Data protection in media litigation

Jennifer Agate and Owen O'Rorke

Summary

With the final text agreed and not even Brexit likely to stop it taking effect in May 2018, the General Data Protection Regulation is looming large on the agenda for all practitioners. This is particularly so in the field of media litigation, with recent case law establishing that not only can data protection be brought alongside defamation claims, as it already has been in alongside privacy claims, but it can be used to claim damages for distress.

In this article we discuss the increasing prevalence of data protection claims in media complaints and litigation and how it fits around the more traditional routes in defamation and misuse of private information.

Background: data protection and the tort of misuse of private information

The synergy between misuse of private information and data protection law is a particularly strong one, with the two being used in tandem since misuse of private information was first developed from the law of confidence.

Misuse of private information is based on the principle under article 8 of the Human Rights Act 1998 that everyone has the right to respect for his or her private and family life. Where a reasonable expectation of privacy exists in information, a balancing act must be carried out between that privacy right and the publisher's article 10 right of freedom of expression. Where the balance falls in favour of privacy, publication can be restrained.

Similarly, the Data Protection Act 1998 (DPA) imposes obligations on data controllers to obtain, hold and process personal data fairly and lawfully, and – among other requirements – to process personal data in accordance with the rights of data subjects (the 6th Principle). These rights include the section 13 right for compensation, but also the right to prevent the processing of personal data likely to cause damage or distress (s 10 of the DPA), and the right to rectify or erase information that is inaccurate (s 14 of the DPA).

In DPA claims, as in misuse of private information (since *Ash v McKennitt* [2006] EWCA Civ 1714), a claim can be brought whether the information itself is false or true. The section 14 right of rectification – almost entirely unchanged with the forthcoming Regulation (under art 16) – derives from the 4th Data Protection Principle, namely that it is the responsibility of data controllers to ensure that the personal information they hold (and process) is accurate.

'Personal data' covers all information which is being processed by equipment operating automatically or is kept on a 'relevant filing system' – which essentially means where it can be easily accessed by reference to the data subject (the person to whom the information relates). That person can be any living individual who can be identified from that data, or from other data in the possession of (or likely to come into the possession of) the data controller.

Nor does information need to be 'private' or confidential to fall within the effect of the DPA, or grant data subjects their legal rights. Whilst weight may be given to whether information is already in the public domain in terms of, for example, the likelihood of damage or distress (under ss 10 and 13) or some other harm resulting from unauthorised processing (a security breach under the 7th Principle), section 2 of the DPA prescribes a very literal test to whether personal data is 'sensitive' or not (which will limit the conditions by which a data controller may process that information).

It was established as early as 2003 that a photograph is capable of constituting personal data within the meaning of the DPA (*Campbell v MGN* [2002] EWCA Civ 1373 and *Douglas v Hello! Ltd (No5)* [2003] EWHC 786 (Ch)). Where a photograph reveals information such as the racial or ethnic origin of the subject, notwithstanding that the information may be widely known, it has been held that will fall within the definition of 'sensitive personal data' (*Murray v Big Pictures* [2007] EWHC 1098 (Ch)).

Data Protection first appeared in early privacy cases brought by Naomi Campbell and Michael Douglas and Catherine Zeta-Jones, although perhaps initially as more of a sideshow. In the Douglas case for example, a court awarded £3,750 for the distress caused by the privacy breach but only £50 each under the DPA. It took the important Court of Appeal ruling in *Vidal–Hall v Google Inc* [2015] EWCA Civ 311 (discussed below) to finally cement data protection as a truly viable standalone alternative.

In *Weller & Ors v Associated Newspapers Limited* [2015] EWCA Civ 1176, the Court of Appeal held unanimously that the High

Court had been correct to find the *Daily Mail* liable for both misuse of private information and breach of the DPA. Paul Weller had initiated proceedings following an article and photographs published by Mail Online which identified the children by name (although incorrectly in the case of the elder daughter, who was identified as his wife).

It was agreed by both parties that the data protection claim stood or fell with the main privacy claim, meaning that the data protection element gains little attention in either the High Court or Court of Appeal judgment. This is a view which has perhaps persisted at the media bar; but data protection lawyers tend not to agree that, on a literal reading of the black-letter law, the overlap between a DPA claim and a tortious claim for misuse of private information will always be quite that neat.

Even so, and while claimants should not expect to 'double dip' in terms of damages recovery, the case is yet another reminder of the increase in the use of the DPA in tandem with the more traditional claims of misuse of private information and defamation and shows how the three remedies are being increasingly combined by claimants. The *Daily Mail* was ordered to pay Weller's costs plus £10,000 in damages (£5,000 for the elder daughter and £2,500 each for the twins).

The Weller proceedings were issued and heard before the *Vidal-Hall* decision, so it seems likely that if they had been heard later, data protection would have played a more major role.

An alternative to defamation?

The impact of the Defamation Act 2013 is often misrepresented as the death of libel cases. While this is not quite the case, the new requirement under section 1 for claimants to show that they have suffered or are likely to suffer serious harm (and for bodies who trade for profit, serious financial loss) has given defendants an answer to many more complaints. Data protection represents a viable alternative, especially in light of *Vidal-Hall,* with the lower bar of suffering 'damage' by reason of a proven contravention of the DPA.

Equally, in complaints about online content under data protection, ISPs cannot rely on the intermediary defences as they could in defamation, making them quicker to take content down. *Google Spain SL & Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez*, Case C-131/12, established that a search engine is a data controller and has an obligation to remove out of date or 'irrelevant' content from search results unless there is an overriding public interest in it remaining. The resulting take-down procedure, the so-called 'right to be forgotten', is to be enshrined in legislation once the new Regulation is in force (art 17).

This decision paved the way for Max Mosley to bring a claim against Google under section 10 of the DPA for its failure to remove images taken from undercover footage filmed by a prostitute for the News of the World in 2008 (*Max Mosley v Google Inc and Google UK Ltd* [2015] EWHC 59 (QB)). That case settled before the case could come to trial.

Data protection can therefore arguably go further than defamation, allowing claimants to tackle historic online material where it is merely inaccurate rather than defamatory. As will be discussed further below, where there is a contravention there may also be grounds for a damages claim.

Nor should data protection stand alone. The High Court has recently confirmed (*His Highness Prince Moulay Hicham Ben Abdullah Al Alaoui of Morocco v Elaph Publishing* ***Limited*** [2015] EWHC 2012 (QB)) that a data protection claim can be run alongside defamation. In that case, the claimant had originally issued under libel but later sought permission (after a finding that only one of three pleaded meanings was capable of being defamatory) to add a claim under the DPA. The defendant had put forward various arguments, including that there was no real and substantial tort and that the litigation would 'not be worth the candle', making the amendment abusive. The judge rejected this argument, holding that the claim was capable of being a real and substantial tort.

Damages for distress

Section 13(1) of the DPA allows a claimant to apply for compensation where the defendant has failed to comply with data protection requirements and the claimant has suffered 'damage' as a result. Section 13(2) specifies that an individual who suffers distress as a result of the breach is entitled to compensation for that distress if: (a) the individual *also* suffers damage by reason of the contravention; or (b) the contravention relates to the processing of personal data for the special purposes.

Prior to the Court of Appeal ruling in *Vidal-Hall*, and despite the suggestion in the earlier Court of Appeal case of *Halliday v Creation Consumer Finance Ltd* (2013), it had been viewed that section 13(2) imposed a bar on recovering damages under the DPA where *only* distress – as opposed to actual financial loss – had been suffered.

For example, in *Johnson v Medical Defence Union* [2007] EWCA Civ 262, the courts had stated that the definition of 'damage' under section 13(1) of the DPA was limited to pecuniary loss and could not encompass damage to reputation. That case concerned a claim against an insurer, where the claimant argued that unfair processing of his personal data and subsequent termination of his professional indemnity cover had resulted in damage to his professional reputation. The Court of Appeal held that as the claimant had not suffered pecuniary loss, he could not recover damages for distress under s13, indicating that the law of defamation was the correct field for such losses:

> *Nor can English law be said in that regard not to respect its obligation to give compensation for loss of reputation caused by unfair processing of automatic data. If an Englishman thinks that that has occurred he can always actually sue in defamation, with the prospect of recovering far more, and on a less exacting basis, than he would find in other member states of the Community.*

The tide began to turn with the Court of Appeal in Murray v Big Pictures Limited [2008] Civ 446, when the court suggested that earlier court may have construed 'damage' too narrowly. The court indicated that this point should be resolved at trial, but the case settled before that could take place. The *Halliday* case raised the prospect that courts might be willing to 'bolt on' substantial damages for distress having only made a nominal finding of actual loss, but when the defence ceded the point the case was resolved without a ruling on the issue.

The position changed in 2015 when *Vidal-Hall v Google Inc* [2015] EWCA Civ 311 established that damages for breach of section 13 of the DPA can be awarded even where there is no evidence that financial loss has occurred.

The case (concerning an application to serve outside the jurisdiction) was brought by a group of claimants who claimed that by tracking and collating information relating to their internet usage on the Apple Safari browser without their consent, Google had (amongst other wrongs) breached its obligations under the first, second, sixth and seventh principles of the DPA. Buxton J's earlier comments, the court found, were *obiter* and not binding. The DPA claim could now take centre stage in media litigation – with the important caveat that the Supreme Court has granted Google permission to appeal.

Subject access requests as a disclosure tool

Although not exclusive to media cases, data protection is also increasingly being used as a tool in the form of subject access requests where litigation is contemplated as an alternative to an application for early disclosure under the Civil Procedure Rules.

The case of *Gurieva & Anor v Community Safety Development (UK) Ltd* [2016] EWHC 643 (QB), concerned a private investigations company who had been investigating the claimant for the purposes of a private criminal prosecution in Cyprus. The claimants made a subject access request and, having been dismissed with what the judge described as 'to say the least, surprising points to take', made an application for an order under section 7(9) of the DPA (courts having the power on application to compel data controllers to comply with subject access requests).

The defendants contested the claim on three grounds: (1) the validity of the subject access request; (2) that the personal data was exempt from the regime by way of the crime and privilege exemptions; and (3) that the claim was an abuse of process, with the subject access request being used as a device with the purpose of gaining an illegitimate procedural advantage in the Cyprus proceedings. Whilst the UK's data protection regulator, the Information Commissioner's Office (ICO), takes the strong view that a data controller's obligations to comply with a SAR must be motive-blind, the courts have tended to take a different view (see *Dawson-Damer v Taylor Wessing* et al on the question of abuse of process).

In *Gurieva,* Warby J demurred from the usual line taken by the bench:

> *I have difficulty also with the notion that the use of a SAR for the purpose of obtaining early access to information that might otherwise be obtained via disclosure in pending or contemplated litigation is inherently improper.*

In coming to this conclusion Warby J quoted from an early 2012 Court of Appeal case (*Durham County Council & Dunn* [2012] EWCA Civ 1654), in which Kay LJ observed:

> *I do not doubt that a person in the position of the claimant is entitled — before, during or without regard to legal proceedings — to make an access request pursuant to section 7 of the Act. I also understand that such a request prior to the commencement of proceedings may be attractive to prospective claimants and their solicitors. It is significantly less expensive than an application to the court for disclosure before the commencement of proceedings pursuant to CPR r 31.16. Such an access may result in sufficient disclosure to satisfy the prospective claimant's immediate needs. …*

The case shows that data protection is not only a useful remedy in itself, but a tool for claimants in other litigation.

Data breach as a basis for claim

One area of data protection law where organisations are already braced for significant financial consequences is in data security failure (where there is contravention of the 7th Principle). The DPA requires that data controllers take appropriate measures to safeguard personal data from accidental loss or unlawful or unauthorised access. Even now, the ICO issues six-figure fines where serious harm is likely to result from these breaches (a list of enforcement action the ICO has taken, against both private companies and public authorities, is available on its website). Under the greater powers afforded national authorities under the new Regulation (up to €20 m or 4% of global turnover) such action is only likely to become more draconian.

What might change the game in terms of claims by individuals is the Morrisons data breach, where a group litigation action – reported to number at least 5,000 claimants – is in process after a disgruntled staff member leaked payroll information of tens of thousands of colleagues, potentially exposing them to financial fraud and identity theft. At issue in the case will be issues of vicarious liability (which might derive from a single unlawful act by an employee) as well as the adequacy of Morrisons' data security measures (as s 13 claims require a proven contravention of the DPA, before questions of damage or distress may be considered).

The court's deadline for new claimants to join passed in April 2016, so next steps will be watched with interest: not simply in how the claim will be pleaded, but also whether Morrisons will accept liability and offer compensation. With damages recovery under DPA claims still at the thin end of the wedge, defendants may be tempted to 'low-ball' offers of amends or roll the dice on how the Court will approach this relatively new territory.

Comment

It seems data protection is not merely here to stay in the context of media litigation, but – depending on the Supreme Court decision in *Vidal-Hall*, and the fate of Morrisons – could be ready to take centre stage.

While damages remain low in data protection claims, the same was once true in the context of misuse of private information. As first the *Mosley* case, then the Mirror hacking damages demonstrated, the courts' approach can change over time: and *Vidal-Hall* only emphasises the point. In the meantime, the real significance of a data protection claim for claimants can be in the difficulties it creates for data controllers by way of nuisance value. As both the media bar and the general public see the growing evidence of the power of individual DPA rights, we can expect an upward curve in the use of data protection law: and, it seems, see it put to some novel uses.

Jennifer Agate, Associate, Farrer & Co
Owen O'Rorke, Associate, Farrer & Co