumer Finance* [2013] EWCA Civ 333 to compensate Mr Halliday's frustration after the Defendant failed to correct his credit records, despite requests). According to the Mail Online report, if the claim proves successful then up to 95% of the adult population in this jurisdiction could receive the same amount of damages as Ms Williams.

This follows news in early February that Mr Peter Jukes, a journalist, has filed a claim against Facebook for a loss of control over his personal data between November 2013 and May 2015. As a CityAM article notes, Mr Jukes is seeking to bring this as a representative action on behalf around 1 million other affected Facebook users in this jurisdiction.[2]

Alongside this litigation news, on 23 February 2021 the government published its Response to Call for Views and Evidence – Review of Representative Action Provisions, which focused primarily on whether new legislation should be implemented to enable non-profit organisations to bring actions on behalf of claimants without their express consent.[3]

As background, Article 80(1) UK GDPR effectively provides an "opt-in" system whereby a data subject may elect for a suitable not-for-profit body, organisation or association to bring a claim on

[1] https://www.dailymail.co.uk/news/article-9307429/Almost-adult-England-Wales-share-34-BILLION-High-Court-case.html
[2] https://www.cityam.com/journalist-sues-facebook-over-loss-of-control-of-personal-data/
[3] https://www.gov.uk/government/publications/call-for-views-and-evidence-review-of-representative-action-provisions-section-189-data-protection-act-2018/uk-government-response-to-call-for-views-and-evidence-review-of-representative-action-provisions-section-189-data-protection-act-2018

their behalf. As the Response noted, whilst this sub-article is currently in force, there has been a low uptake from individuals of this provision.

The Response considered whether Article 80(2) UK GDPR should be implemented. This would permit "*any body, organisation or association"* to act on behalf of individuals *"independently of a data subject's mandate*". Effectively, it would allow a legislative route for "opt-out" proceedings to be brought in data protection cases.

As the Response summarised, privacy groups, consumer rights groups and children's rights organisations had argued that this implementation is required to enable NGOs to complain to the ICO or to bring legal proceedings against data controllers on behalf of people who may not be able to represent themselves (1.5 of the Response). This stance was opposed by business groups, who point to the potential for increased litigation and the negative consequences of this on both businesses and, potentially, consumers (1.6), and that new legislation could increase uncertainty for data controllers.

The Response concluded that Article 80(2) should not be implemented at present, citing wariness of the "*risk of unintended consequences*" if this was done, such as increases in litigation costs and insurance premiums during a period of economic uncertainty (6.16).

Perhaps unsurprisingly given the issues reviewed, the Response expressly referred to the upcoming appeal in the Supreme Court of Lloyd v Google, stating that "[t]*he government will continue to monitor developments in this area closely*" (6.17). It appears that the government are allowing the courts the opportunity to make the first move within this sphere.

The significance of the Lloyd v Google case has already been widely discussed. In brief, Mr Lloyd, a former director of Which?, brought an action against Google for (it is claimed) circumventing the requirement for consent in tracking information. Mr Lloyd brought the action as a representative of a class of more than 4 million Apple iPhone users who, he alleges, were the victims of Google secretly tracking their internet activity for commercial purposes between August 2011 and February 2012.

Mr Lloyd sought to rely upon CPR 19.6 in order to bring this action on behalf of this huge class of people. This provision allows one person to bring an action as a representative of other individuals who have "the same interest" in the claim.

Warby J at first instance found that Mr Lloyd was unable to establish that the 4.4 million people he sought to represent had the "same interest" in this action, and that those 4.4 million people were not ascertainable as members of a specific, identifiable class.[4]

The Court of Appeal disagreed, and found that Warby J had "*applied too stringent a test of "same interest""*".[5] Sir Geoffrey Vos, providing the leading judgment, found that given the affected individuals were not seeking to rely upon any personal circumstances affecting them individually, the represented parties did have the same interest so as to allow Mr Lloyd to bring the action:

> "*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* [browser generated information]".[6]

It appears that the Court of Appeal's judgment on this point flows from its finding earlier in the judgment on whether the claimants had suffered "damage" on these facts. Where Warby J considered that none of the represented class had suffered "damage" under s13 DPA 1998, the Court of Appeal found that "loss of control" over personal data could constitute sufficient damage for compensation to flow (at least on this factual matrix). Given that finding, the Court of Appeal considered that there was sufficient commonality between the claimants represented by Mr Lloyd for CPR 19.6 to be engaged. Each of the 4.4 million claimants had suffered the same "loss of control", and their personal reactions to this loss of control were irrelevant given the way in which this case had been brought.

Much ink has already been spent on the issue of whether the Court of Appeal was correct in finding that the "loss of control" in this case could attract compensation, and it is not the purpose of this article to add to that literature in any depth. Suffice it to say that, should the Supreme Court uphold the Court of Appeal's finding on this point, it might be expected that it would stress that this "loss of control" has to be considered within the context of Google (allegedly) gaining commercial advantage from processing the personal data of individuals without consent. Otherwise, virtually every Article 5(1) UK GDPR breach (which usually amounts to a form of "loss of control") could attract

[4] *Lloyd v Google LLC* [2018] EWHC 2599 (QB), [89]-[92]and [94].
[5] *Lloyd v Google LLC* [2019] EWCA Civ 1599, at [75].
[6] *Ibid.*

compensation, even in cases where that breach is accidental, the data concerned is trivial and the data subject concerned is indifferent to the breach. It should be stressed that the Court of Appeal expressly sought to reject that this could be the consequence of their decision at [55] of their judgment.

Of course, the Supreme Court may overturn the Court of Appeal's finding on this point, and rule that mere "loss of control" is insufficient "damage" to attract compensation under the DPA 1998 without evidence of its consequences upon the victims of that data breach (i.e. material damage or distress). If so, then Mr Lloyd's claim would fail at the first hurdle, and the Supreme Court would not be obliged to determine the issue of whether CPR 19.6 could allow Mr Lloyd to bring this claim on behalf of over 4 million claimants (although it may address this in obiter).

This could leave the question of whether CPR 19.6 can be relied upon in large-scale data breach representative actions unanswered. Would the government revisit the question of whether Article 80(2) UK GDPR should be implemented at that point? Or would it allow the courts to determine the issue in future litigation (perhaps even in the Experian or Facebook litigation)? Given the findings within the government's Response, I suspect the latter.

It goes without saying that everyone involved in data protection law eagerly awaits the Supreme Court's decision in Lloyd v Google. No date has yet been confirmed for this hearing, but it is expected to be heard later this year (permission to appeal having been granted in March 2020). The Experian and Facebook litigation and the government's Response to the Review of Representative Action Provisions provide examples and indicators of just how consequential the decision could be in establishing the landscape of our data protection law in the post-Brexit era.

Alex Platts

March 2021

clerk@stjohnsbuildings.co.uk