Lights, camera, (class) action! - data protection group claims back in the spotlight

Ali Vaziri, Managing Associate at Lewis Silkin LLP , looks at the increasing risk of group data protection claims in the light of two recent decisions of the English courts

October 2019 was marked not only by the launch of 'European Cybersecurity Month' but also by renewed debate about the prospect of data protection class actions, prompted by events in two sets of proceedings in the English courts:

1. Firstly, the Court of Appeal's decision in *Richard Lloyd v Google LLC [2019] EWCA Civ 1599* ('the *Lloyd* case') unanimously overturning the judgment of Mr Justice Warby which had refused the former director of Which? permission to serve a representative action out of jurisdiction on the Delaware-registered corporation. The claim by Mr Lloyd was made on behalf of a class of more than 4 million iPhone users, and alleged that Google secretly tracked some of their internet activity for commercial purposes; and

2. Secondly, that same Judge's order in *Stephen Andrew Weaver & others v British Airways plc* with Claim Number BL-2019-001146 ('the *BA* case') granting the airline's application (yes, you read that correctly) for those of its customers affected by the well-publicised 2018 data breaches to bring compensation claims against it in the High Court.

Renewed debate

Debate was 'renewed' (as opposed to 'new') because, in the run up to the General Data Protection Regulation ('GDPR') coming into force, many pundits anticipated a wave of data protection class actions flooding the English courts. That anticipation was supported by (for example): data subjects' rights being further clarified and strengthened by the GDPR; increased awareness of, and willingness to exercise, those rights by data subjects; increased transparency about how personal data are used and misused, including through mandatory breach notification; and, of course, the introduction of 'representative bodies'.

The experience on the other side of the Atlantic, where class actions seem to follow data breaches like night follows day, also doubtless played a role. Indeed, a wave of class action litigation, often involving household names, appears to have been building Stateside in recent years; and although not every data breach has resulted in class action litigation, high-profile and large-scale data breaches usually have. UK corporates were therefore concerned that, with the introduction of the GDPR, the class action wave would cross the ocean and crash on these shores.

But by the time the GDPR celebrated its first birthday, there was not much to report. Whilst litigation funders continued to take meetings with claimant firms, eyes in the legal community were on *Various Claimants v Wm Morrisons Supermarket PLC* ('the *Morrisons* case') which was steadily working its way up through the appellate courts. Readers will recall that this case involved a disgruntled employee who misused the payroll data of some 100,000 employees, thousands of whom brought a damages claim against the supermarket.

The court at first instance found that although Morrisons was not directly liable for the criminal acts of the rogue employee, the company was nonetheless vicariously liable. The decision was particularly unpalatable for employers given that the UK Information Commissioner's Office ('ICO') had taken no action following an investigation, and the court had found that Morrisons' security was appropriate (save in one inconsequential aspect).

So when the first instance decision was upheld last year, UK corporates drew a sharp breath. Especially since the Court of Appeal's answer, to what it characterised as "*Doomsday or Armageddon arguments*" about the enormous burden a finding of vicarious liability would place on innocent employers, was to be properly insured. But later that same month, there was a partial sigh of relief by organisations when the *Lloyd* case came to an early demise, not even getting permission to serve the claim out of jurisdiction.

It is in this context that October's court decisions on class actions, bringing the *Lloyd* case back to life, and allowing the *BA* case to get off

the ground, are of note. More so since they came shortly before the Supreme Court was due to hear the appeal in the *Morrisons* case in early November 2019. So, along with other good tidings, the New Year is therefore likely to bring some clarity on the important issues raised in the *Morrisons* case. It will also, reportedly, bring the release of Andrew Skelton – the employee whose criminality was the catalyst for those proceedings.

What are 'class actions'?

People understand different things from the term 'class action'. It is probably fair to say that, for most of us, the term calls to mind: (a) the US; and (b) big numbers – both in terms of damages (eye-watering) and claimant numbers (legion). Hollywood has doubtless played a role in influencing our understanding, with fact-based (think Erin Brockovich and the Hinkley groundwater contamination) or fictional (think any number of John Grisham novels adapted for the silver screen) dramas involving class actions in the US, often evidencing some of the worst excesses of the system.

But, in a broad sense, 'class action' refers to procedural mechanisms by which claims can be brought by large numbers of claimants. It is a term which is often used interchangeably with other terms such as 'group litigation', 'collective redress', 'multi-party actions' and 'representative claims' but, as we will see, some of these terms have particular connotations.

In the English courts, there are a number of different procedural mechanisms which can be used to bring such claims. Some are 'informal' in nature. So, for example, the court rules allow for any number of claimants and defendants to be joined as parties to a claim, and for persons to be added or substituted to an existing claim.

Outside of these informal procedures, class actions can be broadly separated into 'opt-in' and 'opt-out' regimes. Whilst these terms will be familiar to many in a data protection and e-privacy context – especially marketers – when it comes to litigation:

> ***"a pan-European collective redress mechanism for consumers in mass harm situations is being developed. The most recent proposal...assumes that collective redress mechanisms would be available for a wide variety of violations, including data protection"***

- *Opt-in claims* can only be brought on behalf of those claimants who are identified in the proceedings and who authorise the claim to be brought on their behalf. Unless a claimant specifically opts in, he will not be included. The Group Litigation Order ('GLO') procedure is an opt-in procedure and provides a case management framework for managing individual claims which give rise to common or related issues of fact or law. It does this by giving directions about (for example) setting up a register on which claims managed under the GLO will be registered, and specifying the issues which will identify the claims to be managed. All claims included on the register remain separate, even though they are managed as one. The procedure is therefore not well-suited to claims that are not economically viable in their own right given that claimants will each be liable for a share of the costs of the litigation, and for adverse costs if the claim is unsuccessful – a significant disincentive, especially where the claim value is low.

- *Opt-out claims* are brought on behalf of a defined class and, as such, it is not necessary to identify all the claimants in the same way as in an opt-in regime, nor to obtain their authorisation. This means that unless a claimant specifically opts out, they will automatically be included. Many will therefore only become involved in, or even aware of, the proceedings when it comes to claiming their share of any damages. The 'representative action' provides that a claim may be brought by (or indeed against) representatives of any others who have the 'same interest' in the claim. The test is very strict and narrow: it must be possible at all stages of the proceedings (and not just at the end) to say of any particular person whether he qualifies for membership of the represented class by virtue of having the 'same interest' as the claimant. That would not be the case if a defence were available in respect of some claims, but not others. Since the represented class are not joined as parties, they are not subject to disclosure obligations or cost consequences. The represented class are, however, bound by the court's determination of a matter.

The GLO against BA

The *BA* case relates to the airline's headline-grabbing breaches in 2018 which affected half a million or so of its customers and which the ICO attributed to "*poor security arrangements*". The intended action is to be brought under a GLO (i.e. a type of opt-in procedure) and applies to claims giving rise to the following two issues:

- whether BA is liable to claimants (whose names are included on the group register) for potential damages under various specified causes of action arising from the 'data event' (which is defined in the order); and

- if so, which claimants are entitled to damages and on what basis?

According to the lead solicitors' website, claimants "*will be able to claim significant compensation in the thousands, or possibly tens of thousands, depending on circum-*

(Continued on page 8)

stances". In exchange, they "*take 35% of any compensation*" for sign-ups after 6 April 2019. Even allowing for some puffery, given the range in damages anticipated by claimants and the hundreds of thousands of individuals affected by the breach, BA's potential liability could conceivably dwarf the ICO's £183.39 million notice of intent (which apparently equated to 1.5% of BA's global turnover).

That being so, it is unsurprising that BA appears to have sought to wrest control of the situation in what is an unusual move for a defendant: applying for a GLO.

A claimant firm reportedly described that application as BA "launching '*a cynical bid' to limit a potential £3bn pay-out over two data breaches by demanding claimants act within just 17 weeks"*. Although following October's hearing the window was extended to 15 months – with a cut-off date of 17 January 2021 – BA did, however, successfully avoid having to publish a notice publicising the GLO on its website and emailing it to affected customers. Those steps, sought by the claimants, would have effectively resulted in BA building the claimant firms' books of business for them.

The representative action against Google

The *Lloyd* case concerns the so-called 'Safari Workaround' by which Google was allegedly able to bypass a restriction on Apple's Safari browser which blocked third party cookies (i.e. cookies which are placed on a user's device by a domain other than the main website which the user is visiting) and set its own DoubleClick Ad cookie on a user's device. That cookie enabled the delivery and display of interest-based ads. By doing so, in 2011-12 Google was allegedly able to obtain information about users' internet activity, through browser generated information ('BGI'), without their knowledge or consent.

The three issues raised by Mr Lloyd's appeal (with salient points) are:

1. Do you need to prove pecuniary loss or distress in order to be compensated under data protection law?

Warby J had said yes, but the Court of Appeal disagreed. Its view, influenced by a phone-hacking decision where damages were awarded for misuse of private information without proof of material loss or distress, was that "*the key to these claims is the characterisation of the class members' loss as the loss of control or loss of autonomy over their personal data*". The Court's reasoning is neatly encapsulated in the following ground-breaking paragraphs:

"The first question that arises is whether control over data is an asset that has value. … Even if data is not technically regarded as property in English law, its protection under EU law is clear. It is also clear that a person's BGI has economic value: for example, it can be sold. It is commonplace for EU citizens to obtain free wi-fi at an airport in exchange for providing their personal data. If they decline to do so, they have to pay for their wifi usage. The underlying reality of this case is that Google was able to sell BGI collected from numerous individuals to advertisers who wished to target them with their advertising. That confirms that such data, and consent to its use, has an economic value.

Accordingly, in my judgment, a person's control over data or over their BGI does have a value, so that the loss of that control must also have a value."

2. Did members of the class have the 'same interest' and were they identifiable?

Warby J thought not. The Court of Appeal disagreed and held that he had applied the 'same interest' test too stringently, partly because he had erred on the meaning of 'damage'. It said, "*Once it is understood that the claimants that Mr Lloyd seeks to represent will all have had their BGI – something of value - taken by Google without their consent in the same circumstances during the same period, and are not seeking to rely on any personal circumstances affecting any individual claimant (whether distress or volume of data abstracted), the matter looks more straightforward*".

However, the Court observed that by not relying on any facts affecting any individuals, damages are reduced to the lowest common denominator. It also thought it "*impossible to imagine that Google could raise any defence to one represented claimant that did not apply to all others*." The Court considered that members were identifiable by reference to the 'same interest' test – identification not being the same problem as verification.

> ***"Even allowing for some puffery, given the range in damages anticipated by claimants, and the hundreds of thousands of individuals affected by the breach, BA's potential liability could conceivably dwarf the ICO's £183.39 million notice of intent (which apparently equated to 1.5% of its global turnover)"***

3. Should the representative action have been allowed to proceed, as a matter of discretion?

Warby J thought not. The Court of Appeal disagreed and, in a key passage which illustrates the weight now attached to privacy and data protection rights by the appellate courts, held:

"… this representative action is in practice the only way in which these claims can be pursued. I do not accept the Judge's characterisation of this claim as "officious litigation". … It is not disproportionate to pursue such

litigation in circumstances where, as was common ground, there will, if the judge were upheld, be no other remedy. The case may be costly and may use valuable court resources, but it will ensure that there is a civil compensatory remedy."

What's next?

Google is reportedly set to appeal the decision of the Court of Appeal. Even then, unless it is overturned, a trial on liability and quantum is a long way off – this decision, however ground-breaking, only gets Mr Lloyd to the start line.

But while this case and others play out through the courts, here are some examples of steps organisations can take to prepare for the threat, not just of class actions, but of litigation in general:

- Mindful that prevention is the best cure, revisit your GDPR and e-privacy compliance, with a particular focus on data security (including breach response), and prioritise higher risk processing by consumer-facing (BA!) and workplace (Morrisons!) functions.
- Ensure that your people are appropriately trained and aware of their responsibilities when it comes to the use of personal data, to minimise the risk of a complaint in the first place.
- Review complaints-handling processes, because prompt resolution of data-related complaints can avoid them later spiralling into claims.
- Put in place a privilege strategy to reduce the risk of potentially damaging internal communications later being used against you in court.
- Watch out for 'weaponised' rights requests which are often used to exert pressure on organisations and, in the case of subject access, to fish for information at a pre-action stage. There is also an increased menace of 'mass rights requests' where, for example, multiple subject access requests are submitted by a single conduit on behalf of multiple data subjects .
- Consider the role of insurance as a means of transferring financial risk.

Meanwhile, note also that a pan-European collective redress mechanism for consumers in mass harm situations is being developed. The most recent proposal (currently before the European Parliament) assumes that collective redress mechanisms would be available for a wide variety of violations, including data protection.

The initiative has its critics, including the US Chamber Institute for Legal Reform (an affiliate of the US Chamber of Commerce) which stated that it "*could make the EU a major global hub for abusive litigation*" and that it "*lacks critical safeguards and may result in a system that is as bad or worse than in the U.S.*"

In any event, given the impact of economic globalisation and digitalisation, where an infringement of EU law has the potential to affect the interests of thousands or even millions of consumers across borders, the debate about data protection class actions is now only likely to intensify.

Ali Vaziri

Lewis Silkin LLP

Ali.Vaziri@lewissilkin.com