Has the Battle Just Begun for Collective Action against Big Tech Companies?

*Julia Hörnle, Professor of Internet Law, CCLS, Queen Mary University of London****[1]***

It is now well known that internet users are widely tracked and profiled by a range of actors and the advancements in data science mean that such tracking and profiling is increasingly commercially profitable[2]. This raises difficult questions about how to balance the value of data with individual privacy. But since there is no point in having privacy (or data protection) rights if no redress can be found to vindicate them, it is even more important to investigate *how* internet users can obtain justice, if their privacy has been infringed. Given the power of Big Tech Companies, their enormous financial resources, cross-jurisdictional reach and their global impact on users' privacy, there are two main litigation challenges for successfully bringing a privacy claim against Big Tech. One is the jurisdictional challenge of finding a competent court in the same jurisdiction as the individual users.[3] Secondly, the challenge is how to finance mass claims, involving millions of affected users. In privacy claims it is likely that there is significant user detriment, potentially with long-term and latent consequences, which are difficult to measure. This constellation provides a strong argument for facilitating collective redress, as otherwise individual users may not be able to obtain justice for privacy infringements before the courts. In privacy infringement claims these two challenges are intertwined and present a double-whammy for successful redress. Courts in a number of recent cases had to grapple with questions of jurisdiction in consumer collective redress cases in the face of existing provision on consumer jurisdiction and collective redress, which have not (yet) been fully adapted to deal with the privacy challenges stemming from Big Tech in the 21st century.

In Case C-498/16 *Max Schrems v Facebook Ireland****[4]*** the Court of Justice of the EU in 2018 denied the privilege of EU law for consumers to sue in their local court[5] to a representative (ie *Max Schrems*) in a representative privacy litigation against Facebook under Austrian law. By contrast, courts in California

and Canada have found a contractual jurisdiction and applicable law clause invalid as a matter of public policy in order to allow a class action privacy claim to proceed against *Facebook*.[6] In England, the dual challenge of jurisdiction and collective actions in a mass privacy infringement claim has presented itself before the English Courts, first in *Vidal-Hall v Google* before the Court of Appeal in 2015[7] and in the Supreme Court judgment of *Google v Lloyd* in November 2021[8]. Both cases concerned preliminary proceedings on the question of whether the English courts had jurisdiction to hear the action, ie whether the claimant was able to serve Google with proceedings in the USA and have illustrated the limitations of English law for the feasibility of bringing a collective action in mass-privacy infringement claims.

The factual background to *Vidal- Hall* and *Lloyd* is the so-called "Safari workaround" which allowed Google for some time in 2011-2012 to bypass Apple privacy settings by placing DoubleClick Ad cookies on unsuspecting users of Apple devices, even though Safari was trying to block such third party cookies, used for extensive data collection and advertising. The claimants alleged that this enabled Google to collect personal data, including sensitive data, such as users' interests, political affiliations, race or ethnicity, social class, political and religious beliefs, health, sexual interests, age, gender, financial situation and location. Google additionally creates profiles from the aggregated information which it sells. The claim made was that Google as data controller had breached the following data protection principles set out in the Data Protection Act 1998 Schedules 1 and 2: 1st (fair and lawful processing), 2nd (processing only for specified and lawful purposes) and 7th (technical and organizational security measures). In particular, it was alleged that Google had not notified Apple iPhone users of the purposes of processing in breach of Schedule 1, Part II, paragraph 2 and that the data was not processed fairly according to the conditions set out in Schedules 2 and 3.

Vidal-Hall[9] concerned the first challenge of jurisdiction and in particular whether the court should allow the serving of proceedings on the defendant outside the jurisdiction under the Civil Procedure Rules[10]. For privacy infringement, previous actions had been brought under the cause of action of breach of confidence[11], which is a claim in equity and, thus it was unclear whether for such actions jurisdiction lies at the place of where the damage occurs. The Court of

Appeal held that misuse of private information and contravention of the statutory data protection requirements was a *tort* and therefore, if damage had been sustained within England, the English courts had jurisdiction and service to the USA (California) was allowed.

The second hurdle for allowing the case to proceed by serving outside the jurisdiction was the question of whether the claimant was limited to claiming financial loss or whether a claim for emotional distress could succeed. The Court of Appeal in *Vidal-Hall* decided that damages are available for distress, even in the absence of financial loss, to ensure the correct implementation of Article 23 of the (then) Data Protection Directive, and in order to comply with Articles 7 and 8 of the Charter of Fundamental Rights of the EU. The Court therefore found that there was a serious issue to be tried and allowed service abroad to proceed, at which point the case settled.

The more recent English Supreme Court judgment in *Lloyd* concerned the second challenge, collective redress. As pointed out by Lord Leggatt in the judgment, English procedural law provides for three different types of actions: Group Litigation Orders (CPR 19.11), common law representative actions, and statutory collective proceedings under the Competition Act 1998. Their differences are significant for the purposes of litigation financing in two respects: first the requirement to identify and "sign-up" claimants and secondly, the requirement for individualized assessment of damages. Since both these requirements are expensive, they make collective redress in mass privacy infringement cases with large numbers of claimants impractical.

Group actions require all claimants to be identified and entered in a group register ("opt-in") and are therefore expensive to administer, which renders them commercially unviable if each individual claim is small and if the aim is to spread the cost of litigation across a large number of claimants.

English statutory law in the shape of the Competition Act 1998 provides for collective proceedings before the Competition Appeal Tribunal in competition law cases only.[12] Since the reforms by the Consumer Rights Act in 2015, they can be brought under an "opt-in" or "opt-out" mechanism. Opt-out means that a class can be established without the need for affirmative action by each and every member of the class individually. The significance of this is that it is notoriously difficult (and expensive) to motivate a large number of consumers to join a

collective redress scheme. Human inertia frequently prevents a representative claimant from joining more than a tiny fraction of those affected. For example, 130 people (out of 1.2-1.5 million) opted into the price-fixing case against JJB Sports concerning replica football shirts.[13] Likewise, barely 10,000 out of about 100,000 of Morrison's employees joined the group action against the supermarket chain for unlawful disclosure of private data on the internet by another employee.[14] Furthermore, s.47C (2) of the Competition Act obviates the need for individual assessment of damages, but limits the requirement to prove damages to the class as a whole, as an aggregate award of damages, as held by Lord Briggs in *Merricks v Mastercard****[15]***. However no such advanced scheme of collective redress has yet been enacted in relation to mass privacy infringement claims.

While the Supreme Court held that Mr Lloyd's individual claim had real prospect of success, the same could not necessarily be said of everyone in the class he represented. This case was brought as a *representative action* where Mr Lloyd represented the interests of everyone in England and Wales who used an iPhone at the relevant time and who had third party cookies placed by Google on their device. One of the interesting features of representative actions is that they can proceed on an opt-out basis, like the collective actions under the Competition Law Act. *Common law* representative actions have been established for hundreds of years and have now been codified in CPR Rule 19.6: "Where more than one person has the *same interest* in a claim by or against one or more of the persons who have the same interest as representatives of any other person who have that interest". Thus representative actions are based on the *commonality of interest* between claimants. The pivotal issue in *Lloyd* was the degree of commonality of that interest and in particular, whether this commonality must extend to the losses, which claimants have suffered, and proof of damages.

Lord Leggatt in *Lloyd* emphasized the spirit of flexibility of representative actions. Previous caselaw in the Court of Appeal had held that it was possible for claimants to obtain a declaration by representative action, which declares that they have rights which are common to all of them, even though the loss and amount of damages may vary between them.[16] He held that a bifurcated approach was permissible: a representative action can be brought seeking a declaration about the common interests of all claimants, which can then form the basis for individual claims for redress. Lord Leggatt held that, depending on the

circumstances, a representative action could even be brought in respect of a claim for damages, if the *total amount of damages could be determined for the class as a whole*, even if the amount for each individual claimant varied, as this was a matter which could be settled between the claimants in a second step. He held that, therefore, a representative action can proceed even if a claim for damages was an element of the representative action, as in *Lloyd*.

Lord Leggatt found that the interpretation of what amounts to the "same interest" was key and that there needed to be (a) common issue(s) so that the "representative can be relied on to conduct the litigation in a way which will effectively promote and protect the interests of all the members of the represented class."[17] The problem in *Lloyd* was that the total damage done to privacy by the Safari workaround was unknown.

Lord Leggatt saw no reason why a representative action for a declaration that Google was in breach of the Data Protection Act 1998, and that each member was entitled to compensation for the damage suffered as a consequence of the breach, should fail. However, commercial litigation funding in practice cannot fund actions seeking a mere declaration, but need to be built on the recovery of damages, in order to finance costs. In order to avoid the need for individualised damages, the claim for damages was formulated as a claim for *uniform per capita* damages. The problem on the facts of this case was clearly that the Safari workaround did not affect all Apple users in the same manner, as their internet usage, the nature and amount of data collected, as well as the effect of the data processing varied, all of which required individualised assessment of damages.

For this reason, the claimant argued that an infringement of the Data Protection Act 1998 leads to automatic entitlement to compensation without the need to show *specific* financial loss or emotional distress. This argument proved to be ultimately unsuccessful and therefore the claim failed. The Court examined Section 13 of the Data Protection Act 1998, entitling the defendant to compensation for damage, but the court held that each claimant had to prove such damage. The level of distress varied between different members of the represented class, meaning that individual assessment was necessary.

The claimant sought to apply the cases on the tort of misuse of private information by analogy. In this jurisprudence the courts have allowed for an award of damages for wrongful intrusion of privacy as such, without proof of

distress in order to compensate for the "loss of control" over formerly private information.[18] Lord Leggatt pointed out that English common law now recognized the right to control access to one's private affairs and infringement of this right itself was a harm for which compensation is available.

However in this particular case the claim had not been framed as the tort of misuse of private information or privacy intrusion, but as a breach of statutory duty and Lord Leggatt held that the same principle, namely the availability of damages for "loss of control" did *not* apply to the statutory scheme. He pointed out that it may be difficult to frame a representative action for misuse of private information, as it may be difficult to prove reasonable expectations of privacy for the class as a whole. This may well be the reason that the claim in this case was based on breach of statutory duty in relation to the Data Protection Act. Essentially the argument that "damages" in Section 13 (1) included "loss of control" over private data was unsuccessful. Both Article 23 of the Data Protection Directive and Article 13 made a distinction between the unlawful act (breach of data protection requirements) and the damage resulting, and did not conceive the unlawful act itself as the damage. Furthermore, it was not intended by the Directive or the Act that each and every contravention led to an entitlement to damages. He held that "loss of control" of personal data was not the concept underlying the data protection regime, as processing can be justified by consent, but also other factors which made processing lawful, so the control over personal data is not absolute.

Furthermore, it did not follow from the fact that both the tort of misuse of private information and the data protection legislation shared the same purposes of protecting the right to privacy under Article 8 of the European Convention of Human Rights that the same rule in respect of damages should apply in respect of both. There was no reason "why the basis on which damages are awarded for an English domestic tort should be regarded as relevant to the proper interpretation of the term "damage" in a statutory provision intended to implement a European directive".[19] He concluded that a claim for damages under Section 13 required the proof of material damage or distress. He held that the claim had no real prospect of success and that therefore no permission should be given to serve proceedings outside the jurisdiction (on Google in the US).

This outcome of *Lloyd* raises the question in the title of this article, namely whether the cross-border battle on collective actions in mass privacy infringement

cases against Big Tech has been lost, or whether on the contrary, it has just begun. One could argue that it has just began for the reason that the facts underlying this case occurred in 2011-2012, and therefore the judgment limited itself to the Data Protection Act 1998 (and the then Data Protection Directive 1995/46/EC). Since then the UK has left the EU, but has retained the General Data Protection Regulation[20] ("the UK GDPR") and implemented further provisions in the form of the Data Protection Act 2018, both of which contain express provisions on collective redress. The GDPR provides for *opt-in* collective redress performed by a not-for-profit body in the field of data protection established for public interest purposes.[21] This is narrow collective redress as far removed from commercial litigations funders as possible. Because of the challenge of financing cross-border mass-privacy infringements claims, this is unlikely to be a practical option. The GDPR makes it optional for Member States to provide that such public interest bodies are empowered to bring *opt-out* collective actions for compensation before the courts.[22] These provisions unfortunately do not add anything to common law representative actions or group actions under English law. As has been illustrated above, representative actions can be brought on an "opt-out" basis, but have a narrow ambit in that all parties must have the *same interest in the claim* and *Lloyd* has demonstrated that in the case of distress this communality of interest may well defeat a claim. For group actions the bar of communality is lower, as it may encompass "claims which give rise to common or related issues of fact or law"[23]. But clearly the downside of group actions is that they are *opt-in*. Therefore, while English law recognizes collective redress, there are limitations to its effectiveness.

The Data Protection Act 2018 imposes an obligation on the Secretary of State to review the provision on collective redress, and in particular, consider the need for *opt-out* collective redress, and lay a report before Parliament. This may lead to Regulations setting out a statutory opt-out collective redress scheme for data protection in the future.[24] This Review is due in 2023.

Thus, the GDPR and the Data Protection Act 2018 have not yet added anything to the existing collective redress. It can only be hoped that the Secretary of State reviews the collective redress mechanisms in relation to data protection law and the review leads to a new statutory collective redress scheme, similar to that enacted in respect of Competition Law in 2015, thereby addressing the challenge of holding Big Tech to account for privacy infringement.[25]

However the new data protection law has improved the provision of *recoverable heads of damage*. This improvement raises the question, if the issues in *Lloyd* had been raised under the current law, whether the outcome would have been different. The Data Protection Act 2018 now explicitly clarifies that the right to compensation covers *both material and non-material damage* and that *non-material damage includes distress*.[26] Since non-material damage is now included in the Act, the question arises whether this new wording could be interpreted by a future court as including the privacy infringement itself (loss of control over one's data). Some of the arguments made by Lord Leggatt in *Lloyd* continue to be relevant under the new legislation, for example that the tort of statutory breach is different from the tort of misuse of private information and that not each and every (minor) infringement of a statute should give raise to an entitlement for damages. Nevertheless it is clear from the new Act that non-material damage is included and that non-material damage includes distress, but is wider than distress. This means that claimants should be able to obtain compensation for other heads of non-material damage, which may include the latent consequences of misuse of personal information and digital surveillance. There is much scope for arguing that some of the damage caused by profiling and tracking are the same for all claimants. A future representative action in an equivalent scenario may well be successful. Therefore, the battle for collective action against Big Tech companies' in privacy infringement cases may just have begun.

[1] J.hornle@qmul.ac.uk

[2] Shoshana Zuboff *The Age of Surveillance Capitalism* (2018)

[3] See further J. Hörnle, *Internet Jurisdiction Law & Practice* (OUP 2021)

[4] ECLI:EU:C:2018:37; discussed further in J. Hörnle fn 1 Chapter 8

[5] Ie the courts of the consumer's domicile, if the business directed their activities to that state, Art 17 and Art 18 (1) Brussels Regulation on Jurisdiction (EU) 1215/2021

[6] *In Re Facebook Biometric Information Privacy Litigation* 185 F.Supp.3d 1155 (US District Court N.D. California 2016) and *Douez v Facebook* [2017] SCC 33; discussed further in J. Hörnle fn 1 Chapter 8

[7] [2016] QB 1003

[8] [2021] 3 WLR 1268

[9] [2015] 3 WLR 409 (CA)

[10] CPR PD 6B para.3.1(9)

[11] *Campbell v MGN Ltd* [2004] 2 WLR 1232 (HL)

[12] Section 47B

[13] *The Consumers Association v JJB Sports Plc* [2009] CAT 2

[14] *Various Claimants v WM Morrisons Supermarkets Plc* [2017] EWHC 3113 (QB)

[15] [2021] Bus LR 25, para 76

[16] *David Jones v Cory Bros & Co Ltd* (1921) 56 LJ 302; 152 LT Jo 70

[17] Paras 71-74

[18] by Mann J affirmed in the Court of Appeal *Gulati v MGN Ltd* [2017] QB 149

[19] Para 124

[20] Regulation (EU) 2016/679, L119, 4 May 2016, p. 1–88

[21] Art 80 (1)

[22] Arts 79 and 80 (2) in relation to effective judicial remedies

[23] CPR Part 19- Group Litigation Orders, Rules 19.10, 19.11

[24] ss. 189-190

[25] The current government, however seems to march in the opposite direction, see Consultation on reform of data protection law https://www.gov.uk/government/consultations/data-a-new-direction

[26] S. 168 (1)