LLOYD V GOOGLE
THE UPSHOT FOR DATA CLASS ACTIONS

Julian Copeman, Andrew Moir, Miriam Everett, Greig Anderson, Kate Macmillan and Rachelle Waxman of Herbert Smith Freehills LLP discuss the outlook for data class actions following the Supreme Court's decision in *Lloyd v Google*.

The exponential growth in the volume of data being collected and shared, along with the ease and reduced costs of gathering, analysing, using and exploiting data, has resulted in a corresponding increase in data protection laws and regulations. Against that background, data class actions have been a growing phenomenon, driven in part by the interest of claimant law firms and litigation funders in this area.

The particular focus on data claims was boosted by the Court of Appeal's high-profile judgment in *Lloyd v Google LLC* in September 2019, as a result of which it appeared that claims for data breaches could be brought as opt-out style class actions under the representative action provisions in Civil Procedure Rule (CPR) 19.6 (*[2019] EWCA Civ 1599; see News brief "Data protection claims: a green light for representative actions", www.practicallaw.com/w-022-5323*).

However, in November 2021, the Supreme Court overturned that decision, finding that a claim cannot be brought under the Data Protection Act 1998 (DPA 1998) simply for an infringement of the data protection legislation (*[2021] UKSC 50; see News brief "Lloyd v Google: one door closes but another one opens?", www.practicallaw.com/w-033-4736*). There must be proof of damage resulting from the infringement in the form of either material damage, such as financial loss, or mental distress. Therefore, the representative action procedure is inappropriate for data claims where the court needs to consider individual cases to establish liability.

Although the Supreme Court's decision may have stemmed the otherwise potential flood of data class actions, it did not completely close the door on bringing data claims as representative actions. This article discusses the influence that the *Lloyd* litigation has had on data class actions and, in particular, the practical implications of the Supreme Court's judgment, including in relation to cyber incident-related data breaches and the role of insurance.

THE LLOYD LITIGATION

Mr Richard Lloyd, a former executive director of the UK Consumers' Association, brought a claim against Google LLC, seeking to use the representative action procedure under CPR 19.6. This allows a claim to be brought by one or more persons as representatives of any others who have the same interest in the claim (*see box "Representative actions under CPR 19.6"*). On this basis, Mr Lloyd sought to bring the claim on behalf of a class of more than four million UK-resident iPhone users, alleging that Google had secretly tracked some of their internet activity for commercial purposes in 2011 and 2012. At a putative tariff

of £750 per head, the ability to represent over four million claimants would result in a claim amounting to billions of pounds.

The claim relied on section 13(1) of the DPA 1998 (section 13), which provides a right of compensation where an individual suffers damage by reason of any contravention by a data controller of any of the requirements of the DPA 1998. The DPA 1998 was the law applicable at the time of the alleged breach, having since been replaced by the Data Protection Act 2018 (DPA 2018), the General Data Protection Regulation (*679/2016/EU*) (GDPR) and, after the end of the Brexit transition period, the retained EU law version of the GDPR (UK GDPR).

In bringing the action, Mr Lloyd disavowed any reliance on the individual circumstances of class members, arguing instead that damages could be awarded on the basis of an equal, standard tariff award for each class member to reflect the infringement of their rights and their loss of control over their personal data, ignoring any factors which might differentiate them and might mean that some of them had larger damages claims.

High Court judgment

The High Court refused to allow the action to proceed as a representative action under CPR 19.6, finding that a claim for compensation under the DPA 1998 requires proof of damage and Mr Lloyd had failed to identify any harm caused as a result of the alleged breach (*[2018] EWHC 2599 (QB)*). It held that compensation cannot be awarded merely for the fact of the infringement and associated loss of control over the personal data. In addition, the same interest requirement under CPR 19.6 was not met because the amount of compensation would still depend on the facts, as neither the breach of duty nor the impact of it would be uniform across the entire class membership.

In any event, the court stated that it would have exercised its discretion to refuse to allow the claim to proceed under CPR 19.6, taking into account various factors, including that:

- The costs were likely to be high.
- The compensation recoverable by each class member would be "modest at best".
- The main beneficiaries of any award would be the litigation funders and lawyers.
- It would be difficult to ascertain whether any given individual fell within the affected class.
- The class members had not authorised the claim.

Court of Appeal judgment

The Court of Appeal upheld Mr Lloyd's appeal, overturning the High Court's decision. In doing so, it found that damages are in principle capable of being awarded for loss of control of data, even if there is no pecuniary loss and no distress, subject to a threshold for a trivial or de minimis infringement.

The court held that the High Court had applied the same interest test too stringently for the purposes of CPR 19.6, partly because of its determination of the meaning of "damage" under section 13. The court considered that the represented class were all victims of the same alleged wrong, had all sustained the same loss of control over their personal data and were not seeking to rely on any individual personal circumstances. While this meant that any damages would be reduced to "what may be described as the lowest common denominator", the result was that it was impossible to imagine that a defence could apply to one represented claimant that did not apply to all of the others. In the court's judgment, therefore, the represented parties did have the same interest in the relevant sense under CPR 19.6.

As for the High Court's exercise of discretion, the court considered that the High Court had taken into account two irrelevant factors:

- The inability to identify the members of the class, as the court saw no reason why each class member could not be identified.

Representative actions under CPR 19.6

Civil Procedure Rule (CPR) 19.6 allows a representative action to be brought by, or against, one or more persons who have the same interest in a claim as representatives of any other persons who have that same interest, without the need to identify the represented parties. It is an opt-out procedure and can be used where it is impractical to join all of the affected members of a class to the litigation.

Where claimants are required to take steps to opt in to a group claim in the usual way, such as using the group litigation order procedure, participation tends to be quite low. For example, in the data breach group action in *Various Claimants v Wm Morrison Supermarkets Plc*, only about 10% of the potential class chose to opt into the proceedings (*see feature article "Data class actions: the outlook after Morrison", www.practicallaw.com/w-026-2617*). Conversely, because CPR 19.6 requires everyone in the class to have the same interest in the claim, it has proved difficult to use for mass claims, because the larger the class, the more likely that the interests of the claimants will differ (*see feature article "Class actions in England and Wales: key practical challenges", www.practicallaw.com/w-015-9333*).

In addition, the courts have applied the same interest requirement strictly and have emphasised the limits of the representative action procedure. For example, in *Emerald Supplies Limited and another v British Airways*, the Court of Appeal held that it would be inappropriate to bring a claim under CPR 19.6 if the class cannot be determined at the outset or if there is a conflict of interest because the remedy sought is not equally beneficial to all members of the class (*[2010] EWCA Civ 1284; see News brief "Different class: UK representative actions suffer a setback", www.practicallaw.com/7-504-0554*).

In *Jalla and another v Shell International Trading and another*, the Court of Appeal held that a claim in relation to an oil spill was unsuitable for a representative action procedure as the parties did not have the same interest in the claims "for all practical purposes" (*[2021] EWCA 1389; see News brief "Representative actions under CPR 19.6: still limited in scope", www.practicallaw.com/w-033-1153*). Each of the more than 28,000 claimants would have had to prove on an individual basis the loss or damage that they had suffered due to the oil spill.

- The fact that the members of the class had not authorised the claim.

It was therefore open to the court to exercise the discretion afresh. It concluded that the representative action should be allowed to proceed, for reasons including that, given the value of the individual claims and the cost of pursuing each one individually, this was in practice the only way in which the claims could be pursued.

Supreme Court judgment

The Supreme Court upheld Google's appeal and overturned the Court of Appeal's judgment. Mr Lloyd had argued that a uniform sum of damages could be awarded to each class member on a tariff basis without the need to prove any facts particular to that individual. This was on the basis that compensation could be awarded under the DPA 1998 for the loss of control of personal data constituted by any non-trivial contravention of any of the requirements of the DPA 1998. Alternatively, Mr Lloyd argued that class members were entitled to "user damages" in the amount that they could reasonably have charged for releasing Google from the duties it had breached.

The court concluded that, in order to recover compensation under section 13, it is not enough to prove a breach; there must be some damage suffered as a consequence of that breach. On a proper interpretation, compatible with Article 23 of the Data Protection Directive (*95/46/EC*) (which applied at the relevant time), the term "damage" in section 13 refers to material damage such as financial loss or mental distress. This damage must be distinct from, and caused by, the unlawful processing of personal data. It cannot be the unlawful processing itself. By declining to plead individual causation and damage, the claim was bound to fail. This conclusion also precluded a claim for user damages based on a reasonable release fee for contravention of the right (*see box "Misuse of private information and user damages"*).

In any event, even if, contrary to the court's conclusion, it were unnecessary to show that an individual had suffered material damage or distress as a result of the unlawful processing, it would still be necessary to establish the extent of the unlawful processing in the individual case. In deciding what amount of damages, if any, should be awarded, relevant factors would include:

- The period of time over which the browsing history was tracked.
- The quantity of data that was processed unlawfully.
- Whether any of the information was of a sensitive or private nature.
- The use that was made of the information.
- What commercial benefit, if any, was obtained from using the information.

The generic facts that Mr Lloyd alleged in the claim could not establish that any individual class member was entitled to compensation, given that, as Mr Lloyd accepted, there is a threshold of seriousness that must be crossed before there is an entitlement to compensation under the DPA 1998. In other words, if limited to the "lowest common denominator", it was impossible to characterise the damage as more than trivial.

The court analysed the history and scope of the representative procedure under CPR 19.6, briefly comparing it to the two other methods of claiming collective redress currently available in English procedural law:

- The group litigation order (GLO), which can be an effective way of enabling large numbers of claims to be litigated and managed together, where they are of sufficiently high value. However, as it is an opt-in regime, where claimants must take active steps to join the group, it is uneconomic for claims that individually are of low value as the initial costs may easily exceed the potential value of the claim and because these actions often suffer from low participation rates.
- The collective proceedings regime for competition claims in the Competition Appeal Tribunal (CAT), subject to certification by the CAT as satisfying relevant criteria set out in statute. The court recognised the significant advantages for claimants, particularly where many people have been affected but the value of individual claims is small, because proceedings may be brought on an opt-out basis in appropriate cases, and the regime enables liability to be established and damages recovered on an aggregate basis, without proving individual losses by class members.

The representative action procedure has its origins in the procedure of the Court of Chancery, long before the Judicature Act 1873. The court noted that while the world has changed since then, it has done so in ways that have added to the potential for collective harm, such as through the industrial production of goods, the mass provision of services and the development of digital technologies.

Misuse of private information and user damages

The Supreme Court in *Lloyd v Google LLC* made a number of obiter comments in relation to claims for misuse of private information (*[2021 UKSC 50; see News brief "Lloyd v Google: one door closes but another one opens?", www.practicallaw.com/w-033-4736*). In contrast to a statutory claim, in a claim for misuse of private information, general damages can be awarded for the commission of the wrong itself as well as to compensate the claimant for distress, hurt feelings and loss of dignity. This is because the English courts have recognised privacy of information as worthy of protection in its own right (*Representative Claimants v MGN Limited [2015] EWCA Civ 1291*) (also known as *Gulati*).

As damages for the misuse of private information may be awarded on the basis that the defendant's conduct prevented the claimant from exercising their right to control the use of their information, the Supreme Court in *Lloyd* pointed out that a claim for misuse of private information would naturally lend itself to an award of user damages, based on a hypothetical fee to allow the relevant use of the information. The court was of the view that if a defendant's very purpose in wrongfully obtaining and using private information is to exploit its commercial value, the law should not be shy from awarding compensation based on the commercial value of the exercise of the right. Accordingly, it is to be expected that claimants will consider bringing representative actions in misuse of private information cases to recover user damages.

Given both the difficulty of litigating multiple individual claims and the impracticality of making every prospective claimant a party to a single claim, the court acknowledged that the only practical way to achieve justice in cases of collective harm is to combine the claims in a single proceeding and allow one or more persons to represent all of the others who share the same interest in the outcome. CPR 19.6 is "a flexible tool of convenience in the administration of justice", and the courts of Canada, Australia and New Zealand are right to have said that, while a detailed legislative framework would be preferable, the absence of such a regime does not mean that representative procedures should be avoided or interpreted restrictively.

The fact that the relief claimed includes damages is not a bar to a representative claim. However, since the aim of damages is to put the claimant in the same position as if the wrong had not occurred, this ordinarily requires an individualised assessment, which cannot fairly or effectively be carried out without the claimant's presence in the proceedings, and so a representative action would not be suitable in cases such as *Lloyd*. The court highlighted previous case law in which representative claims had been successfully brought in relation to issues of liability only, and in doing so said that this demonstrated the potential for a bifurcated process in which common issues of law or fact are decided through a representative claim, leaving any issues that require individual determination, such as the amount of damages, to be dealt with subsequently (*see "Bifurcation" below*).

Indeed, the court said that Mr Lloyd could have brought a representative claim to establish whether Google was in breach of the DPA 1998, with subsequent individual claims for compensation. The court assumed that this was not done because the first, representative stage would not generate any financial return for Mr Lloyd's funder and pursuing separate damages claims on behalf of individual class members would not be economically viable.

The court did not completely preclude bringing data claims as representative actions. Firstly, the decision considers the position only under the DPA 1998, and not under the GDPR or the UK GDPR (*see box "The position under the UK GDPR"*). Secondly, and perhaps more significantly, the court put forward another way in which these claims might be pursued using the representative action procedure: the bifurcated procedure.

The position under the UK GDPR

The claim in *Lloyd v Google LLC* was brought under the Data Protection Act 1998 (*[2021] UKSC 50*). The Supreme Court specifically stated that it was not considering subsequent legislation, that is, the General Data Protection Regulation (*679/2016/EU*) (GDPR), which is now incorporated into UK law as the retained EU law version of the GDPR (UK GDPR). This could leave the door open for future loss of control claims under the UK GDPR.

Interestingly, the compensation regime under the UK GDPR expressly refers to compensation being available in relation not only to material damages but also non-material damages. In addition, the recitals specifically reference loss of control over personal data as an example of possible damage resulting from a personal data breach. On the other hand, Article 82 of the UK GDPR refers to material or non-material damage as a result of an infringement, which echoes the Supreme Court's conclusion that the infringement and the damage are distinct.

There is therefore still an argument that claims in relation to the loss of control over data can be brought under the representative action procedure but, since the Supreme Court did not engage with the GDPR, it is unclear how it would view a claim of this kind. While the door is not closed, only time will tell if there is appetite to test this point again under the current data protection regime.

BIFURCATION

The Supreme Court in *Lloyd* suggested that a bifurcated procedure could be used to bring data and other class actions on a (partly) opt-out basis in which the representative action procedure is used to determine common issues, such as whether there has been an actionable breach, leaving damages to be dealt with in later individual claims or groups of claims. One question will be whether claimant law firms and litigation funders consider these claims to be economically viable, despite the court's assumption to the contrary. There is also a secondary question as to whether some types of claim are more viable than others.

Cyber incidents

The claim in *Lloyd* arose from the unauthorised collection and use of personal data. However, data class actions often arise where there has been a cyber incident resulting in a data breach.

As part of responding to cyber incidents, it is necessary to conduct a forensic investigation and risk assessment as to how data subjects have been affected by the incident (*see feature article "Cyber security: top ten tips for businesses", www.practicallaw.com/3-621-9152*). This feeds into whether they need to be notified about the incident, but also what has to be said to those data subjects in any notification. This is relevant because data subjects may be affected in different ways, for example, some may have had only their email address compromised whereas others might have had more sensitive data affected, such as banking details.

The prospective defendants will have analysed this in order to respond to the cyber incident. Potential claimants may therefore bring pre-action or early disclosure applications seeking this information from prospective defendants in order to assess the viability of the claim, both in terms of the numbers of people affected and how seriously, but also whether any initial representative claim in relation to liability might be successful and therefore viable from a costs perspective.

Liability in cyber-related data breach claims also falls neatly to be dealt with first. In a cyber-related data breach claim, a key issue will be whether the defendants had "appropriate technical and organisational measures" in place before the incident under Article 5(1)(f) of the UK GDPR (Article 5(1)(f)), as supplemented by Article 32 of the UK GDPR (Article 32). How well the defendants responded to the incident and whether they followed best practice to reduce the

claimants' risks and prospective losses will also be relevant.

In its analysis of section 4(4) of the DPA 1998, which is now replaced by Article 5(1)(f) and Article 32, the Supreme Court's judgment in *Lloyd* reinforced that the duty to have in place appropriate technical and organisation measures is not a strict liability requirement. It does not follow, just because a company has been hacked, that there has been a breach of Article 5(1)(f) and Article 32. Rather, the court expressly confirmed that a breach of this duty is similar to an allegation of negligence, predicated on a failure to meet an objective standard of care.

At the liability stage, the defendant will have to justify the technical and organisational measures in place before any cyber incident. This is unlikely to depend on the individual circumstances, so claimants can proceed on a representative basis without having to build a class at that stage.

If liability is established, the claimant law firms would then build opt-in groups of claimants based on the type of loss suffered. In cyber and data breach claims, potential claimants will naturally stratify into various groups depending on which data was affected. Class building would be advertised on the basis of an existing successful liability finding, which is likely to increase opt-in uptake. Prospective claimants would join a particular group with others who had been similarly affected, and there would be test cases for each group, with a view to assessing the quantum of damages for each type of claimant. The Supreme Court stated that, in this scenario, the liability trial will have stopped the clock on the limitation period, leaving time for the subsequent gathering of relevant claimant groups to deal with quantum.

On the key issue of funding and economic viability, the Supreme Court in *Lloyd* posed, without answering, the question of whether it would be acceptable for a funder to take its fee from the overall pot in an opt-out class action without the consent of everyone in the class, which would be impossible in a claim such as *Lloyd* where there was a class of four million.

However, for a cyber incident-related data breach claim, the quantum stage would be a collection of GLO claims with different assessed levels of quantum. The funder could agree with those who have opted into each claim to take its fee from the resulting awards of damages. The only issue, therefore, would be how the initial liability phase is funded, since the representative would not "own" the subsequent phase and other firms would be likely to take advantage of a first phase win by building quantum groups. Costs would be payable by the defendant if liability were established, so the initial claimant would recover costs and be in prime position to build the quantum groups.

ONGOING AND FUTURE CLAIMS

It remains to be seen what will happen with other data claims that were commenced on the basis of the Court of Appeal judgment in *Lloyd* and stayed pending the Supreme Court judgment. They may be reformulated as bifurcated claims or as GLOs. As to future claims, claimants may instead shift their attention for data use claims to competition law, alleging that personal data is being taken without a fair price being paid and pursuing opt-out class actions in the CAT. Regulators have recognised that a blend of regulation is needed to ensure that online services work well for consumers and businesses alike, as evidenced by the Information Commissioner, the Competition and Markets Authority and Ofcom establishing the Digital Co-operation Forum so that they can work more closely together (*www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022*).

Related information

This article is at practicallaw.com/w-034-4674

Other links from uk.practicallaw.com/

Topics

Case management	topic/2-203-6794
Data security	topic/8-616-6189
Funding litigation	topic/5-381-9613
Privacy	topic/6-383-8687
Rights of data subjects	topic/6-616-6190
Sanctions and remedies: data protection	topic/0-616-6193

Practice notes

Data Protection Act 2018: overview	w-014-5998
Data security under the UK GDPR and DPA 2018	w-013-5138
Data subject rights (UK)	w-024-3178
Funding options for civil litigation in England and Wales	1-525-8555
Group litigation and group litigation orders	w-028-3312
Multi-party litigation: overview	9-509-2801
Overview of cybersecurity	9-617-7682
Overview of privacy law	1-507-0879
Overview of UK GDPR	w-013-3757
Privacy law: remedies	2-507-2566
Security breach notification requirements	9-616-4019
Third party litigation funding in England and Wales: an overview	8-521-3304
UK GDPR and DPA 2018: claims for compensation	w-018-4325
UK GDPR and DPA 2018: enforcement, sanctions and remedies (UK)	w-005-2487

Previous articles

Changing face of cyber insurance: the devil finds work for idle hands (2021)	w-031-9892
Data class actions: the outlook after Morrison (2020)	w-026-2617
Class actions in England and Wales: key practical challenges (2018)	w-015-9333
Cyber security: top ten tips for businesses (2016)	3-621-9152
Cyber security: litigation risk and liability (2014)	1-568-4185

For subscription enquiries to Practical Law web materials please call +44 0345 600 9355

INSURANCE

Class actions pose a significant financial risk to businesses and their insurers because they can be costly to defend and there may also be significant settlements or judgments to pay. They are typically insurable in principle, subject to terms and financial limits of cover.

Insurance may be used by businesses to transfer at least part of the risk under their enterprise risk management strategy. For example, data class actions may be covered by cyber insurance, securities class actions may be covered by D&O insurance, consumer class actions may be covered by public or products liability insurance and competition class actions may be covered by civil liability insurance (*see feature article "D&O insurance: diving for cover", www.practicallaw.com/5-521-6870, Briefing "Cyber insurance requirements in commercial contracts: getting it right", www.practicallaw.com/w-011-7000 and feature article "Product liability class actions: a vision of the future?", www.practicallaw.com/3-556-5412*).

The financial risk associated with class actions is exacerbated in an opt-out class action, given the potential size of the represented class. Insurers, as well as businesses, will be relieved that the floodgates have not opened for opt-out data class actions, particularly given the current hard market for cyber insurance and the policy renewal challenges facing many policyholders, due mainly to an increase in ransomware exposure. Any enhanced exposure to opt-out data class actions stimulated by the Court of Appeal's decision in *Lloyd* might have caused the position to deteriorate further at a time when prices have already increased significantly.

As to the possibility of representative claims on a bifurcated basis, or top-down claims where a global loss can be assessed to avoid the same interest issue, liability insurers are likely to adopt a wait-and-see approach. If claimant groups and their funders do pursue further representative claims, some of the key issues that would need to be considered by policyholders and insurers include:

- The uncertainty over whether policyholders have a legal liability to the claimants for any amounts within the scope of a proposed early settlement, particularly in the case of bifurcated claims, given that liability insurance policies are often directed to covering legal liabilities. That said, it is relatively common for insurers to have to take a view on whether to cover potential settlements well before quantum is determined. As part of assessing this, complexities may also arise in determining who any settlement agreement would bind in a bifurcated process.

- Whether there is any restitutionary element to the claims, which may not be covered, or rather whether they are properly claims for material or non-material damages. This could arise, for example, in a top-down claim if claimants are seeking an account of profits on a global basis.

- If the class action is based on alleged deliberate conduct attributable to the policyholder, coverage may be excluded by virtue of a conduct exclusion in the policy or on the basis of the doctrine of ex turpi causa (where the claim arises from illegal or immoral conduct). This is often an issue in class actions, although it tends to crystallise after judgment if there are adverse findings based on the conduct of individuals that is attributable to the policyholder.

- Which policy or policies may be engaged when there are potentially a range of policies in play. This may be because more than one kind of policy could provide coverage, or because the issue has evolved over time and there is a question over which policy years are engaged.

As ever, claims require active management and engagement with liability insurers from the earliest stages if policies are to provide the cover that is expected.

ATE insurance

After-the-event (ATE) insurance is commonly used in class actions to cover the claimant's or funder's liability for adverse costs, if they are the losing party, or their liability for irrecoverable disbursements. Challenges may arise in the context of a bifurcated claim. ATE policies will need to be adapted to be appropriate for claims where a representative action deals only with liability, leaving damages for follow-on GLO claims. There may be questions about when the policy will be triggered and whom it will cover, which will be entwined with how the action is structured. These considerations will need to be factored into decisions about the viability and structuring of representative claims in the future.

Julian Copeman, Andrew Moir, Miriam Everett and Greig Anderson are partners, Kate Macmillan is a consultant, and Rachelle Waxman is a senior associate, at Herbert Smith Freehills LLP.

