SLAUGHTER AND MAY/

CLIENT BRIEFING
November 2020

THE PERILS OF DATA: ARE MASS CLAIMS FOR DATA PRIVACY BREACHES THE NEW NORM?

BIGGER CLAIMS AND BIGGER DAMAGES; HANDLING COLLECTIVE ACTIONS IN A WORLD OF THIRD PARTY FUNDING AND INCREASED INDIVIDUAL AWARENESS

A version of this article first appeared in the Privacy Laws & Business UK Report, Issue 112 (November 2020)

Since the GDPR came into force in 2018, organisations have faced sweeping changes to the European data privacy regime, with increased obligations when dealing with personal data coupled with the risk of large fines for getting it wrong. Regulators are increasingly flexing their muscles with their enhanced powers, notable examples including the French CNIL's €50m fine against Google and the UK ICO's recent fines against British Airways and Marriott for £20m and £18.4m respectively. However, this is only part of the picture. Potentially, the most significant risk facing organisations is that of mass civil damages claims from large groups of aggrieved individuals for breaches of their data privacy rights. This article looks at the latest developments in this area and the practical steps organisations can take to address this developing risk.

Collective claims - why now for data cases?

Save for limited circumstances, individual claims for misuse of personal information and breaches of data rights will not generally give rise to substantial damages because the loss or harm suffered by an individual is relatively low. These claims have typically been brought against media outlets by public figures where an individual's reputation stands to suffer seriously due to disclosures by the press (notably, Sir Cliff Richard against the BBC and Naomi Campbell against the Mirror Group) or for very significant privacy infringements (such as the claims brought by Shobna Gulati and others and other phone-hacking cases). Data or privacy claims have therefore typically been of less concern to non-media organisations.

By contrast, collective claims present a greater risk for all organisations as they significantly increase the potential damages exposure. The case against Google by consumer rights activist, Richard Lloyd, for example, has purportedly been brought on behalf of five million Apple iPhone users.

We are seeing an uptick in the number of collective claims brought in the English courts against companies in different areas, including competition and environmental claims. This is mirrored in data-related claims, driven in part by greater public awareness of data privacy rights following well-publicised enforcement action and a heightened global focus on holding large businesses to account for their use and protection of data.

A key factor for all collective claims is the rapid growth of the third-party litigation funding market and claimant-focused law firms prepared to act on a 'no-win, no-fee' basis. Earlier this year, City A.M. reported a jump in asset values of the UK's top 15 litigation funders to £1.9bn in 2019. This well-developed market is now turning its attention to data privacy, with several high-profile data breach claims issued in the last year against the likes of British Airways, EasyJet, Equifax, YouTube, Marriott, Facebook, TalkTalk and Salesforce and Oracle. Other claims are also reportedly waiting in the wings, pending the outcome of the case against Google.

The legal toolkit for individuals

Individuals have an extensive toolkit at their disposal when seeking to bring a claim against an organisation for data privacy breaches:

Breach of the GDPR, Data Protection Acts (DPA), and Privacy and Electronic Communications Regulations (PECR): The GDPR and DPA 2018 (and its predecessor) give an individual data subject who has suffered damage from an infringement of data

protection laws a right to compensation from the controller or processor. A claimant must prove that (i) the breach relates to 'personal data', i.e. any information relating to an identified or identifiable natural person, and (ii) the controller or processor has breached the relevant data protection rules when processing that data. The courts have set a low bar for the availability of damages in data breach cases, establishing that it is not necessary for a claimant to show financial loss. The claims against Salesforce and Oracle for alleged data breaches linked to the 'ad-tech' market are reportedly based on alleged breaches of the GDPR and PECR (which governs the use of personal data for marketing communications).

***Misuse of private information*:** This type of claim, based on an individual's Article 8 human right to private and family life, is the primary cause of action for the protection of privacy. An individual must show a reasonable expectation of privacy in relation to the misused information. Developed from breach of confidence claims (described below), it can be used where there is no duty of confidence between the individual and a company or where the information disclosed is already public. It is available regardless of financial loss or distress because loss of control over the use of private information is itself considered by the courts to be a form of damage.

Breach of confidence: Deliberate or accidental disclosure of an individual's confidential or private data in breach of duties of confidentiality could give rise to a claim. Duties of confidence can arise in different contexts, such as in an employer-employee relationship or due to confidentiality terms in a contract.

Other types of claims: Individuals may bring other types of claims if available, including for breach of employment or customer contracts.

Often individuals will bring several of these claims in parallel. The claim against British Airways following its 2018 data breach, for example, involves claims for breaches of the GDPR and DPA 2018, breach of contract, misuse of private information and breach of confidence. No doubt the claimants in that case and in the Marriott case will also now be looking to rely on the ICO's recent penalty notices against the companies to reinforce their existing claims.

Whilst most claims are brought on a primary liability basis (i.e. the organisation itself is directly at fault for a data breach), organisations can sometimes face claims for vicarious 'no fault' liability for the wrongful acts of others, such as employees. In April, the Supreme Court held in a case against supermarket chain, Morrisons, that an employer can in principle be vicariously liable for an employee's data breach even when the employer has not breached its data protection obligations.

DSARs – another tool in individuals' legal toolkit

We are seeing an increasing use of data subject access requests (DSARs) under the GDPR by potential claimants before and / or during litigation proceedings to support claims. DSARs can be used to get early access to documents in a potential dispute outside of the court's disclosure process or as a strategic tactic to place an additional burden on an organisation at a time when it wants to focus its energy on defending potential litigation. The ICO's guidance is that the purpose of a DSAR should not affect its validity (unless it is a manifestly unfounded or excessive request). However, the recent decision of Lees v Lloyds Bank indicates that the court is willing to take a robust approach to numerous and repetitive DSARs that have a collateral tactical purpose.

Types of collective actions

Outside of the competition law sphere, two alternative formal collective claims procedures are available to claimants (under Part 19 of the Civil Procedure Rules (CPR)):

- ***Group actions:*** Multiple claims that give rise to **'common or related issues of fact or law'** can be managed and tried together by the court using a mechanism called a group litigation order (GLO). GLOs are brought on behalf of identified individual claimants who **'opt-in'** to a GLO (i.e. authorise the claim to be on their behalf). Each claim remains an individual claim in its own right. The recent data breach cases against Morrisons, British Airways and Marriott are examples of GLO claims. The claims against EasyJet and TalkTalk are also expected to be managed using GLOs.
- ***Representative actions:*** A claim can be brought by an individual acting as a representative of others who have the **'same interest'** in the claim. Representative actions are brought on an **'opt-out'** basis, meaning that the claim is brought on behalf of everyone within the defined claimant class unless they positively opt-out. The represented class do not need to authorise the claim, be joined as parties or identified on an individual basis. Examples of representative actions are the claims against Google and Equifax.

Representative actions vs GLOs

Representative actions have, in principle, significant advantages for claimants over GLOs. GLO claims can be complicated and expensive to get off the ground due to the need to book build related claims, then structure and manage the separate claims during the proceedings. It is also practically impossible to involve the whole affected class. For example, in the Morrisons case, around 100,000 employees were affected by the data breach, but only around 10% joined the claim.

However, GLOs have been the mechanism of choice and the representative action regime has not been widely used. The main reason for this is that following the Court of Appeal's 2010 decision in Emerald Supplies v British Airways (in which Slaughter and May acted) the courts have restrictively interpreted the threshold requirement that members of the class have the 'same interest', requiring that it address both the legal basis of the collective claims and the damages sought. With its lower threshold of 'common or related issues', GLOs have to date therefore been the more popular route for mass claims.

That said, the Court of Appeal's recent decision against Google has opened up the possibility that the 'same interest' test may be more easily met in data-related opt-out representative actions on the basis that individuals could claim damages for "loss of control" of their data. That decision has been appealed to the Supreme Court with the hearing and final decision expected in 2021.

Lloyd v Google

The claim has been brought on behalf of a class of iPhone users allegedly affected by the 'Safari workaround', which enabled Google to use iPhone users' data without their consent by circumventing Safari's block on third party cookies. The Court of Appeal allowed the representative action to proceed on the basis that the individuals in the represented class all suffered the same alleged wrong and same loss, namely "loss of control" of their personal data. Although there was no financial loss or distress, the Court of Appeal found that damages could be awarded under the DPA 1998 on the basis that the information collected held economic value and therefore its loss was a loss to the claimant class. The whole class had the "same interest" because claimants had their data taken without their consent over the same period and in the same circumstances.

Have the floodgates opened for collective actions?

The recent claim against Equifax shows that obstacles remain to bringing representative actions. The claimants deployed similar arguments to those used against Google, arguing the class had suffered damage due to a loss of control over their data owing to Equifax's alleged lax data security. However, following service of Equifax's defence, which challenged a number of aspects of the Court of Appeal's decision in Google, the claim was withdrawn. All eyes remain on what the Supreme Court's take in Google will be and whether it does indeed open the floodgates to data breach representative actions.

There is also the recently concluded consultation by the Department for Digital, Culture, Media and Sport (DCMS) into the effectiveness of existing provisions in the GDPR that enable individuals to ask certain non-profit bodies to take action on their behalf for data law breaches, including bringing court claims.

Significantly, that review is also looking at whether to introduce a form of 'opt-out' rule enabling non-profits to take action on behalf of individuals without their consent. The DCMS's report is expected late-November.

While there is clearly momentum behind data-related collective claims, there remain unanswered questions that may be hurdles in the way of prospective claimant groups, including whether a claimant class can include data subjects outside the jurisdiction, the possibility of using sub-classes for different damage claims, the effect of mass claims on limitation periods and the need to demonstrate causation between a data controller's errors and the damage claimed. The law on what measure of damages may apply in different cases also remains nascent; will more be payable by the defendant data controller when data is unlawfully hacked (and sold) by a third party or when data is unlawfully exploited by the data controller themselves?

Mass claims for data breaches: if Lloyd v Google doesn't open the floodgates then perhaps the DCMS will?

The DPA 2018 (under s187) already allows 'representative actions' whereby individuals can ask certain non-profit organisations to complain to the ICO on their behalf about a data controller or processor, represent them in court when seeking to resolve those complaints and bring court claims against organisations for data breaches.

The DCMS has recently consulted on the effectiveness of the existing provisions, acknowledging that to date the take-up under the existing regime is "quite low".

Significantly, the review will also consider introducing a form of 'opt-out' rule enabling non-profit organisations to take action for breaches of individuals' data rights without affected individuals' consent or the need for claimants to meet the strict "same interest" test needed in Google-style cases under the CPR. The importance of this change, particularly in terms of bringing mass compensation claims in the courts and the consequential risks for large data controllers (and the (dis) incentives this may bring for more innovative uses of data), is difficult to underestimate.

Where English law goes on this will be of real interest to data controller organisations and individuals wishing to give effect to their data privacy rights (and claimant law firms and funders looking to bring mass claims). If the DPA 2018 rules are changed, even if the Supreme Court rules against the Google decision, data controllers may still face the risk of 'opt-out' mass claims for data breaches against them in the future.

The DCMS consultation period ended on 22 October 2020. The government must report to Parliament on the s.187 DPA 2018 provisions by 25 November 2020.

See Slaughter and May's digital blog The Lens for future updates on the outcome of the DCMS consultation.

Practical steps

There are clearly many reasons to watch this space in the coming months and see how this area of law develops. In the meantime, organisations should ensure litigation risk is accurately factored into their data privacy risk management frameworks. Practical steps to reduce and mitigate the risk of litigation include:

- ***Know what data is being processed or retained (and why):*** Keeping personal data for longer than is necessary is not only a breach of the GDPR and DPA 2018 but also a sure way to increase an organisation's

liability in the event of a cyber-attack or rogue employee incident. Likewise, using data in a way that is inconsistent with data subjects' expectations (or privacy notices) is likely to increase the risk of challenge

- ***Insurance:*** Consider insuring against cyber and data risks or checking that existing policies cover the additional risk of related civil litigation and provide access to the necessary external support. Organisations should be clear on the implications of this for their risk and governance strategies and how it will work in practice, including agreeing with insurers pre-approved experts to call on.
- ***Learn lessons:*** Failure to act on past audits or reports (internal or external) is likely to provide unhelpful (and disclosable) material in the event of ICO investigation or litigation. When the ICO fined the owners of Dixons and Currys PC World £500,000, the highest amount possible under the old DPA 1998, it relied heavily on a report produced before the data breach in question by an external information security consultancy. Likewise, the absence of past incidents was a mitigating factor in the recent British Airways decision.
- ***Incident handling:*** The initial response and immediate customer handling of any data breach or incident will be key in terms of the organisation's exposure to follow-on litigation. Legal advice should be sought for the preparation of, and reliance on, internal policies around document creation, customer handling and privilege. Internal co-ordination will help with avoiding self-incrimination and ensuring communications with regulators and other third parties are aligned before being distributed.
- ***Cooperation vs. self-incrimination:*** Co-operating with relevant regulators in the event of a breach would usually be encouraged but it is important to ensure material created as part of this process – such as internal forensic reports – is not itself later used against the data controller in follow-on litigation.

Slaughter and May advises on all aspects of data privacy law, including regulatory considerations following data breaches, and has extensive experience acting on group litigation proceedings before the English courts.

CONTACT

RICHARD JEENS
PARTNER
T:020 7090 5281
E:richard.jeens@slaughterandmay.com

ANNA BROADLEY
ASSOCIATE
T:020 7090 3852
E:anna.broadley@slaughterandmay.com

SAMANTHA HOLLAND
PROFESSIONAL SUPPORT LAWYER
T: 020 7090 3674
E:samantha.holland@slaughterandmay.com