



Data analysis

Andrew Hogan examines the best way to apply costs budgeting in data breach litigation

Data breach litigation is on the rise. Earlier this year the Supreme Court heard arguments in the case of *Richard Lloyd v Google LLC*, and at the time of writing this article, the handing down of the judgment is awaited. That case raises important issues, including the concept of what is or can be ‘damage’ for the purposes of a data breach claim; and how a representative claim where millions of potential claimants might sue should be structured.

But several actions have already been brought where group litigation orders have been made that provide for a register of thousands, or tens of thousands of claimants, all of whom may have suffered a data breach. Such a case may involve very high levels of costs to establish liability, but to establish the quantum for each individual claimant, may require very little time to be spent on each client.

This latter type of litigation also illustrates with clarity how a solicitor’s retainer may need to be rethought from the traditional time-and-rate basis, to accommodate the dynamics of such litigation; and how this may then feed through into costs capping or costs budgeting. As I will discuss below, a solicitor may very well be doing themselves a disservice in not adapting their charging structure to move with the times.

THE COURT OF APPEAL

The case of *Richard Lloyd v Google LLC* [2019] EWCA Civ 1599 was summarised by the Court of Appeal in these terms:

‘The claimant, Mr Richard Lloyd (Mr Lloyd), is a champion of consumer protection. This action seeks damages against Google LLC, the defendant, a Delaware corporation (Google). Mr Lloyd makes the claim on behalf of a class of more than 4 million Apple iPhone users. It is alleged that Google secretly tracked some of their internet activity, for commercial purposes, between 9 August 2011 and 15 February 2012.

‘Warby J dismissed Mr Lloyd’s application for permission to serve Google outside the jurisdiction on the basis that: (a) none of the represented class had suffered “damage” under section 13 of the Data Protection Act 1998 (the DPA), (b) the members of the class did not anyway have the “same interest” within CPR Part 19.6(1) so as to justify allowing the claim to proceed as a representative action, and (c) the judge of his own initiative exercised his discretion under CPR Part 19.6(2) against allowing the claim to proceed.’

These are important issues. The claimant succeeded in the appeal court, and the part of the judgment that deals with the nature of ‘damage’ for the purposes of a claim in tort for data breach is extremely significant. If, for example, someone’s medical records are scattered over the internet, it is not going to be hard to establish that they may well feel distress.

If someone’s bank details are stolen, and their account is emptied by a criminal, they have plainly suffered economic loss. But the case of Lloyd is concerned with a subtler kind of damage, when a person loses control over their data, and may be unaware of the loss of their control, and suffer no obvious adverse effects.

If loss of control amounts to damage, then the net of liability is going to be cast far more widely in respect of claims for data breach than might otherwise be the case. The appeal court found for the claimant on this point: ‘The first question that arises is whether control over

data is an asset that has value. That question again should, in this context, be answered as a matter of EU law. In *Your Response Limited v Datateam Business Media Limited* [2014] EWCA Civ 281, this court held that, as a matter of English law, an electronic database was not a form of property capable of possession and that, therefore, it could not be subject to a possessory lien. That question may in due course need to be revisited, but it does not, in my judgment, affect the answer to the relevant question for current purposes.

‘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 [browser generated information] 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 wi-fi 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.’

If this judgment is upheld, then the scope for data breach litigation to become more costly for the tortfeasor will be very great.

A solicitor may very well be doing themselves a disservice in not adapting their charging structure to move with the times

THE SUPREME COURT

Google has appealed to the Supreme Court. The issues ventilated in the appeal can be summarised as follows: whether the claimant should have been refused permission to serve his representative claim against Google out of the jurisdiction (i) because members of the class had not suffered ‘damage’ within the meaning of section 13 of the Data Protection Act 1998 (DPA); and / or (ii) the claimant was not entitled to bring a representative claim because other members of the class did not have the ‘same interest’ in the claim and were not identifiable; and / or (iii) because the court should exercise its discretion to direct that the claimant should not act as a representative. The decisions on these issues will set the parameter of representative actions for years to come, though they will not supersede group actions in appropriate contexts.

CHARGING FOR WORK

Most data breach actions will be funded by claimants making conditional fee agreements that can trace their pedigree back to variants of the Law Society model CFA. They will provide for time-based charging, with hourly rates, and the charging of units, for routine tasks. But only liability costs will really be facilitated by such a model, dealing with what might be termed the generic or common costs of the litigation, and then only to a degree.

A factor that retainers devised 30 years ago do not cater for is the rise

DATA BREACH





7

and use of information technology, and increasingly, artificial intelligence (AI), to automate and streamline and turn into a process of mass production, the bespoke, artisan practice of litigation.

This is the concept of ‘near zero marginal cost’ – a phenomenon of the digital age, where it costs virtually nothing to provide additional products at minimal, or even zero costs. The music and publishing industries, providing digital downloads of identical products to millions of users, are the clearest examples of how services can be provided at near zero marginal costs. There is scope despite its bespoke heritage for some litigation services to be delivered in a similar fashion.

In terms of low-value individual claims such as data breach claims, increasing automation makes a nonsense of the notion that time claimed is a reliable indicator of reasonableness. Indeed, if the solicitor found that the actual cost to him of running a case was £25, or that only 30 minutes of grade D fee-earner time represented the totality of the ‘touches’ on a file, he might be doing himself a serious disservice by charging on a time incurred basis. In effect, time-based charging for work on generic costs and a value-based charge for work done for an individual claimant’s specific costs makes a lot more sense. But even this ‘bright line’ division may not go far enough.

In terms of high-value litigation, AI tools permitting key word searches

and automation of the disclosure process will greatly reduce the amount of fee-earner time hitherto routinely spent in enormous quantities. How does a solicitor quantify and charge for the use of a software programme in the context of a multi-million-pound dispute? Logically, it should be by the added value given to a case.

BUDGETING DATA BREACH LITIGATION

The cracks are already starting to show between automation, time-based charging and costs budgeting.

In the well-known British Airways data breach case, several of the costs budgeting hearings before a High Court judge, Mr Justice Saini, were reported. *Weaver v British Airways (No 1)* [2021] EWHC 217 (QB) confirmed that the costs of advertising were not recoverable as an item of costs, but were an overhead subsumed in the hourly rates. The more interesting judgment is the second one: *Weaver v British Airways (No 2)* [2021] EWHC 520 (QB).

In that case, the High Court judge had to grapple, among other things, with the individual costs of the claims that were sought to be budgeted:

‘It is fair to observe at the outset that in terms of the individual costs per case, the claimants’ solicitors’ figures have varied quite substantially.

Continued on page 8



**Continued from page 7**

Originally, the claimants were seeking a sum of about £1,200 per case. That was modified down to £800 per case and, on the figures before me this afternoon, the figure sought by way of estimated costs has come down further to £624 per case. That £624 has been broken up into a detailed schedule of 25 specific sub-steps and I have been taken through those steps by counsel both by way of oral and written submissions.'

Logically, because there was no marginal cost in time to producing 'round robin' letters, he found that there was no cost to be budgeted: even though the 'round robin' letter would be a service to the client, of use to them, and capable of having a value ascribed to it:

'Following further argument on this issue (and reference by both leading counsel to the *Motto* case at para. 504, and to Langstaff J's judgment in *Various Claimants v Morrisons* (unrep. 12 January 2017) at paras.22-27), I have determined there is no evidential basis for adopting a per capita approach (even to only two round robin letters) in the form suggested in the narrative I have set out above. That is, an approach which multiplies the claimed average unit cost of a round robin letter by the number of individual claimants (as if that unit cost would in fact be incurred in the sending of the standard letter).

'I note that the costs of drafting the common letters to be sent to all clients have already been covered in the generic costs. So the real legal "brain work" is already accounted for. What is left is simply sending the product of such work to the many claimants. However, the claimants' legal representatives were not able to point to any evidential basis for the assumption that the simple electronic sending of those same letters to tens of thousands of individual clients would each take an average of one minute of chargeable time. It is obvious how the sums claimed under this head would increase by very substantial sums, potentially running into hundreds of thousands of pounds, if the multiplier per capita approach was endorsed.

'I am not satisfied charging on the basis of this approach would be either reasonable or proportionate. As I explained at the hearing, my view is that the sums claimed are excessive for the relatively straightforward matter of what seems to me (based upon my own basic and limited technological knowledge) to be the act of undertaking some keystroke work to enable a mailing of the already drafted letters to clients whose details are already electronically stored.

'I accordingly rule that no sum is claimable in the budget under item 23 for the round robin letters. For completeness, I should record that I did not find it easy to follow how the allowance for such letters was fixed in the *Motto* and *Morrisons* cases, where the facts were very different. It was however rightly not suggested that either of those cases applied some principle of law or practice which required me to take an approach different to that which I have decided to adopt on the evidence before me.'

Would a different, perhaps fairer result have been obtained, had

Value-based fees may be a logical way forward for most of the individual costs of data breach claims

the solicitors charged each client a flat fee of £500 for handling the individual elements of their case from start to finish, together with charging them an hourly rate for their share of generic or common costs? It is difficult to say: because convention and tradition can be heavy hands, pressing down on innovation in any field, particularly a traditional one such as the practice of law. Moreover, judges are used to hourly rates: they are not used to assessing value-based charges of which they may have little experience.

But if costs charged on a 'value added' basis without reference to time are challenged, either by a regretful client or a paying party in a recoverable costs assessment, how should the court approach their quantification? The court's approach to the assessment of contentious costs is governed by rule 44.4 CPR containing the seven (now eight) pillars of wisdom.

Of these factors, only one, factor (f), specifically enjoins the court to have regard to the amount of time spent on the case. In addition, there is a respectable body of case law on non-contentious costs derived from the Solicitors (Non-Contentious Business) Remuneration Order 2009 and its predecessors, where a value charge is the norm in areas such as probate, to allow the court to draw upon by analogy, when determining whether a contractually agreed fixed fee is reasonable.

It follows that far from being an economic disaster, fixed demonstrably justifiable value-based fees may be a logical way forward for most of the individual costs of data breach claims, and other similar, expensive litigation where the monetary reward for each individual client may be modest.

Andrew Hogan practises from Kings Chambers in Manchester. His blog on costs and litigation funding can be found at www.costsbarrister.co.uk



DATA BREACH

