Securing anonymity in breach litigation: the uncertainties

Following the Ashley Madison hack of the summer of 2015, legal action in the US has commenced against the website's parent company Avid Life Media Inc. ('ALM'), with ALM accused of failing to protect user information adequately. A curveball was thrown in the way of such lawsuits however in the shape of a recent Missouri court decision in which the Judge ruled that participants in a class action suit against ALM cannot proceed in the action anonymously. In the UK, Ashley Madison has a significant number of users, who may wish to take similar legal action. In this article, Bryony Hurst of Bird & Bird considers the potential for those affected to take such action while retaining their anonymity.

Most of us have heard the story of the hacking last summer of the extra-marital affairs website, Ashleymadison.com ('AM'). The site's servers were raided by hacktivist group Impact Team and the data of over 30 million users from more than 40 countries was dumped online for the world, including users' nearest and dearest, to peruse - including names, financial information and sexual preferences described in excruciating detail.

In the US, class actions remain commonplace and the legal fallout from this hack is already underway. Civil lawsuits have been filed in various US states against AM's parent company, ALM, for failing to adequately secure user information. Most plaintiffs have sought to protect their identity, bringing claims in the name of John/Jane Doe. However, on 6 April, a ruling was made in one of these suits in St Louis, Missouri (where the US class actions are likely to be consolidated) that putative class representatives may not use pseudonyms. The judge ruled that if they do not use real names they must drop down into the general class and leave their lawyers the unhappy task of finding replacement class representatives willing to be named publicly.

The judge's reasoning was based upon the constitutional principle of openness in court proceedings, which, he noted, could only be overridden where possible injury to the plaintiff exceeded 'mere embarrassment.' He relied upon earlier cases identifying the need for "some social stigma or the threat of physical harm to the plaintiffs." Whilst the judge held that this threshold had been met, he was swayed by the fact that putative class representatives owe obligations to fairly represent the class and must disclose their identities "so that the public, including the putative class members they seek to represent, know who is guiding and directing the litigation."

This is not likely to spell the end of the road for US class actions against ALM; with sufficient due diligence, plaintiffs with nothing left to lose by being named will probably be found. Ironically, in Canada, where class actions can be brought using pseudonyms, a plaintiff (widower Eliot Shore) is willing to be named and is acting as class representative for all affected Canadians. However, the Missouri decision certainly throws a curveball at the claimant lawyers and slows down the litigation.

AM had 1.2 million users in the UK and claimant law firms are considering group litigation here. We know of the protection afforded by our courts to the mystery celebrity known as 'PJS' in the latest super-injunction case involving private sexual encounters and infidelity, but would they be willing to extend the same courtesy to a larger number of litigants, desperate to avoid becoming celebrities as a result of suing ALM?

For those wondering whether such a claim would even be viable in the UK, increases in in-group litigation following data breaches are anticipated. The Court of Appeal's recent decision in *Vidal-Hall v. Google* confirmed two valuable principles for potential AM claimants; that proceedings can be served upon a non UK-based entity (ALM is Toronto-based) for misuse of private information and data protection claims and also that damages are available under the UK Data Protection Act where only distress has been suffered (not pecuniary loss). Whilst former AM users may now be facing expensive divorce proceedings (or, at least, invoices for replacing tyres/clothes/body parts attacked by aggrieved other halves), the fact that UK law now recognises that the sheer embarrassment of being linked to the hacked site is potentially compensation-worthy makes the task of demonstrating loss easier. The recently adopted EU General Data Protection Regulation will also provide for damages for distress once in force; consequently claimant lawyers and litigation insurers are preparing to enter a new legal battleground following high-profile data breach incidents.

What then might still deter potential claimants from pursuing ALM in our courts? On a relatively small island where media outlets have a history of hounding individuals accused of falling below the general moral standard, the ability of potential claimants to protect their identity in court proceedings is likely to be of great

significance in the UK.

Under our Civil Procedure Rules, the starting principle is that parties should be named in orders and judgments and court hearings are open to the public. The public/media can access and publish details of court cases/records. This stems from the principle of open justice, a public interest in transparency in the way in which the courts administer justice. This principle has been protected for centuries; however, in more recent history there has been a creeping recognition that it should sometimes be overridden.

In the case of *Scott v. Scott*, a case involving a woman filing for the nullity of her marriage due to her husband's impotence and an order that the hearings be *in camera* (private), this was discussed. Whilst Ashleymadison.com may well have provided a far neater solution to Mrs Scott's problem, alas for her these proceedings took place in 1913. Despite this, it remains a leading case on the subject with the Court recognising that in certain circumstances "it may well be that justice could not be done at all if it had to be done in public." Nevertheless, and unfortunately for Mr Scott, the Court held that the judge could not order *in camera* hearings and noted that "in the darkness of secrecy, sinister interest and evil in every shape have full swing." The mind boggles at what that Court might have made of the activities in full swing on AshleyMadison.com, but one can surmise from the Court's comments that it would not have been sympathetic to the claimants' plight.

How, though, would a court of 2016 differ in its approach? Today, national courts must act (at least for the time remaining up to the Brexit referendum) in accordance with the rights laid down in the European Convention of Human Rights. This includes a right to private and family life under Article 8, but also a right to freedom of expression under Article 10. Anonymity orders/other privacy measures are available and, as the celebrity super-injunction debate rages on, it appears that the judicial psyche relating to protection of private matters has, in some cases, evolved considerably from the days of *Scott v. Scott*.

Interesting questions might arise in the case of Ashley Madison claimants - should they receive less protection since their claims have arisen as a result of their straying beyond normal moral bounds?

CPR 39.2 formally confers powers on the court to order that hearings should be private, that the identity of parties should not be disclosed, and (under CPR 5.4C) that restrictions on inspection of the court file should be imposed. These powers are exercisable by a Master of the Court and can be invoked prior to issuing a claim form by anonymous application; in practice a confidential schedule containing the applicant's name is included in the application and placed on the court file with strict instructions that it should not be opened without the Court's permission.

The application requires the Court to consider whether the restriction requested is both necessary and proportionate. In order to do so, submissions from the parties will be considered. Once an order has been granted, it is possible for a party claiming an interest in open justice to apply for the order to be discharged; the press, for example, may argue there is public interest in knowing the identity of the parties, or in being able to follow the conduct of the proceedings.

The court's decision requires a balancing act between competing rights of affected parties; no right has precedence and the decision is fact-dependent. Interesting questions might arise in the case of AM claimants - should they receive less protection since their claims have arisen as a result of their straying beyond normal moral bounds? What of the right to privacy of their partners/children?

Although the court has not yet heard this type of application in data breach group litigation, we can glean influential factors from other cases. In favour of anonymity/other restrictions these include:

- Impact upon the claimant's private life - in suspected terrorist cases, courts have scrutinised the likelihood of identification having a serious effect upon reputation, and relationship with family and friends and, in certain cases, the local community.
- Impact upon family's private life - this can be more persuasive than the impact upon the claimant himself/herself if evidence of serious impact can be shown, particularly upon children; in the *PJS* case, the court even recognised the future impact upon the applicant's children (who are currently too young to be affected by the threatened publication).
- Risk of abuse/violence - the court has refused to identify suspected terrorists if there is a real risk that identification could lead to the suspect or his/her family suffering abuse or physical violence, or could provoke outbreaks of public disorder. Courts have also ordered anonymity if identification could prevent the police/officials from carrying out their duties.
- Vulnerable individuals - where children or protected persons are involved and court approval of dispute settlements are required, courts have recognised that anonymity should be the default position, to protect vulnerable individuals from harassment which they would not withstand as well as others. Courts have also taken account of the risk of injustice/discrimination that could be caused if identification deterred

claimants from pursuing legal remedies that would be available to others.

Balanced against this, the court will consider:

- Public interest - courts recognise the public interest in understanding the courts' workings and adopt measures necessary to enable this. They sometimes focus on the relative importance of allowing publication of more details of a case, but on an anonymous basis, versus naming the claimant but restricting publication of details. Their tendency is towards ordering the former; see, for example, the Court of Appeal in *JIH v. News Group Newspapers*. For AM claimants, the argument would need to be made that no public interest lies in knowing their identity; in light of Lord Neuberger's comments in the *PJS* case ("there is no public interest in kiss and tell stories"), they could also try to seal details of their claims; however, this seems unlikely to succeed - public interest resides in enabling people to understand the case brought against ALM, which necessarily involves details of the information hacked and loss suffered.
- Public domain - the very complaint brought by AM claimants is publication of their identities. Having already been 'outed' online and in newspapers, a further argument that could work against the claimants is that nothing private is left to protect and anonymity/other measures would serve no useful purpose. The court's view on this will depend upon the extent to which it determines the private information has already become known; the question of whether the information has become 'generally accessible' is relevant (including repeated publication, where and how widely) and what care was taken by the claimant to keep it out of the public domain. This may prove a real hurdle for certain claimants; if they have already been the subject of press reports following the hack, their identity may no longer be deemed private.

Factors unlikely to be taken into account include:

- Moral standard of the claimants' behaviour - in *PJS* the Supreme Court stated, "criticism of supposed infidelity is not the guide under which the media can disclose kiss and tell stories of no public interest in a legal sense." Whilst this was stated in the context of an injunction application, it provides a useful insight into judges' approach to dealing with private conduct that may dip below the general moral standard.
- The role of class representatives (as in the Missouri case) - in the UK, US-style class actions, on an opt-out basis with class representatives, are not available in the civil courts. Individual claimants must file their own claims, and then a group litigation order can be applied for, which essentially allows the Court to bundle together claims and manage them together. Whilst individuals may, as a tactic, be selected as 'test cases,' the role of class representative does not have the same significance as in the US.
- Consent/agreement of parties - even if ALM was to agree to measures to protect claimants, the Court in *JIH* made clear that this was not a determinative factor and that it had an independent duty to the public to determine the best way to conduct the proceedings.

In summary, whilst it is never possible to predict with certainty how the UK courts will treat issues of privacy, in the current climate AM claimants should have grounds for optimism. A range of measures exist to keep proceedings private, and the courts are well-used to ordering these. As a second line of defence, injunctions imposing reporting restrictions upon particular parties or the press are available where publication of private material is threatened. However, the greater battle for anonymous claimants in such circumstances may lie in achieving compliance with such injunctions; whether they can, in the era of global online (and social) media, ever be effectively enforced is another question.

Bryony Hurst Senior Associate
Bird & Bird, London
bryony.hurst@twobirds.com