CLIFFORD
CHANCE

# DATA COLLECTIVE ACTIONS: THE COSTS OF LOSING CONTROL

— THOUGHT LEADERSHIP

APRIL 2020

# DATA COLLECTIVE ACTIONS: THE COSTS OF LOSING CONTROL

Data breaches are an increasing focus for English litigation, and collective actions are on the rise as public concern grows about how our data is used. All companies – not just big tech firms – use data, and therefore risk being faced with these claims. Businesses with deep pockets are the most likely to be sued. In this briefing, the first in a series, we explore the potential claims that firms may face following a data breach.

Reports of data breaches by companies, political parties, charities and government bodies are constantly in the news. These breaches tend to hit the headlines when data has been taken by hackers; but data can also be misused if, for example, it is sold or tracked, or if unauthorised electronic communications are sent, or facial recognition technology is used inappropriately. A firm that holds data in a manner that exposes it to a breach, e.g. on an unsecured laptop or a USB stick, or in unlocked containers, could also face claims under data protection or privacy laws. Whilst many employees are remote working as a result of coronavirus, we expect these security risks to heighten – creating further opportunities for cyber criminals.

Claims can be about information that is personal or non-personal, commercial or non-commercial, sensitive or non-sensitive. This could range from, for example, names, email addresses, corporate financial information, private photographs, medical history, browser-generated information (BGI) or genetic data.

In addition, claimants do not need to have suffered financial loss or distress to claim for misuse of their data, as the recent case of *Lloyd v Google LLC* [2019] EWCA Civ 1599 demonstrates. This case, which we discuss further below, is a collective action against Google for allegedly tracking the BGI of 4.4 million iPhone users, to sell to advertisers. Companies may face claims even where the ICO (the UK regulator) has not taken enforcement action (although such claims are more likely following enforcement action). If there has been a relevant regulatory ruling or penalty, it will doubtless be relied on by claimants seeking to bring follow-on claims, so companies considering taking a commercial decision to pay (and not appeal) penalties imposed by a relevant regulator must be alive to this risk.

Individual claims for misuse of data do not attract high damages – normally, they are in the thousands-of-pounds. However, if all or most of a customer base has been affected, and those customers join forces to claim as a group, or "class", damages can soon reach the billions. Thus, another significant consequence of the Court of Appeal's decision in *Lloyd* to allow the case to proceed in the UK courts, is that it has allowed that claim to proceed as a representative action. (This may not be the last word: last month Google was given permission to appeal to the Supreme Court.)

Just two days after the Court of Appeal's decision in *Lloyd*, on 4 October 2019, the High Court permitted British Airways customers to bring a collective action (this time, under the mechanism of a Group Litigation Order), following a cyber attack in 2018 that enabled the attackers to obtain the data of 500,000 customers. Collective actions have also begun against Equifax and Ticketmaster, following the cyber attacks that took place on each of those companies' systems – although the Equifax group action has just been withdrawn. Initially, there was scepticism about the rise of US-style class actions in this area, but in the light of these recent developments, they now seem an inescapable reality.

## Some recent cases

| Various v Morrisons | |
|---|---|
| **Background** | In January 2014, a disgruntled employee disclosed former and current employees' data on the internet |
| **Position of the ICO** | The ICO determined that no formal action against Morrisons was necessary |
| **Date claim/ application issued** | 8 December 2015 |
| **Type and size of collective litigation** | Group Litigation Order on behalf of 9,263 claimants. The amount claimed is not clear |
| **Potential claims** | Breach of confidence, misuse of private information (MOPI) and breach of the DPA 1998 |
| **Status of litigation** | Both the High Court and the Court of Appeal found Morrisons not directly liable, but vicariously liable, for the actions of its employee, for breach of confidence, MOPI and breach of the DPA 1998. This was appealed to the Supreme Court, who reversed the Court of Appeal's decision, unanimously finding Morrisons not liable |
| **Funding** | We are not aware of the funding position |

| Lloyd v Google | |
|---|---|
| **Background** | Between April 2011 and February 2012, Google is alleged to have harvested BGI of approximately 4 million iPhone users without their knowledge or consent, bypassing Safari's privacy settings |
| **Position of the ICO** | The ICO has taken no regulatory action against Google |
| **Date claim/ application issued** | 31 May 2017 |
| **Type and size of collective litigation** | CPR 19.6 representative action on behalf of an estimated 4.4 million individuals. £750 per individual is claimed |
| **Potential claims** | Breach of the DPA 1998 |
| **Status of litigation** | In October 2019, the Court of Appeal granted permission for the claim to be served out of the jurisdiction and to proceed as a representative action (although Google is appealing this decision to the Supreme Court). The litigation is at an early stage, and there has been no decision as to liability or quantum |
| **Funding** | We understand that this claim is being funded by Therium Litigation Funding (a third-party litigation funder), and that the claimants have "After the Event" (ATE) insurance in place in the event that they are unsuccessful at trial (and an adverse costs order is made) |

| Various v British Airways | |
|---|---|
| **Background** | Between August and September 2018, users of British Airways' website were diverted to a fraudulent site from which around 500,000 customers' data was obtained |
| **Position of the ICO** | In July 2019, the ICO provided a notice of intent to fine BA a record £183.39 million. This is not a final determination; the ICO had until 31 March 2020 (the period having been extended by agreement) to serve a monetary penalty. We await news of this decision |
| **Date claim/ application issued** | 14 June 2019 |
| **Type and size of collective litigation** | Group Litigation Order. The number of claimants and amount claimed are not yet clear |
| **Potential claims** | Breach of confidence, MOPI, breach of the DPA 2018 and breach of contract |
| **Status of litigation** | The High Court has allowed the litigation to be brought under a Group Litigation Order (October 2019). The litigation is at an early stage: claimants have until January 2021 to serve claims |
| **Funding** | We are not aware that litigation funding is in place. However, we understand that solicitors act for claimants on a "no-win-no-fee" basis, effectively funding the claim. We also understand that ATE insurance is in place in the event that claimants are unsuccessful at trial (and an adverse costs order is made) |

| Atkinson v Equifax | |
|---|---|
| **Background** | Between May and July 2017, a file containing around 15 million records relating to UK customers was the subject of a cyber attack, via Equifax's US parent company |
| **Position of the ICO** | In September 2018, the ICO issued a £500,000 monetary penalty (the then-maximum). This was not appealed |
| **Date claim/ application issued** | 4 October 2019 |
| **Type and size of collective litigation** | CPR 19.6 representative action. The size of the class and amount claimed was not clear |
| **Potential claims** | MOPI and breach of the DPA 1998 |
| **Status of litigation** | Statements of case were served last year. The claim has since been withdrawn |
| **Funding position** | We are not aware that litigation funding was in place. However, we understand that solicitors acted for claimants on a "no-win-no-fee" basis, effectively funding the claim. We also understand that ATE insurance was in place |

## What are the potential claims that companies might face following a data breach?

### Breach of confidence

In the context of a data breach, disclosure of an individual's data in breach of contractual terms which require confidentiality, or an employer/employee relationship of confidence, could give rise to this cause of action. A claimant will need to prove:

- that the information is confidential, or "secret". It could be personal data, or could concern commercial matters.
- that the confidential information was disclosed in circumstances of confidentiality, and there has been a threatened or actual disclosure of the information. The disclosure need not be intentional.

If information disseminated during a data breach was already in the public domain (e.g. addresses and telephone numbers), or there is no relationship of confidence between claimant and defendant, claimants may instead need to rely on the tort of "misuse of private information".

### Misuse of private information

The European Convention on Human Rights provides a right to respect for private and family life. This right can be secured under English law using an action for misuse of private information. This cause of action is relatively young, and continues to evolve rapidly. A claimant must demonstrate:

- a "reasonable expectation of privacy" in respect of the information (*Campbell v MGN Limited* [2004] UKHL 22).
- that this information was misused. Although the tort has largely developed through cases involving newspapers, it does not require publication of information to the world at large. It can also occur if a defendant accesses or stores an individual's information. Another important case is *Gulati v MGN Limited* [2015] EWHC 1482, which concerned the infringement of privacy rights in the interception of voicemails by The Mirror newspapers. The Court of Appeal held that not only were the claimants entitled to damages for distress, as is usual for MOPI, but also for being deprived of the right to control their private information.

Often, a breach of confidence will add little to a MOPI claim, but it depends on the nature of the data. For example, a company whose commercial information has been misused may need to claim for a breach of confidence, rather than for MOPI. In addition, in *AVB v TDD* [2014] EWHC 1442, the claimant relied on a breach of confidence to obtain an injunction against disclosure of information about the claimant's wife and children, and of sexual and financial information about various women with whom he had relationships. The claimant could not rely solely on MOPI, because it was not just his own private information, but also information relating to third parties, that was misused.

### The GDPR and Data Protection Acts

The GDPR and the Data Protection Act 2018 (the DPA 2018), and their predecessor, the Data Protection Act 1998 (the DPA 1998), provide a right to compensation for people who suffer damage as a result of infringement.The GDPR became directly applicable in EU member states on 25 May 2018, supplemented, in the UK, by the DPA 2018. It will remain in effect in the UK through the Brexit transition period and will then be implemented into UK law with minor amendments. Familiarity with the DPA 1998 remains important, since any data event that took place before 25 May 2018 may still be within the limitation period. Fortunately, there is significant overlap between the two regimes. A claimant must prove:

- that the data is "personal", which means any information relating to an identified or identifiable natural person. A DPA claim is often relied on because of this broad definition, which can include data that would not satisfy a MOPI claim (e.g. an individual's name). Certain categories of personal data (e.g. data concerning genetics, health,

or racial or ethnic origin) are deemed "special category" data, to which additional restrictions apply.

- that a controller (that is to say, a person who makes decisions about how and why personal data is processed) or processor (that is to say, a person who processes personal data on behalf of the controller) has failed to comply with a relevant provision when processing personal data. Some examples of provisions under which a claimant might claim following a mass data breach or mass misuse of data appear below.

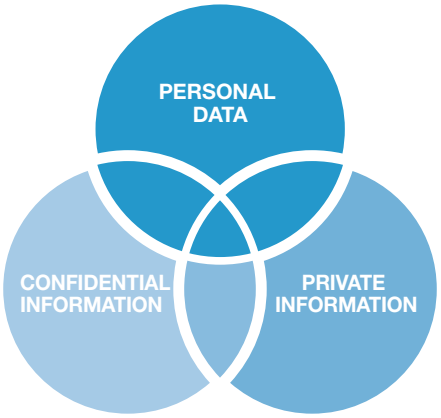
| | |
|---|---|
| **Article 5(1)(a) (Data Protection Principle 1 under the DPA 1998)** | Personal data must be processed lawfully, fairly, in a transparent manner, and only where the conditions specified in article 6 (Schedule 2 of the DPA 1998) are met. Claimants might rely on this, for example, where BGI is sold to a third party without consent (or without one of the other conditions being met), or where a company permits a contracting party to continue to hold customer data when there is no longer a lawful purpose for doing so, and that data is then subject to a third-party cyber attack. |
| **Article 5(1)(b) (Data Protection Principle 2 under the DPA 1998)** | Personal data must be collected for one or more specified and legitimate purposes and not further processed in a manner incompatible with those purposes. Claimants might rely on this, for example, where data has been shared with a third party in a manner incompatible with a relevant privacy notice. |
| **Article 5(1)(e) (Data Protection Principle 5 under the DPA 1998)** | Personal data must be stored for no longer than is necessary. Claimants might rely on this, for example, where a company has inconsistent policies in respect of document retention, and those documents are then stolen. |
| **Article 5(1)(f) and/ or article 32 (Data Protection Principle 7 under the DPA 1998)** | Appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, and damage to, personal data, to ensure a level of security appropriate to the risk. Claimants might rely on this, for example, where data is stolen from a USB stick, and the company had an inadequate encryption policy, or no policy requiring data to be deleted from USB sticks after a certain number of days. |
| **Chapter V (Data Protection Principle 8 under the DPA 1998)** | Personal data must not be transferred outside the European Economic Area unless individuals' rights in respect of personal data can be protected in another way, or one of the exceptions applies. Claimants might rely on this, for example, where a company has permitted a foreign company in its group to host data, without agreeing sufficient protections, and that data is then subject to a third-party cyber attack. |

Under the GDPR it is a defence if a controller or processor proves that "it is not in any way responsible for the event giving rise to the damage". Similarly, under s13(3) DPA 1998 it is a defence if a controller proves that it took such care as in all the circumstances was reasonably required. This is an important defence for businesses which face litigation following a cyber attack carried out by a third party, but businesses must show that they have taken all appropriate measures to protect data from such risk.

In *WM Morrison Supermarkets Plc v Various Claimants* [2020] UKSC 12, Morrisons faced claims following the disclosure of former and current employees' data on the internet by a disgruntled employee. Morrisons did not need to rely on the s13(3) defence, because it was held not to be carrying out the functions of a "data controller" when the information was put on the internet. The employee became the "data controller" for that purpose. Instead the lower Courts found Morrisons vicariously liable for the employee's wrongdoing. This week the the Supreme Court reversed that decision. Morrisons has therefore avoided primary and vicarious liability. But businesses should not be complacent: the Supreme Court made it clear that employers can, in principle, be vicariously liable for data leaks caused by rogue employees. The question of whether they will be liable is highly fact-sensitive. We have written more about this case in our Talking Tech post.

Damages can be awarded for non-pecuniary loss (i.e. distress). *Lloyd* has also confirmed that claimants do not need to have suffered distress to bring a claim for misuse of their data. The Court of Appeal said that, since damages are available without pecuniary loss or distress for MOPI, and since they are "two parts of the same European privacy protection regime", it would be inappropriate to apply a different approach to the DPA. This raises an interesting philosophical question: if you don't know that your BGI has been used, or know but don't care, have you really suffered loss? The Court of Appeal said yes: since the BGI had economic value to Google, so did a person's control over that BGI. A "loss of control" was therefore sufficient to attract damages. Although *Lloyd* is a claim made under the DPA 1998, the Court of Appeal observed that the same conclusion would be reached in an equivalent claim under the GDPR (not least because recital 85 to the GDPR cites loss of control as an example of "material or non-material damage" that might occur following a data breach). The Court of Appeal did provide some comfort to defendants, confirming that, like MOPI, a damages award under the DPA requires a threshold of seriousness to be crossed, which would "undoubtedly exclude" a claim relating to "an accidental one-off data breach that was quickly remedied".

In practice, it is common to rely on multiple causes of action, since a data breach normally involves different things happening to different data.




### Other causes of action

Other causes of action may be available, such as if an individual has suffered loss as a result of a breach of a customer contract (including terms of use or a privacy policy), or breach of an employment contract requiring data to be dealt with in a certain way. A data incident could also give rise to criminal liability, e.g. for breach of section 45 of the Human Tissue Act 2004, which relates to misuse of a person's genetic information, section 3 of the Investigatory Powers Act 2016, which relates to interception of communications without lawful authority, or the Computer Misuse Act 1990, which relates to computer hacking.

## The rise of the class action

Another significant consequence of *Lloyd* is that the Court of Appeal allowed the claim to proceed as a representative action, which, until recently, was considered an impractical route. Although uncommon, claimants have had the ability to bring collective actions under English law for some time.

### What are the mechanisms for bringing collective actions?

There are two types of formal collective action: Group Litigation Orders (GLOs) and representative actions.

**Group Litigation Orders**

These are made under CPR 19.11, where multiple claims give rise to certain common or related issues. The British Airways and Morrisons Group Litigation Orders are recent examples. There will be a generic trial of common questions of fact (for example, whether British Airways is liable for the cyber attack), but claimants plead individual facts, and damages are tailored accordingly. Claimants have to "opt-in" to GLO actions.

**"Representative actions"**

These face a higher threshold: they may only be brought by or against one or more persons who have the "same interest" in the claim, which has meant they are typically difficult to bring. They are governed by CPR 19.6, and, similar to US "opt-out" class actions, there is no need for each individual in the represented class to be joined as a party to the action (although the Court's permission is needed to enforce a judgment or order against a non-party).

*Lloyd* has been brought by an informal association, "Google You Owe Us", led by the former executive director of the consumer organisation Which?. The claim is on behalf of an estimated 4.4 million iPhone users who had the applicable versions of Safari at the relevant time and did not change the default settings. The claimants do not seek to rely on personal circumstances and do not claim for distress. The Court of Appeal has allowed the claim to proceed as a representative action on the basis that the individuals in the represented class were all victims of the same alleged wrong, and had all suffered the same loss (loss of control of their personal data).

This decision is likely to encourage further representative actions following data breaches, on behalf of people that have suffered no financial loss or distress. However, representative claimants will only be able to seek damages that represent the "lowest common denominator" of loss. Because distress or other individual circumstances cannot be relied on, such claims are likely to be of low individual value (in *Lloyd*, just £750 per person is sought). But Google might have to pay aggregate damages of £3.3 billion, before costs are considered.

Until the outcome of Google's appeal is known, we predict that GLOs will be favoured over representative actions by claimants and those funding the claims.

Group proceedings could also be brought under the following procedures:

- A defendant willing to compensate potential claimants could establish an out-of-court compensation scheme. This could save both parties some of the costs associated with litigation. It could appeal to the defendant, who would be able to design the eligibility criteria and other rules, and it might help to show the ICO (or other relevant regulator) that the business is taking a pro-active approach towards mitigating any possible adverse effects of a breach. It could also appeal to

> **The case may be costly and may use valuable court resources, but it will ensure that there is a civil compensatory remedy for what appear, at first sight, to be clear, repeated and widespread breaches of Google's data processing obligations and violations of the Convention and the Charter**
>
> — **SIR GEOFFREY VOS C, LLOYD V GOOGLE**

claimants, who would probably receive compensation sooner than if they were to bring Court proceedings. However, whilst the Court could be asked to vary or stay proceedings to give effect to such a scheme, it cannot force claimants to give up their right to bring court proceedings, so the defendant would need to be prepared to defend such proceedings in parallel.

- A Managed Litigation, where claims are brought individually, but managed by one Managing Judge, using the Court's case management powers and often under a common-costs regime. An example is the ongoing voicemail interception litigation against News Group Newspapers, on which Clifford Chance acts.
- A large number of claimants could be joined in an ordinary action. For example, shareholder class actions, in which Clifford Chance has considerable experience, are frequently brought by multiple claimants.
- Article 80(1) of the GDPR now enables a qualifying non-profit organisation to bring representative proceedings on behalf of data subjects. In the UK, this is (for now) only possible if data subjects authorise such organisations to act on their behalf (i.e. on an "opt-in" basis). However, article 80(2) of the GDPR gives member states discretion to provide that qualifying non-profit organisations can act on behalf of data subjects without being appointed by them. The UK government has not implemented article 80(2), but is keeping this under review. Such a provision could give rise to a flood of consumer association-led claims.

The increase in collective proceedings is significant, because, without them, individuals are less likely to bring claims. The low level of damages may not justify the inconvenience, cost and risk of having to pay the other party's costs, but law firms can encourage claimants to join collective litigation on a "no win, no fee" basis (albeit they can no longer recover success fees from the defendant, following a change in the rules last year). This is also fertile territory for third-party litigation funders, who are becoming increasingly prominent in this field. Companies dealing with the defence of claims should therefore ensure that their legal teams have experience in dealing with funded counterparties.

## Key issues

An increased awareness about data rights and obligations, technological change and the increased risk of data incidents, rapidly evolving case law, and certain increased protections under the GDPR, are emboldening claimants and other stakeholders in group litigation.

Although rulings by the ICO do not bind decisions in any follow-on litigation, they are likely to be heavily relied on; therefore, the process of dealing with the ICO requires even greater care.

Collective data actions are disproportionately costly to contest, and the financial consequences of losing a collective data action could dwarf any regulatory penalty. Careful strategic thought should be applied when defending such claims, given the potential for adverse-costs orders.

The risk of group litigation in relation to data breaches is real, and large profitable businesses are being watched by claimant law firms and litigation funders. Businesses cannot afford not to build this risk into their data strategies.

# CONTACTS


**Lucy Hall**
**Senior Associate**
**London**
T: +44 20 7006 2271
E: lucy.hall
@cliffordchance.com

**Maxine Mossman**
**Partner**
**London**
T: +44 20 7006 4204
E: maxine.mossman@
cliffordchance.com

**Kate Scott**
**Partner**
**London**
T: +44 20 7006 4442
E: kate.scott
@cliffordchance.com

**Haafiz Suleman**
**Senior Associate**
**London**
T: +44 20 7006 4348
E: haafiz.suleman
@cliffordchance.com

# OUR INTERNATIONAL NETWORK
## 32 OFFICES IN 21 COUNTRIES

Abu Dhabi
Amsterdam
Barcelona
Beijing
Brussels
Bucharest
Casablanca
Dubai
Düsseldorf
Frankfurt
Hong Kong
Istanbul
London
Luxembourg
Madrid
Milan
Moscow
Munich
Newcastle
New York
Paris
Perth
Prague
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.

Riyadh*

*Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh
Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

CLIFFORD

CHANCE



www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ



2002-000354