Boom or bust? The data breach claims landscape in 2025

Justin Tivey
Partner
T: +44 (0) 117 918 2697
jtivey@dacbeachcroft.com

Georgina Jones
Solicitor
T: +44 (0) 117 366 2473
gejones@dacbeachcroft.com

The UK Information Commissioner's Office (ICO) can act against organisations but crucially cannot award compensation to individuals affected by an alleged breach of their data rights. Left to pursue organisations themselves, these individuals are faced with making a claim against the at fault organisation.

These innovations continue to generate serious questions about whether the obtaining and processing of data via these methods is compliant with data protection laws. A number of the current regulatory responses to these activities are discussed in our accompanying piece 'Approach to Regulatory Enforcement in the UK and EU: two sides of the same coin?'

Recent developments in AI raise further compliance issues. At one end of the spectrum, AI systems need vast amounts of training data and, at the other end, AI systems themselves support faster, more targeted data collection and analysis. Data as a commodity is becoming ever more valuable. There is profit to be had in the exchange of an individual's personal data, whether for worthwhile or nefarious purposes.

Of course, there are occasions when personal data is exposed, when an organisation holding that data discloses it, knowingly or unknowingly, to a third party. Data has helped to shape every aspect of the modern world. Every day, vast volumes of personal and non-personal data are processed, carrying enormous value to businesses and to governments. Continuous innovation has produced new ways to obtain and aggregate data from the use of websites and social media. Cookies and tracking technologies are now considered a normal element of the online experience. Developments in 'consent or pay' models offer individuals access to online services such as social media and news websites at the cost of consenting to the use of personal data for personalised advertising.

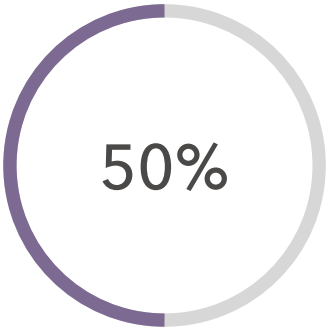
A brief history lesson

The right to compensation for a breach of data protection law has been enshrined since the Data Protection Act 1984 and Data Protection Act 1998 (DPA 1998) which allowed for a compensation claim for damage caused by a data breach. Initially, it was understood a claim for distress under the DPA 1998 had to be accompanied by some form of pecuniary damage, however the 2015 judgment in *Vidal-Hall v Google* held that a claim for distress could be brought without the need for pecuniary damage.

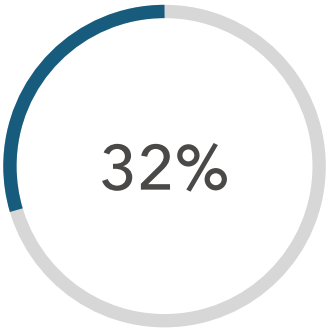
The subsequent introduction of the GDPR and the Data Protection Act 2018 (DPA 2018) was expected to light the blue touch paper and generate a data claim boom. This expectation was created in part by successful lobbying by the insurance industry to tackle the large number of whiplash claims in motor collisions. Inevitably, in light of these reforms, attention turned to the next source of claims for the claimant practitioner market and, following the implementation of the GDPR and DPA 2018, data breach actions were often referred to as the next potential source of a claims influx.

However, from the early days of the GDPR in 2018 until now, our experience is that the flow of data breach claims in the UK has dwindled to a relative trickle as possible avenues for claims have been slowly restricted or closed off by judicial decisions or financial considerations.

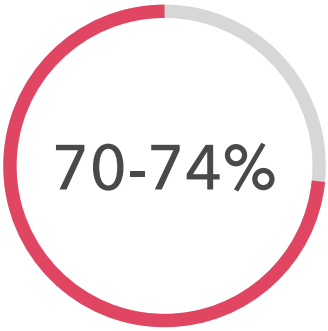
What does this mean for the data breach claims market in the UK in the coming year?



Businesses experienced a cyber breach or attack



Charities experienced a cyber breach or attack



Increased risk for medium and large size bussiness

On the right track?

Using available data, and our own extensive experience in advising clients affected by data breaches, breach events themselves continue to occur, increasing rather than decreasing, at pace. In 2024, the Department of Science, Innovation and Technology reported that 50% of business and 32% of charities experienced some form of cyber security breach or attack in the last twelve months. The risk for medium and large size business increases significant, with 70% and 74% respectively suffering an attack or breach in the preceding twelve months.

Therefore, the number of data subjects affected by data breaches continues to increase, and corresponding claims are brought pursuant to Article 82 of the UK GDPR. Article 82 provides a data subject who has suffered material or non-material damage the right to bring a claim for compensation for the damage suffered. The distinction between the two types of damage can be summarised as: 'material damage' resulting in a direct financial loss, and losing money or 'non-material damage,' meaning that the data subject has suffered distress.

It is rare for a data breach action to include a claim for material damage. Actions for 'non-material' distress claims are the standard basis for many of the data breach actions we handle.

In both the EU and UK, there have been judicial considerations as to whether the simple act of infringing the GDPR is sufficient for a compensatory award and/or if alleged 'non-material' distress must reach a degree of seriousness, passing the de minimis threshold.

However, even in the event that a claim for non-material distress is sufficient to justify an award of compensation, most individual data breach claims are notoriously low in value, meaning that the legal costs to pursue them easily outstrip the claim value.

Many claimant practitioners have made efforts to supplement their statutory data breach actions with claims for breach of confidence and misuse of personal information (MPI). However, the Courts have already shown their dislike of 'kitchen sink' claims which seek to attach MPI, or breach of confidence claims to statutory data breach claims, particularly where that choice will potentially increase the costs awarded in a claim.

In the UK, a civil action such as a data breach claim will be assigned to a track depending on the value of the claim and its complexity.

The lowest reported claim to exceed the de minimis threshold in the UK was awarded £250, placing this and other such claims firmly into the small claims track. This track is for those monetary claims valued under £10,000 or valued under £1,500 for personal injury claims (unless they are legally particularly complex). In most cases the parties do not recover legal costs should they win a small claims trial. This can make low value data breach claims unattractive to claimant legal representatives, and it has become well-trodden path for many data claims to be allocated to the small claims track, only to fall away in the absence of any prospect of costs recovery.

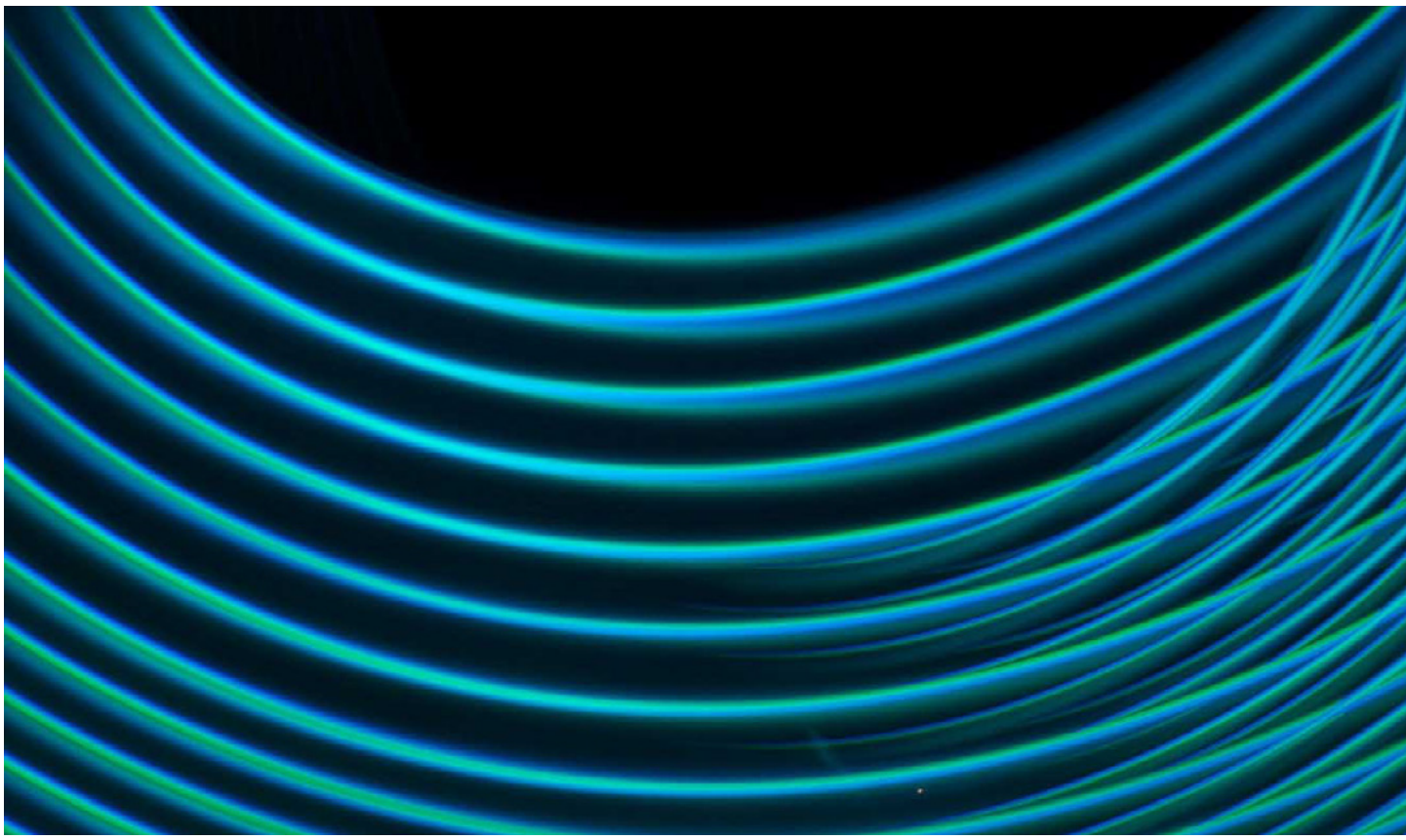
However, outside of 'kitchen sink' claims, other practitioners have made efforts to bring claims outside of the scope of the small claims track, potentially increasing the costs recovery available on conclusion. To this end, we have seen claimants, and their representatives argue that distress is a personal injury or that data claims are inherently complex, commonly supporting this with a psychologist's medical report. These reports are often no more than a pro-forma template, based on a brief telephone interview with a claimant and a copy of the letter of claim.

Applications to transfer data breach actions to the fast track are becoming increasingly common, as transfer to the fast track will result in an award of costs in the event that the claim is successful. Of course, this would make a fast track action more attractive to claimants and legal representatives.

For claims issued after 1 October 2023, the introduction of the Fixed Recoverable Costs (FRC) regime has created an additional buffer between the fast and multi-track. There is a new intermediate track for claims between £25,000 and £100,000 and although this is unlikely to be troubled by a data claim, a fixed recoverable costs regime also applies. This gives costs certainty, although the permitted costs are low and there are tiers depending on the complexity of the case.

After a year in operation, it remains early days to see the full impact of this on data claims. However, if it were thought that claimant firms would work out a model for making the recoverable costs pay which would boost the prospects for more low value claims, this does not appear to have happened yet. It may be that the low costs recoverable under the FRC model is not attractive enough to make low value data claims a viable source of revenue.

We expect to see the regime tested in 2025 and arguments over whether distress is a personal injury, the right track and level of complexity will rumble on.



All aboard the class action train… or the omnibus?

Various forms of collective redress exist in the UK, such as group litigation orders which involve a large number of individual claimants, or representative actions offering the chance for a single claimant to advance a claim on behalf of a class of individuals affected by a civil wrong. It should be noted that both models of collective redress require significant time and cost investment to bring together the claimants, even before there is consideration of whether the claims pursued are viable.

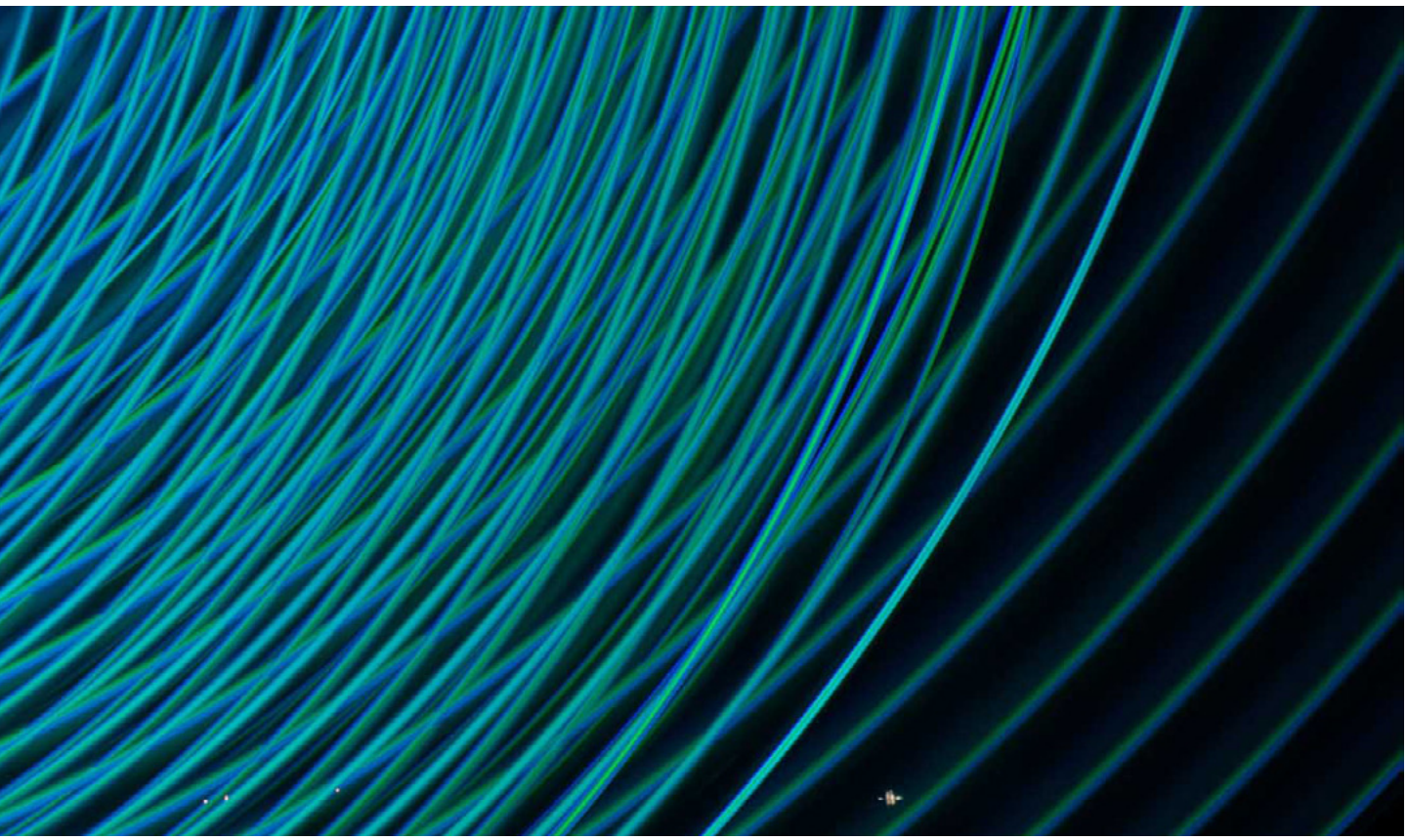
Representative actions

The Supreme Court's ruling in *Lloyd v Google* is the key case demonstrating the difficulty in bringing data claims under the representative party procedure permitted by CPR 19 of the Civil Procedure Rules. The claim alleged Google improperly collected user browsing histories when using the Safari browser. The Supreme Court held that the simple loss of control over data (in this instance, the browser history) was not a cause of action in itself and did not give an automatic right to damages.

If a breach of data protection legislation was established, then the claims required the damages for distress to be assessed individually for each class member depending on the extent of the data and their personal circumstances. The representative action procedure required class members to have the 'same interest' in the claim. In this instance, there was found to be no 'same interest', despite the representative claimant submitting that each claim would be limited to the same monetary figure.

The limited prospect of successful collective redress for data privacy breaches has been reinforced by the recent decision *Prismall v Google*, where the Court of Appeal upheld a decision rejecting an opt-out representative action for misuse of private information. The 'same interest' test was again applied, with the court specifically noting that a representative class claim for misuse of private information *"is always going to be very difficult to bring". In this instance, "relevant circumstances will affect whether there is a reasonable expectation of privacy for any particular claimant, which will itself affect whether all of the represented class have "the same interest."*

This action was itself an effort to circumvent the outcome in *Lloyd v Google* by reformulating the claim to one for misuse of private information, seeking damages for the loss of control of data. However, as noted in the judgment with reference to the outcome in *Lloyd*, *"to establish a reasonable expectation of privacy, it would be necessary to adduce evidence of facts particular to each individual claimant."*



In short, the decisions in *Lloyd* and *Prismall* make it clear that data representative actions, whether brought in data protection or for misuse of private information, will struggle to circumvent the obvious judicial restraint seen.

Competition Appeal Tribunal

A broader class action regime does exist in the UK in the Competition Appeal Tribunal (CAT), raising the question of whether pursuing data claims in competition law could be a way to circumvent *Lloyd v Google* issues?

Considering this prospect, we note the issue of collective proceedings by Dr Liza Lovdahl Gormsen on behalf of 46 million Facebook users against Meta. The basis of this claim is that Meta abused its position in the UK social media market by allegedly forcing Facebook users to let Meta utilise their data gathered on third party websites and applications. The claim seeks damages of up to £2.1 billion plus interest. Meta has twice sought to block the claim on the basis that it is without merit, but in October 2024 the Court of Appeal permitted the complex issues to be determined at trial.

Although the claim references a number of data protection concepts and issues it has been brought as a breach of competition law alleging abuse of a dominant market position. The trial is expected to take place in 2026 but it will be interesting to see if other data claims are launched via this route in 2025.

Where claims are based on organisational practices which allegedly infringe data subject rights this could be an option, however, it should be noted that the CAT route would not be suitable for claims based on a data breach where records are compromised by a hacker and where security of processing is the issue. In these cases, it would be difficult to reformulate the alleged failings of the data controller as an abuse of its market position as opposed to a failure to meet a required level of security.

The 'lead' claimant option

The CPR 19 procedure also permits any number of claimants to be joined to a claim, as discussed in the *Farley v Paymaster* decision in the Court of Appeal below. The Court can then order 'lead' cases only to proceed to decide common issues of breach or quantum. All claimants are participants in the proceedings and carry a costs risk.

Farley v Paymaster (trading as Equiniti) involved a pension scheme administrator which in August 2018, posted annual pension statements to the former addresses, rather than current addresses, of hundreds of police officers. 474 individuals issued a claim against Equiniti for a breach of the GDPR and misuse of private information, alleging anxiety, alarm,

distress and embarrassment by the fact that personal data, such as their employment status, had been passed and/or may have been passed into the hands of unknown third parties. Of 474 claimants, fourteen claimed a third party had opened their letter. Two claimants were able to evidence that the letters had been opened by a third party who was not a family member or colleague.

Mr Justice Nicklin held that the basis of the claims was closer to the *TLT v Secretary of State for the Home Department* line of cases (accidental publication of data) than the *Warren v DSG Retail* (data hacked). In *TLT* the claims had succeeded based on misuse of private information and data protection grounds. However, at the crux of a successful data claim was demonstrating that distress (financial or psychological harm) has actually been suffered. The Court found that was simply not the case here for most of the claimants when the pleadings were made on a merely inferential basis.

Nicklin J emphasised that to have a viable claim for misuse of private information, a claimant must be able to show a real prospect that the information was seen by a third party. Misuse was an essential element of this tort. In addition, claims had to pass the threshold of seriousness. In essence, the High Court found there had not been any *"real processing"* unless the statement had been opened or read by a third party and struck out the majority of the claims.

However, the Court of Appeal has granted leave for these claimants to appeal the High Court's decision. In doing so, the Court of Appeal recognised that *"in principle an individual may establish that personal data have been processed in breach of their data protection rights without proving that the information or data have in fact been read or otherwise communicated to anyone"* with the example given of the transfer of data from a secure location to an insecure location, or transfer of personal data to a foreign jurisdiction. This in itself would be considered 'processing' in the context of GDPR and the claimants therefore would have a real prospect of success on this argument.

Given the importance of the point the ICO has been invited to intervene to assist the court for those remaining actions.

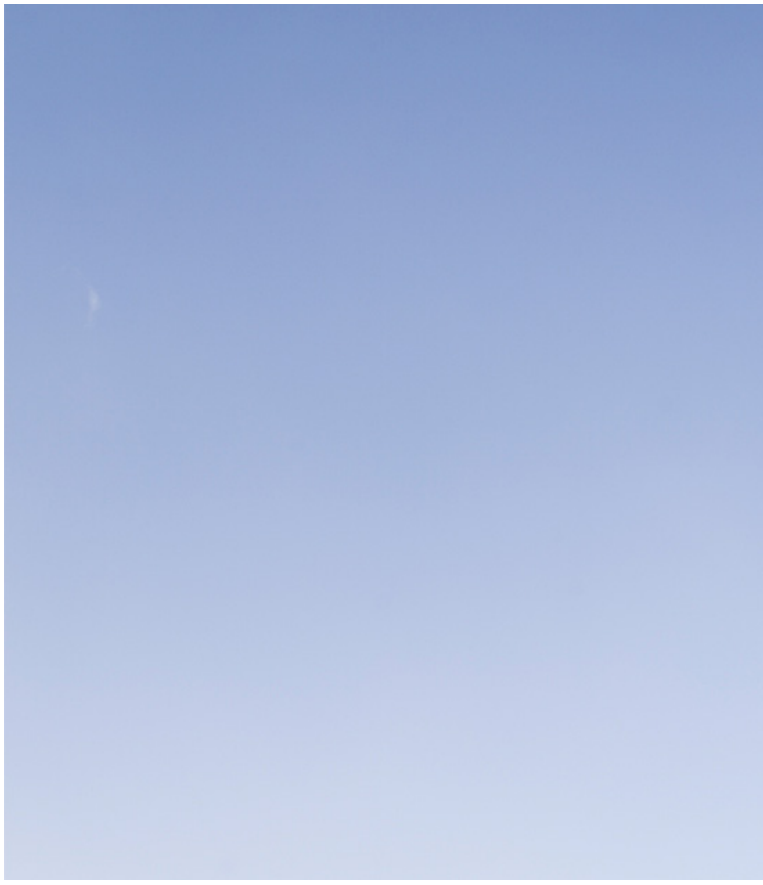
The judgment highlights the future of the minor data breach claims that are prevalent in the market, reinforcing that any claimant must show that their case passes the threshold of seriousness, and that burden rests firmly with the claimant. More importantly, prospects of success will not be improved by making perceived exaggerated claims as to the impact of a breach.

The omnibus claim form

Although not a data breach action, the claim of *Adams v Ministry of Defence* earlier this year demonstrated the possible value of omnibus claim forms to the claimant data breach community who are seeking to limit their financial exposure to individual court fees. Mentions of an 'omnibus claim form' are effectively a reference to the type of claim form permitted by CPR 7.3, which specifically allows claimants to *"use a single claim form to start all claims which can be conveniently disposed of in the same proceedings"*. The claim is then brought by multiple claimants alleging separate but very similar claims against the same defendant.

In short, omnibus claim forms avoid the costs and complications of the representative and group litigation order processes, and also avoid the alternative of issuing individual claims which incur individual court fees and are at the mercy of low value claim costs restrictions.

Again, although not a data breach action, *Adams* considered the question of convenience for the parties and the court, and will offer an option for those practitioners who may wish to pursue data breach actions in this fashion. In addition, it is understood that the Civil Procedure Rules Committee will offer further clarity on these actions in the coming months.



What will 2025 bring?

Data claims existed before the introduction of the GDPR, yet this was expected to be the trigger for a data claim boom. However, the Courts have taken clear action limiting the efficacy of class actions, actions involving multiple causes of action and to date, have taken a robust view of whether trivial claims merit damages at all. Combined with fixed recoverable costs, the environment is making pursuing these claims financially challenging for claimant law firms.

However, it would be unwise to assume that data breach actions are unlikely to pose issues in the future. They will continue to be brought in 2025 in large numbers. One-off breaches can still be pursued if the grounds are clear enough often with the aim of seeking an early settlement. Defendant costs can be as prohibitive as the costs of bringing a claim, and the application of the fixed recoverable costs regime may yet find a claims model that works for claimants. Similarly, large scale multi-claimant cases may yet find a route through as competition claims and the omnibus claim form is viable for the right claims.

From the perspective of making rights enforceable and holding the wrongdoer to account, the picture is difficult for claimants, but the Courts have, correctly, tried to limit the use of the litigation process to the most serious breaches – and no one seems to be calling for a Data Ombudsman Service!

Full list of references available upon request