Lloyd v Google: towards a more restrictive approach on privacy protection in the UK?

Eleni Frantziou 2021-11-22T11:51:26

On 10 November, the UK Supreme Court delivered its much-awaited judgment in Lloyd v Google. The case was a representative claim for damages under the Data Protection Act 1998 (the implementing legislation of the EU Data Protection Directive in the UK), brought by Richard Lloyd – former executive director of the consumer reviews company *Which?* – on behalf of more than four million iPhone users, who had suffered data breaches through Google's covert placing of advertising cookies on the Safari web browser between August 2011 and February 2012. In a unanimous judgment, the Supreme Court found in favour of Google, reversing an earlier judgment in Lloyd's favour by the Court of Appeal.

The case is highly significant for the development of privacy law in the United Kingdom and addresses three questions of wider interest from the perspective of European and comparative constitutional law:

1. Does mere 'loss of control' over personal data amount to compensable damage under EU law? The Supreme Court finds that it does not, at least under the pre-GDPR framework;
2. Does each individual member of a class action have to prove damage to obtain compensation? The Supreme Court answers this question affirmatively, thus practically precluding further class actions in this field;
3. Should common law causes of action, such as misuse of private information, which have been developed in the UK in the light of Article 8 ECHR, and actions arising from EU law, be given the same treatment in remedial terms, considering both types of action have a common source in the fundamental right to privacy? The Supreme Court answers this question in the negative, which may be suggestive of a broader hesitancy to unify human rights standards stemming from EU law and the ECHR in the future – an issue of increased relevance in the post-Brexit constitutional landscape in the UK.

The Supreme Court's answers to these questions paint an overly thin picture of data privacy and raise important concerns about possible divergence from EU standards in the future.

Loss of control over personal data

It was not disputed that Google placed advertising cookies in Safari browsers of iPhone users in the above-indicated period– an issue known as 'the Safari workaround', which was previously addressed by the Court of Appeal in *Vidal-Hall*

v Google (Google eventually settled that case and it never went to the Supreme Court). In *Vidal-Hall*, the Court of Appeal found that aspects of Section 13 DPA, which set out the possibility of compensation for distress due to data breaches following material damage only, were incompatible with the Data Protection Directive read in the light of Article 8 of the Charter and the right to an effective remedy protected in Article 47 thereof. The Court of Appeal therefore disapplied this provision in part (Section 13(2) DPA) and read the concept of 'damage' (Section 13(1) DPA) widely, so as to encompass distress. The *Lloyd* case was predicated upon a *Vidal-Hall* argument, namely that there should be no need to show that distress had been sustained on an individual basis, because everyone who was a member of the represented class (Safari on iPhone users in the relevant period) had suffered the loss of control over their personal data as a minimum common denominator, which in itself amounted to 'damage'. The Supreme Court rejected this argument, finding that it would amount to reading the concept of 'damage' in a manner that could not be justified by the wording of the DPA. As Lord Legatt put it, '*To say, as the claimant does in its written case, that what is "damaged" is the data subject's right to have their data processed in accordance with the requirements of the Act does not meet this point, as it amounts to an acknowledgement that on the claimant's case the damage and the contravention are one and the same*' [115]. The Supreme Court noted that no EU member state had, at the relevant time, legislated to protect against the mere loss of control over one's data, rather than for damage suffered thereby [122].

To my mind, these findings construe the idea of non-material damage as a result of privacy violations too narrowly. While it is true that Article 23 DPD was not as clear as Article 82 GDPR in protecting against non-material damage, the very same question of whether the data breach is in itself a form of damage has now arisen under the GDPR. It is noteworthy that the judgments of national courts confronted with this issue elsewhere in Europe, such as in Germany, Bulgaria and Austria, acknowledge that it raises important interpretive difficulties and have referred questions about the appropriate interpretation of EU law in this respect to the CJEU (currently pending: see here and here). Various comments in German case law suggest that a 'modern approach' should now be taken: recognising the data breach as 'non-material damage' follows from the fundamental character of the right to privacy and the need to protect it effectively, as causality is otherwise difficult to prove in these cases. It should be noted, for the purposes of clarity, that the possibility of a preliminary reference was not open to the Supreme Court in this case, as the Brexit implementation period has now expired. The case is also not directly authoritative in respect of prospective case law concerning the GDPR itself, rather than the pre-2018 legal framework only. Nevertheless, as the same issue has arisen in respect of the GDPR framework, it will be interesting to see whether the Supreme Court will in future choose to follow its own interpretation in *Lloyd v Google* or that of the CJEU, should the latter set a higher standard for privacy protection (i.e. a lower threshold for what is meant by non-material damage).

It is also essential to query what the claimant must actually prove in order for non-material damage to be successfully remedied in the UK. The Court's reasoning on this point appears to me to engender a problematic conflation in practice of the

conceptual element of the case, that is, whether the loss of control over one's data amounts to a compensable harm suffered by all victims of a data breach, with its evidential component, that is, whether the claimant has to prove that they actually suffered this damage (i.e. that they were in fact a victim of the data breach, and not just someone who happened to own an iPhone at the relevant time). *Vidal-Hall*, where damage for distress was recognised, is cited approvingly in the judgment [43], yet it is unclear how the two cases should be reconciled. The focus of *Vidal-Hall* was not on proving distress, and the Court of Appeal had simply found that '[*i*]*t is the distressing invasion of privacy which must be taken to be the primary form of damage (commonly referred to in the European context as „moral damage") and the data subject should have an effective remedy in respect of that damage*' [77]. In light of this, the Supreme Court's analysis could be read at best as maintaining the prospect of recovery for non-material damage such as distress in theory, but only after surpassing a more significant evidential threshold of proving victim status, or as substantively reducing the prospect of compensation by taking a stricter view of what amounts to an actionable, non-trivial breach of privacy [153] than the Court of Appeal in *Vidal-Hall*. This could have important implications both for the future of collective privacy claims in the UK, as well as for the future of the UK's post-Brexit privacy landscape, more widely.

The future of privacy class actions

The clearest and most immediate bearing of the case is that it nearly wipes out the possibility of large-scale class actions on privacy before UK courts and will thus surely be welcomed by data controllers. This is an interesting development, as it is a further indication of prospective divergence from EU rules. Taking note of the difficulties in bringing class actions across several Member States, on 25 November 2020 the European Union adopted a directive to regulate and facilitate collective actions, which will also cover actions regarding data breaches. This directive will not, however, affect the UK, as it is only scheduled to enter into force in 2023. The judgment in *Lloyd v Google* means that claimants in representative actions will have to be able to prove that they suffered the same non-material damage beyond the mere data breach (e.g., the same level of distress). This significantly reduces the feasibility of class actions and, unless Parliament decides to address the issue, the UK will not keep pace with emerging EU standards in this regard.

The future unavailability of class actions is also likely to signal a decline in privacy litigation more generally, as the impossibility of forming part of a broad represented class would make going to court financially unsustainable for many affected parties. The judgment suggests that this is all the better, as these types of claims are nothing short of 'officious' litigation for 'trivial' harm ([158] and [153]), rather than amounting to serious attempts to protect a fundamental right by continual attacks by private actors. That raises, in my view, a final, conceptually significant aspect of the ruling, as it suggests an understanding of privacy whereby data protection enjoys a lower constitutional pedigree than the protection of reputation or of the collection, processing or publication of private information.

The rejection of the ‘common source’ argument

Beyond the breadth of the class action, the main constitutional novelty in Mr Lloyd’s case was that he had pleaded an important point of principle: that all breaches of the fundamental right to privacy should be remedied in a similar manner, regardless of whether they consist in the covert use of advertising cookies, as in this case (an area regulated by EU secondary legislation read in the light of Article 8 of the Charter) or in the unauthorised collection and/or publication of a person’s private information (an area also regulated by the tort of misuse of private information under the common law, interpreted in the light of Article 8 ECHR). As that argument goes, whereas EU law and ECHR law have operated as two separate streams of rights protection in the UK, there is no principled basis for distinguishing the rules of compensation under Article 8 of the Charter and Article 8 ECHR, as these rights are drawn from a common source: the fundamental right to privacy (albeit that its EU protection eventually went beyond the minimum standard set out in the ECHR in terms of data privacy). The Supreme Court emphatically rejected this contention. Devoting to it a subsection entitled ‘flaws in the common source argument’ (at paras 124-129), it wholly distanced itself from the ‘common source’ approach, which had found favour before the Court of Appeal, and affirmed the existence of a bright-line divide between the EU and ECHR conceptions of privacy. This is an important gesture regarding the way in which the Supreme Court views the relationship between EU and ECHR law in the future, which raises concern about a potentially more deferential approach towards the application of human rights to disputes between private parties by domestic courts.

The reason for Mr Lloyd advancing the ‘common source’ argument was that this is an area where domestic law interpreted in line with Article 8 ECHR had offered precisely what he was seeking: damages for the loss of control over private information. In its judgment in *Gulati v MGN,* the Court of Appeal had found that such ‘damages are an award to compensate for the loss or diminution of a right to control formerly private information,’ [48] the basis for which was none other than that ‘privacy is a fundamental right’ [46], of which domestic courts had to ensure the effective protection. Whereas the Supreme Court’s judgment in *Lloyd v Google* does not overrule *Gulati*, it painstakingly seeks to show that the protection of private data under EU law is not only a separate, but also a less significant category of privacy protection than cases about the targeted interception of private data (e.g. phone hacking), when seen from the ECHR perspective (i.e. the only authoritative external perspective on human rights in the UK post-Brexit). To do so, Lord Leggatt cites the ECtHR’s case law on protective duties, which affords states a wide margin of appreciation in respect of the balance struck between the right to private and family life and the interests of other private actors [*Lloyd v Google*, 125]. Nevertheless, Lord Leggatt’s reliance on ECtHR case law about employment monitoring, such as *B#rbulescu v Romania,* is not wholly convincing in this context and comes across as overly selective.

First, while the case law on employee monitoring is useful in appreciating that contracting parties enjoy a margin of appreciation in respect of whether and how they legislate for the application of the right to privacy in disputes between private

actors, that case also lists a series of considerations that national courts must take into account when they are confronted with a privacy claim against a private actor (most notably, requirements of notice and reasons, at para 121 of *B#rbulescu*), which were not present in *Lloyd v Google*. Secondly, the Supreme Court's analysis lacks references to the increasing tendency of the ECtHR to accept data protection as an intrinsic part of the right to private life. For example, in *Big Brother Watch*, the ECtHR accepted that there was in principle no difference between the anonymised and the targeted collection of private data, noting that advances in technology meant that '*metadata could paint a detailed and intimate picture of a person: they allowed for mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with*' [317].

Of course, Mr Lloyd did not argue that he had a claim in misuse of private information, so that the Supreme Court's analysis can simply be read as a summary of the differences between the two streams of protection, without precluding the possibility of misuse of private information developing in a way that comprises a high level of data privacy in the future. But a more sinister reading of the judgment might be that it maintains a remedial fragmentation of privacy in the UK, which is undesirable from the perspective of legal certainty and indicative of a potential reduction of data protection to the minimum allowed under the Convention in the future. It is perhaps especially disappointing that *Lloyd v Google* is a unanimous judgment delivered in a single speech, so that there is no opportunity to compare different views on how *Gulati* should be interpreted, particularly as Lady Arden, one of the sitting judges at the Supreme Court, had delivered the lead judgment in that ruling as a Court of Appeal judge.

Conclusion

The overall implications of *Lloyd v Google* are threefold: first, the judgment has a chilling effect on further class actions against Internet actors for violations of the right to privacy; secondly, it maintains dissonance between the remedies available for breaches of the EU and common law/ECHR aspects of the right to privacy; and, finally, it paves the way for a more cautious approach towards privacy claims, which tracks the minimum permissible standard under the Convention. In each of these respects, *Lloyd v Google* is, in my view, a judgment that puts pragmatism over principle. Most crucially perhaps, the manner in which the Court weighs up the leeway afforded to it under Article 8 ECHR, rather than setting out a high a level of data privacy as a domestic constitutional commitment independently of the Convention, could be thought to form part of a broader judicial retreat to rulings displaying technical skill, but proffering little by way of constitutional innovation.