Data breach claims: a rebalancing by the English Courts?

12 October 2018

Summary

Personal data breaches and the risks of follow on litigation are very topical: British Airways, Facebook and Uber are just a handful of the organisations facing breach-related claims. Alongside the risk of fines of up to £20 million pounds or 4% of annual turnover, the claims have been seen as one of the unwelcome costs of the enhanced data privacy rights introduced under the GDPR since May 2018. However, recent cases show that the courts are willing to uphold boundaries in respect of individuals' claims for compensation, to ensure that the balance of rights is not unfairly or unjustifiably tipped towards claimants and their lawyers.

Emerging trends

Two cases this week suggest that compensation claims by individuals for a breach of data protection legislation are not a quick and easy ride to vast sums of money. The English Courts will uphold individuals' data privacy rights, but not to the extent of allowing generic claims for unspecified damages just because there has been a breach of the relevant data privacy rules. In addition, the English Courts are also currently considering whether an employer should always be on the hook for data privacy infringements carried out by disgruntled or 'rogue' employees. Three points in particular stand out for organisations from these cases.

Linking breach with damage

In *Lloyd v Google*, the first key point the Court had to consider was whether the breach of the DPA 1998 in fact led to a basis for any compensation. In this case, Mr Lloyd was seeking permission from the Court to serve proceedings on Google Inc. in the US, as part of a representative action under the civil procedure rules. The alleged breach was fairly clear: Google was said to have used the "Safari Workaround" between 2011 and 2012 to secretly track, collate and then sell the internet activity of Apple iPhone users. This much had already been largely laid out in the earlier *Vidal-Hall* case.

However, unlike in *Vidal-Hall*, where specific distress was alleged, here Warby J found that the individuals said to be concerned in the claim had not been shown to have suffered any specific damage or distress from the breach in question. With no compensation to award, the attempted claim fell at the first hurdle.

In the current environment of heightened data protection awareness by individuals and increased media coverage, it is often all too easy for organisations to lose sight of whether individuals have in fact suffered any distress or damage as a result of a personal data breach. Organisations suffering data breaches may well want to offer

compensation as part of a broader remediation or customer relations strategy, or a decision to settle out of court, but the decision in *Google* reminds us that courts will look for a **causal link** between the damages claimed and the breach. Clearly, by following regulatory guidance on data security and putting in place protective measures such as encryption or pseudonymisation, the risk of distress or damage to individuals will be reduced in the event of a breach.

Warby J in *Lloyd v Google*, para 26

"This claim does not depend upon any identifiable individual characteristics of any of the claimants, or any individual experiences of or concerning the Safari Workaround. It is generic. It does not allege the disclosure, or possible disclosure, on any screen of any personal information. There is no allegation that any individual suffered any distress or anxiety, however slight."

Really representative?

The second key point from the *Google* decision is a reassuring example of the English Courts preserving the balance between allowing access to justice whilst preventing unfounded claims. In particular, Warby J found that for a representative claim to succeed, it was not enough for potential claims to be linked to the same data breach, in addition all claimants must have suffered the same or similar damage to have the "same interests" in the claim. In this instance, he found the members of the class did not have the "same interests" as they suffered damage to differing degrees, with some suffering no damage at all. This will be important for organisations when facing claims from 'mass' groups, or handling communications in the immediate aftermath of a breach, as they will need to tailor their response to recognise that data subjects are not a homogenous class.

Morrisons and vicarious liability

While the *Google* decision will be welcomed by many, a potentially more significant case is the current appeal in *Various Claimants v Morrisons*. The case originally concerned a data breach committed by a rogue employee, who copied Morrisons employees' personal data and then later posted the data online. Following a claim for compensation by the affected employees, the judge at first instance found that, even though Morrisons was not primarily liable as a data controller, it was vicariously liable for the rogue employee's acts. Morrisons appealed and the case was heard before the Court of Appeal on 9-10 October.

The appeal

At the hearing, the Court seemed sympathetic to the view that data protection legislation is designed to achieve a balance between protecting individuals' rights **and** allowing the free flow of data. Ms Anya Proops QC, counsel for Morrisons, argued that there should be no separate vicarious liability where there is no relevant breach of the primary data privacy legislation. This has echoes of the causal link point in the *Google* case and it is also a reminder of how critical it is to establish the evidence to challenge the (public) perception of a data breach as an unbroken chain of events, and be clear what the organisation is really responsible for.

Further, Ms Proops pointed out that there is a false assumption that data should be protected no matter the cost to the data controller. In fact, the legislation is more balanced: under UK and EU law measures must be "appropriate". That balance (and some of the incentive for having protective measures) would be removed if organisations were always liable as employers, despite not being 'controllers' in respect of a rogue employee's actions.

Organisations need employees to access personal data, not just to run their businesses but also to meet the demands and expectations of their customers and other individuals they interact with. So it is encouraging to see these technical and policy arguments being clearly articulated in the courts. Whether ultimately determined by the Court of Appeal, Supreme Court or Parliament, organisations should be clear about this balance when approaching data security.

An unbroken chain of events?

In the *Morrisons* case, the rogue employee unlawfully disclosed the data (and so caused the damage alleged) via his personal computer at home on a Sunday two months after he was given access to the data, and after the completion of the specific task for which he was given the data. On this basis, Ms Proops argued that the employee's actions were part of his independent criminal plan and very obviously removed from his employment both by time and location. These arguments reflect what many organisations would expect – and indeed modern views on work and life balance – and will hopefully be accepted by the Court of Appeal so as to overturn the first instance decision that "*there was an unbroken thread that linked his work to his disclosure*".

What does this mean in practice?

Much is being said and written about the importance of preparing for personal data breaches in the context of the GDPR's mandatory breach notification regime. These cases emphasise that how you deal with a breach in those first few days, including the potential notification to regulators and communications to individuals is likely to have a huge impact on the eventual costs, financial or reputational.

The very existence of the *Google* and *Morrisons* cases shows that with individuals ever more aware (and ever encouraged by claimant law firms to be aware) of their GDPR rights, compensation claims will only become more common. However, the 'immediate response' to a data breach can mitigate the risks of litigation further down the line so long as all the relevant teams (including legal, PR and comms) bear in mind the issues likely to be key in any litigation, such as causation, who is the controller and whether claims can truly be grouped as representative actions.

Slaughter and May advises on all aspects of data protection and privacy. If you would like further information, please contact Richard Jeens or your usual Slaughter and May advisor. Further publications are available on our website.

Richard Jeens
T +44 (0)20 7090 5281
E **richard.jeens@slaughterandmay.com**

Cindy Knott
T +44 (0)20 7090 5168
E **cindy.knott@slaughterandmay.com**