Keeping control of personal information in the digital age: efficacy and equivalence of tortious and GDPR/DPA remedial relief?

Fiona Brimblecombe, Helen Fenwick

Subject
Privacy

Keywords:
Privacy online; right to erasure, Article 17 GDPR; misuse of private information; injunctions; monetary remedies

Legislation cited:
General Data Protection Regulation 2016; Data Protection Acts 1998, 2018; Data Protection Directive 1995; Human Rights Act 1998; Articles 8 and 10 ECHR; Electronic Commerce Directive 2000; Electronic Commerce Regulations 2002

I. Introduction

A global recognition of the threat to the protection of private information online, coming in particular from the big "tech" companies, is currently increasingly apparent.[1] The same concerns, this article will argue, are driving significant legislative changes and recent and emerging jurisprudence determining the reach of both the tort of misuse of private information in England and Wales and data protection. To illustrate these points, this article identifies three key areas in which private information is under coming threat in the digital era, and the reforms in response being brought about legislatively and judicially to the contours of the applicable privacy-protective framework formed by both causes of action. In the first, the more traditional concerns of both the tort and data protection are engaged when private information is published without consent online, by private posters on privately-

[1] E.g. India is following the GDPR model in introducing the Personal Data Protection Bill 2019. See further D. Erdos "The 'Right to be Forgotten' beyond the EU: an analysis of wider G20 regulatory action and potential next steps" [2021] *Journal of Media Law*: https://doi.org/10.1080/17577632.2021.1884947.

owned web-sites or on social media platforms, sometimes anonymously or from outside the jurisdiction, where the platform has merely acted as a passive host.[2] In the second an intermediary enables any interested individual to access private information about an individual (and/or further threatened disclosures are likely) in breach of one or both causes of action, and the potential breaches are brought to its attention.[3] In the third, browser-generated information is collected by an online intermediary without consent to disclose for commercial gain.[4] The term "intermediary" will be used in a limited fashion in this article to cover social media platforms and search engines, and the focus will largely be on those owned by the global tech companies. As far as intermediaries are concerned, the second and third situations reach beyond the privacy concerns traditionally associated with mass media activity. The three reflect a spectrum, capturing passive engagement with the information to a more active engagement, including harvesting it for disclosure to third parties.

Remedial relief was already available under both the tort and data protection[5] to those seeking redress for unconsented-to disclosures of private information, but those causes of action are currently undergoing a transformation to meet the challenges posed by those three forms of misuse of private information. Data protection is entering a new and enhanced iteration in the form of the General Data Protection Regulation 2016 (GDPR), applicable domestically as retained law after Brexit – the "UK GDPR",[6] and reflected in the Data Protection Act 2018 (DPA). Judicial recognition of threats posed by the reach and activity of the tech companies in interacting with private information is also becoming apparent as recent and current claims arise in situations far removed from those envisaged at the inception of both the previous data protection regime and the tort. Those recent developments to be discussed have tended to adopt an expansive stance towards privacy protection, with a view to reining in the power of the tech companies to invade online privacy, as given

[2] As in: *ZXC v Bloomberg LP* [2020] EWCA Civ 611; [2021] Q.B. 28; *JQL v NTP* [2020] EWHC 1349 (Q.B.).
[3] As in *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2018] EWHC 799 (Q.B.); [2019] Q.B. 344.
[4] The situations in: *Google v Judith Vidal-Hall* [2015] EWCA Civ 311; [2016] Q.B. 1003; *Lloyd v Google LLC* [2019] EWCA Civ 1599; [2020] Q.B. 747; *SMO (a child) by their litigation friend Anne Longfield (Children's Commissioner) v TikTok Inc and others* [2020] EWHC 3589 (Q.B.) (concerning children's browsing data, and regarding anonymity only).
[5] Under the Data Protection Act (DPA) 1998, reflecting the Data Protection Directive 1995 (Directive 95/46/EC).
[6] Regulation (EU) 2016/679, [2016] O.J.L.119/1 (04.05.2016). Under the European Union (Withdrawal) Act 2018 the GDPR forms part of EU law retained as domestic law following the end of the post-Brexit transition period: 31.12.20, now being referred to as the "UK GDPR". The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419 provide the key statutory instrument for modifications to the UK GDPR/DPA 2018.

expression in one of the key stated objectives underlying the GDPR, in Recital 6.[7] That stance was also typified by the approach of the Court of Appeal in *Lloyd v Google LLC*[8] in relation to collection of browser-generated information, which found: "The actions in tort for MPI and breach of the DPA both protect the individual's fundamental right to privacy; although they have different derivations, they are, in effect, two parts of the same European privacy protection regime".[9] The Court went on to find, based on the EU principles of equivalence and efficacy, that remedies under relevant EU law – in that instance, under data protection - should be enhanced to be no less favourable to claimants seeking to protect the fundamental right of respect for private information, than remedies aimed at the same objective under the tort of misuse of private information.[10]

The fundamental question this article is asking is whether the privacy-protective scheme created by these two causes of action, often put forward in the same claim,[11] is now becoming more effective in terms of providing remedial relief, bearing in mind that remedies under the tort were largely designed with the traditional media in mind.[12] The role of one of the key remedies under the GDPR, the "right to be forgotten" under art. 17, reflected in s.100 DPA, will in particular be looked at alongside the role of injunctions under the tort, in order to consider their efficacy in the online context, their equivalence, and to question whether their roles need to be viewed as entirely distinct. Adopting a radical stance in the face of threats to privacy online, the courts, as will be discussed, have had to overcome, or are in the process of overcoming, a range of barriers to finding remedies under the tort and data protection. While recent decisions regarding data protection were reached under the previous regime, they will also influence the jurisprudence about to arise under the UK GDPR and DPA 2018. As will be argued, the courts appear to be prepared to reject or modify traditional understandings as to the ambit or reach of remedies under both causes of action in order to provide relief for privacy invasion in the three online contexts identified.

---

[7] "Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows…private companies…to make use of personal data on an unprecedented scale…".
[8] [2020] Q.B. 747.
[9] At [53].
[10] *Lloyd v Google LLC* [2020] Q.B. 747 at [52].
[11] See: *ZXC v Bloomberg LP* [2019] EWHC 970 (Q.B.); [2019] E.M.L.R 20 both at [3]: the claimant accepted that if he could not succeed with the misuse of private information claim, he would not succeed in the DPA claim. See also *Google v Judith Vidal-Hall* [2016] Q.B. 1003 (first instance: [2014] EWHC 13 (Q.B.); [2014] E.M.L.R. 14).
[12] See J. Rowbottom, "A landmark at a turning point: Campbell and the use of privacy law to constrain media power" (2015) 7(2) *Journal of Media Law* 170 at 187.

II. Widening the net of remedial privacy-protection and enhancing the value of damages/compensation as a remedy for misuse of private information online

1. Intermediaries as data controllers/tort-feasors; loss of their "shield"?

Clearly, if remedies were to be provided in relation to forms of online privacy invasion, it was necessary to find that search engines and social media platforms could fall within the definition of data controllers, now arising under art. 4(7) GDPR, and could also be sued in tort when they misuse private information in the ways set out in categories two and three above. Facebook has been found to be a data controller in a number of decisions taken under the previous data protection regime,[13] as has Google.[14] In, for example, *Townsend v Google Inc. & Google UK Ltd*[15] the plaintiff made a request for Google to de-list seven of the twelve previously notified U.R.L.s because they indicated that he was a sex offender. The claim failed under both the tort and DPA 1998, but not on the basis that Google was not a data controller or tort-feasor.

It has further recently been found that the protection for intermediaries available under the e-commerce Directive[16] implemented in the Electronic Commerce (E.C. Directive) Regulations 2002, providing the so-called intermediary "shield", may not apply to relieve them of obligations to provide compensation for privacy-invasion under either the tort[17] or data

[13] See: Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] (ECJ) ECLI:EU:C:2018:388 (under the old regime, but the definition of a data controller has remained the same); *J20 v Facebook Ireland* (2016) N.I.Q.B. 98; in *CG v Facebook Ireland Limited and McCloskey (Joseph)* [2016] N.I.C.A. 54; N.I. 21 Facebook conceded that it was a controller, so the point was not subjected to legal argument.

[14] See: Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* EU:C:2014:317 [34]; [2014] Q.B. 1022 both at [34]; *Mosley v Google* [2015] EWHC 59 (Q.B.); [2015] C.M.L.R. 22; *Case C-136/17 GC, AF, BH, ED v Commission nationale de l'informatique et de Libertes (CNIL), Premier ministre, Google LLC* ECLI:EU:C:2019:773. See further O. Lynskey "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costjea Gonzalez" (2015) 78(3) M.L.R. 522 at 522-534.

[15] [2017] N.I.Q.B. 81; [2020] N.I. 120.

[16] Directive 2000/31/EC.

[17] See e.g., *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2019] Q.B. 344 where Google had notice, although no award was made under either action because Google had not failed to take reasonable care to comply with the legal requirements under either cause of action, at [228],[227],[230]. But note: a much narrower defence would now apply under the UK GDPR (art. 82(3)) so an award for a breach of data protection would be more likely to arise. In *J20 v Facebook Ireland* (2016) N.I.Q.B. 98 once Facebook had notice in respect of the information posted, found to be private, Facebook was found to be liable under the tort to pay damages since the protection of the e-Commerce Directive no longer applied, at [71],[75].

protection[18] where their role is not merely passive and they have notice as to the claimed unlawful invasion. The "shield" still applies under the 2002 Regulations, although the Directive ceased to apply at the end of December 2020,[19] but is still relevant to cases arising before that date. Articles 12-15 of the Directive set out the limited liability exemptions ('safe harbours' or 'shields') containing the conditions under which certain intermediary service providers falling within art 1(5)(b) are exempted from liability for third party content, where their role is merely passive and they do not have "actual knowledge" of illegal activity or information. Under art. 15 member states may not impose a *general* obligation on service providers to monitor information which they transmit or store. Under art. 14 (reflected in s.19(a)(i) 2002 Regulations) hosting providers are not liable for the information stored at the request of recipients of the service but will lose the benefit of that exemption if, upon obtaining actual knowledge of illegal activity or information, or awareness of facts or circumstances from which such activity/information is apparent, they fail to act expeditiously to remove or disable access to the information.

In *CG v Facebook Ireland Limited and McCloskey (Joseph)*[20] it was found that all the circumstances had to be considered in deciding whether an I.S.P. had actual knowledge of the unlawfulness of the material; Facebook appeared to have such knowledge due to an earlier action; it therefore fell outside the shield under the e-Commerce Directive. On appeal it was found, however, that the shield *would* apply as far as the damages were concerned[21] since the Court disagreed with the judge's conclusion that the earlier litigation - *XY v Facebook*[22] - meant that Facebook had the requisite knowledge, partly on the basis that that litigation had related to harassment rather than the tort.

The relevant decisions arising under the previous data protection regime will influence the current one: the likelihood that an intermediary would be found both to be a controller, and to lose its shield appears as high or higher under the UK GDPR; as de Gregorio argues, the GDPR "has challenged the historical gap between the system of the e-Commerce Directive

[18] See: Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [2014] Q.B. 1022 at [38]; *Mosley v Google* [2015] C.M.L.R. 22; *AY v Facebook* (2016) N.I.Q.B. 76 at [11],[12].
[19] See Department for Digital, Culture, Media & Sport, "The e-Commerce Directive and the UK", (18.1.21).
[20] [2015] N.I.Q.B. 11 at [94],[95],[102].
[21] *CG v Facebook Ireland* [2016] N.I.C.A. 54; [2019] N.I. 21.
[22] [2012] N.I.Q.B. 96 at [52]-[73]; see in particular [63].

and that of the Data Protection Directive",[23] indicating a recognition, influencing the design of the GDPR, that since the inception of the previous Directive, intermediary providers had become more active, offering new services for sharing information via search engines and social media platforms. Erdos finds that the shield would be lost where intermediaries "carry out their activities so independently as to fall outside even a broad construction of the codified host intermediary shield".[24]

2. Compensation for distress and loss of control over personal data/information

The value of informational autonomy has long been recognised under the tort in remedial terms, meaning that it has not been found to be necessary to prove financial loss or an impact on health to attract damages: distress caused by unconsented-to disclosure of personal information is sufficient.[25] More recently, it was found in *Gulati v MGN* that compensation can be awarded under the tort for the misuse of the private information in *itself*.[26] But that was not the case under the DPA 1998 s.13(2), since it appeared that pecuniary loss was needed[27] or processing for "the special purposes". In *Google Inc. v Vidal-Hall and others*,[28] concerning unconsented-to collection of browser-generated information (BGI) with a view to its disclosure, it was found that s.13 DPA, providing for compensation for "damage" suffered by a DPA breach, would only allow damages to be awarded for distress if one of the criteria in s.13(2) was met, and they were not applicable.[29] Therefore the Court of Appeal determined that s.13(2) should be disapplied because it was in conflict with art. 7 (right to private life) and art. 8 (protection of personal data) of the EU Charter of Fundamental Rights, in

[23] See G. De Gregorio, "The E-Commerce Directive and GDPR: Towards Convergence of Legal Regimes in the Algorithmic Society?" (2019) E.U.I. Working Paper R.S.C.A.S. 2019/36, at https://cadmus.eui.eu/bitstream/handle/1814/63044/RSCAS%202019_36.pdf?sequence=1&isAllowed=y, 6.

[24] D. Erdos, "Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU *acquis*" [2018] *International Journal of Law and Information Technology* 189 at 217.

[25] See *Campbell v MGN Ltd* [2004] UKHL 22; [2004] 2 A.C. 457 both at [51].

[26] [2015] EWCA Civ 1291; [2017] Q.B. 149. The appeal from Mr Justice Mann's orders for damages at trial concerning the phone hacking of multiple individuals and the consequent misuse of private information was rejected: at [1],[49] for both citations. He had held that awards did not have to be limited to distress caused by the phone hacking/interception: they could also be awarded since the claimants' privacy had been infringed by the very act of the hacking since their private information had been "misappropriated" at [16], supporting this conclusion by reference to ensuring the effectiveness of art. 8 ECHR and Strasbourg jurisprudence generally at [17].

[27] See *Google v Judith Vidal-Hall* [2016] Q.B. 1003 at [83].

[28] [2016] Q.B. 1003.

[29] At [59]; the claimants did not allege that they had suffered pecuniary loss in addition to distress.

accordance with the requirement of an effective remedy for breach of those rights in art. 47.[30] Therefore it was found that compensation could be awarded for distress without the need to prove financial loss. That finding opened the door to further claims brought in respect of BGI collection, since the loss in question would usually consist largely of distress. It is also possible for a claimant to be awarded additional damages where aggravating features are present, including what can be termed "special dignity harm".[31] Claims for such damages have also been put forward in cases concerning collection of BGI, on the basis that the intermediary was or should have been aware of the collection and failed to act.[32]

A further step was then taken in *Lloyd v Google LLC*:[33] one of the bases on which compensation can be awarded under data protection was found to be loss of control over personal data, without more. Again, the case concerned unconsented-to BGI collection with a view to its disclosure; the claimant successfully relied on *Gulati v MGN*, claiming compensation that would have been available under the tort.[34] The Court of Appeal found: "the characterisation of the class members' loss [was] as the loss of control or loss of autonomy over their personal data".[35] That decision would be likely to be followed under the GDPR/DPA in a similar case, but in any event compensation for such loss appears to be available: Recital 85 lists 'the loss of control over personal data' as an example of damage, while Sir Geoffrey Vos C also noted that s.169(5) DPA 2018, which covers compensation for breaches of data protection other than under the GDPR, is non-exhaustive in listing distress as an example of damage not involving financial loss.[36] It would be anomalous if the basis for awarding monetary compensation in respect of unconsented-to disclosure or threatened disclosure of personal data was found to be narrower under the GDPR. The basis for awarding such compensation under data protection thus appears to be incrementally aligning itself with the tort basis: data protection is therefore discarding the constraints rendering its

[30] [2016] Q.B. 1003, at [105], applying *Benkharbouche v Embassy of the Republic of Sudan* [2015] EWCA Civ 33; [2016] Q.B. 347. See now DPA 2018, Part 6, s.168, "Compensation for Contravention of the GDPR", including both material and non-material damage.

[31] See *Max Mosley v News Group Newspapers Limited* [2008] EWHC 1777 (Q.B.); [2008] E.M.L.R 20. Mr Justice Eady found: "damages…may include distress….[extreme] loss of dignity," striking at his core personality, at [216] for both. C. Hunt notes that the ECtHR has not found that awarding aggravated damages is likely to lead to an art. 10 breach: "Strasbourg on Privacy Injunctions" (2011) 70(3) C.L.J. 489 at 491; see *Mosley v UK* App. No. 48009/08 (ECHR, 10 May 2011).

[32] See *Google v Judith Vidal-Hall* [2016] Q.B. 1003: "aggravated damages [are claimed since]….the defendant ought to have been aware of the operation of the Safari workaround [the means of collecting the BGI] during the [relevant] period…or was aware of it and chose to do nothing", at [5].

[33] [2020] Q.B. 747.

[34] [2017] Q.B. 149.

[35] [45].

[36] *Gulati v MGN* [2017] Q.B 149 at [65].

remedial regime inapplicable to a number of threats to privacy online, and they may be entirely discarded once cases arise under the UK GDPR.

3. Traditional inadequacies of compensation in protecting private information

Although the developments discussed have brought data protection more closely into line with protection for informational autonomy, the use of monetary compensation in this context has traditionally demonstrated clear inadequacies. Judges have persistently argued in the tort context that compensation provides an insufficient remedy for misuse of private information; the same argument would now clearly apply under the GDPR art. 82 right to compensation. *Post-facto* monetary compensation largely fails to address the harm done by the form of misuse of personal information under discussion; it is awarded for injury to feelings or loss of control of information without being able to remedy the injury in any meaningful fashion, although it may have some symbolic affirmatory effect: at the least recognition has occurred that a wrong has been done. Mosley received an award that was significantly higher than those in previous cases,[37] even though punitive/exemplary damages were not available, but Mr Justice Eady recognised that the sum still failed to provide redress for privacy invasion as opposed to reputational damage, finding "…reputation can be vindicated by an award of damages…[since]…the claimant can be restored to the esteem…he was previously held in …that is impossible where embarrassing personal information has been released for general publication…".[38] Strasbourg has, however, found that monetary compensation provides an adequate domestic remedy for violations of art. 8 rights arising from the unconsented-to press publication of private information, in *Mosley v UK*,[39] although its findings indicated that it was largely seeking to refrain from delving into the precise arrangements for providing domestic redress where the only alternative would be the award of an injunction, reflecting an aspect of subsidiarity.

The fear of further privacy-invasion exacerbates the problem of the lack of alignment between loss of privacy and the award of monetary compensation: many claimants may decide not to pursue an action under the GDPR/DPA or the tort if the data has (fully or partly) already been made public since they do not want to prolong the pain and the possible

[37] *Max Mosley v News Group Newspapers Limited* [2008] E.M.L.R 20 at [236] (para no relates to neutral citation at n 31).
[38] At [230]-[231].
[39] App. No. 48009/08 (ECHR, 10 May 2011) at [120].

negative publicity created originally by the disclosure.[40] In some circumstances, however, a summary judgment can be given,[41] avoiding a full trial of the action and at least bringing a degree of closure in terms of prolonged privacy-invasion, as occurred in *Duchess of Sussex v Associated Newspapers* in which the information had already been published;[42] given that her privacy case in respect of her letter published without consent was found to be so strong, a summary judgment was found to be warranted.[43]

Despite the failures of compensation in addressing harm flowing from misuse of private information, it is still accepted under both data protection and the tort that it has the capacity to provide some redress in respect of such misuse, as part of a struggle to do justice to claimants affected by privacy invasion, and also possibly to create deterrence. But as far as the mass media, online news' sites or private posters misusing private information via publication are concerned, any deterrent effect would be unlikely to flow from the relatively low levels of damages, often below £20,000, that have been awarded in tort cases,[44] a matter that has raised judicial concern.[45] Even the relatively high award in the recent *Cliff Richard* case (which included aggravated damages),[46] representing the upper echelons of what a claimant could currently expect to receive in a successful tort claim, might have little deterrent effect, given the counter-balancing financial incentives and the availability of liability insurance. In *Mosley* the judge also ordered that Mosley's substantial legal fees should be paid by the respondents,[47] but while such an award could have a deterrent effect as far as the mainstream media is concerned, publishers might decide to take the risks, both of losing the action and of paying the other side's fees, given the commercial value of selling

[40] Litigious claimants like Max Mosley are rare: C. Hunt "Strasbourg on Privacy Injunctions" (2011) 70(3) C.L.J. 489 at 490.
[41] C.P.R. 3.4(2)(a) allows the court to strike out a Defence, or part of one, while C.P.R. 24.2 allows the court to give summary judgment against a defendant on the whole of a claim, or on a particular issue.
[42] [2021] EWHC 273 (Ch.); [2021] 3 All E.R. 1163. See also *BVG v LAR* No 2 [2020] EWHC 931 (Q.B.); No 1: [2019] EWHC 2388; the claimant was also granted summary judgment on his misuse of private information claim.
[43] It was found that it would be "fanciful" to imagine that a reasonable expectation of privacy would not be established, [95]; the balancing free expression claim was also readily dismissed, at [128].
[44] In e.g. *Campbell v MGN Ltd* [2004] 2 A.C. 457 the award was £2,500; in *Douglas v Hello! Ltd (No.2)* [2003] E.M.L.R. 585, £14,600; in *McKennitt v Ash* [2006] EWCA Civ 1714; [2008] Q.B. 73, £5,000.
[45] In *Spelman v Express Newspapers* [2012] EWHC 355 (Q.B.) Tugendhat J found: "If a remedy in damages is to be an effective remedy, then the amount…[awarded] must not be subject to too severe a limitation", at [114].
[46] Richard was awarded £210,000 in damages, in part due to the presence of aggravated damages: *Cliff Richard v BBC* [2018] EWHC 1837 (H.C.); [2019] Ch. 169, both at [365], aggravated since the BBC had sought to win "scoop of the year". The award overall was deemed justified *inter alia* due to the degree of intrusion and distress engendered, at [350]-[357]. Special damages were also awarded: [370]-[428]. In the claims (involving phone-hacking) in *Gulati v MGN Ltd* [2017] Q.B. 149 the awards ranged from £72,500-£260,250.
[47] *Max Mosley v News Group Newspapers Limited* [2008] E.M.L.R 20, amounting to £850,000.

the information in question, and a costs-award would also usually be covered by liability insurance.

The fact that publication has occurred online may be having some, albeit inconsistent, impact on the level of awards. In *ZXC v Bloomberg LP*[48] only £25,000 was awarded in relation to the misuse of private information that was found to have occurred, due to publication of details as to a criminal investigation into the claimant online by a media organisation. The low award, which was, however, combined with an injunction preventing further publication, was deemed sufficient, possibly partly because dissemination of the information was fairly limited, although the judge found that "the claimant has been caused significant distress and anger by…publication of the information…it has negatively impacted his dignity and standing…[But]…not…his health".[49] But in *Sicri v Associated Newspapers,*[50] which also concerned information linked to a possible prosecution, £83,000 was awarded in damages under the tort, although £33,000 were for financial loss. He had been arrested in connection with the Manchester terrorist attack, and his arrest, eventually with identifying details, was publicised in the MailOnline; this information was not removed for some time when he was released without charge; it then received a lot of publicity, including on social media. There is also some evidence that awards in relation to online publication are rising, even where dissemination is limited. In *JQL v NTP*[51] a woman brought a claim against her uncle in respect of a Facebook post revealing information about her mental health; it was only available for about 3 hours, and viewed by only about 35 people. Nevertheless, Mr Justice Lewis awarded her £15,000 damages for a malicious invasion of privacy.

4. Re-envisaging monetary awards as a real deterrent to the tech companies; class claims?

Public law monetary sanctions that can be administered under the GDPR far exceed damages as typically awarded under the tort. The GDPR provides for fines equivalent to either 20 million Euros or 4% of turnover, according to art. 83(5)(a) and (b) where a right to erasure under art. 17 is wrongfully refused by a data controller. Similar levels of fine are also

[48] [2019] [2019] E.M.L.R 20. The finding that the privacy claim should succeed was unsuccessfully appealed in *ZXC v Bloomberg L.P.* [2021] Q.B. 28, leaving the findings as to quantum of damages undisturbed.
[49] At [155].
[50] [2020] EWHC 3541(Q.B.).
[51] [2020] EWHC 1349 (Q.B.). In *In WXY v Gewanter* [2013] EWHC 589 (Q.B.); [2013] Info. T.L.R. 281: the claimant was awarded £24,950 damages after the defendants published allegations regarding her sexual conduct and details of her private discussions online.

available for breaches of the data protection principles.[52] Clearly, that terminology was not included with ordinary online posters or small non-media blogs/sites in mind; fines awarded where such actors have disclosed private information without consent would be far lower: turnover would normally, not always, be irrelevant: posters on established platforms such as YouTube show high levels of profit due to advertising revenue. In general, such punitive sanctions clearly create the potential for deterrence.

The role of *compensation* available to the claimant under either cause of action is not, however, seen as one of deterrence. The possibility of suing the intermediary hosting or providing access to the private information has recently been accepted in the courts,[53] but the damages awarded have been undisclosed or comparable to those awarded traditionally in the mass media cases.[54] At present it seems probable that this situation will not change under the GDPR art. 82 where claims for compensation are brought against *individual* posters of private information and/or the intermediary hosting the information. It may be unlikely that a judge would favour awarding a higher level of compensation to a claimant under the GDPR/DPA than would have been awarded on the same facts under the tort, bearing in mind the number of recent cases in which the claim has been brought under both causes of action under the previous data protection regime.[55]

But the situation may differ where, rather than hosting private information, the intermediary has actively collected such information to disclose for gain, or provided the means whereby it can be disclosed. *Google v Judith Vidal-Hall*[56] was found to concern a misuse of private information under the tort because the defendant had collected such information about the claimants' internet usage via their Apple Safari browser; it therefore concerned an instance of *potential* disclosure of private information. It was the "subsequent use of that information", the BGI, which was found to bring the situation within the area of tortious liability, leading to

[52] Under art. 83(5)(a) GDPR for: breaches of the principles in art. 5; unlawful data processing (art. 6); breaching conditions for consent to processing (art. 7); processing of "special category data" has occurred unlawfully (art. 9). Non-compliance with an order to limit data processing or flow is covered: art. 83(5)(e).

[53] E.g. Facebook was successfully sued in 2018 when naked images of the teenage claimant were posted on Facebook. She sought damages before Mr Justice Maguire in the Belfast High Court for misuse of private information and breach of the DPA; the claim was settled, confidentially, by Facebook: https://www.irishtimes.com/news/crime-and-law/courts/high-court/girl-14-settles-landmark-action-against-facebook-over-naked-images-1.3349974. See also: *Mosley v Google* [2015] EWHC 59 (Q.B.); [2015] C.M.L.R. 22; *CG v Facebook Ireland Limited and McCloskey (Joseph)* [2015] N.I.Q.B. 11.

[54] See e.g. *J20 v Facebook Ireland* N.I.Q.B. 98; the claimant was awarded damages (£3,000) due to breach of the tort and injury to feelings.

[55] See *ZXC v Bloomberg LP* [2019] E.M.L.R 20 [3].

[56] [2016] Q.B. 1003 at [3],[1052].

the settlement.[57] The levels of compensation available under the GDPR *would* potentially be able to create a deterrent in those circumstances, but in that instance it seemed to be assumed that the levels of compensation that could be awarded under data protection would be quite modest and comparable to the awards under the tort.[58]

But the position in relation to claims brought against the large tech companies whose platforms collect private information from multiple users for disclosure for gain could be about to change dramatically: very significantly, the Court of Appeal in *Lloyd v Google LLC*,[59] concerning the collection of BGI without consent by Google, involving millions of users, opened the way under data protection to class claims. Lloyd had issued a claim for breach of statutory duty under DPA 1998 s.4(4) (the requirement of a data controller to abide by the Data Protection Principles). He alleged that Google, in its capacity as a data controller, had failed to comply with Principles 1, 2 and 7 in Part 1, Sch. 1 DPA, now retained in the GDPR art. 5 (processing that is fair and lawful; data was only obtained for specific and lawful purposes; appropriate technical and organisational measures were taken against unauthorised or unlawful processing of personal data, respectively). The Court found that the data subjects were entitled to recover damages pursuant to s.13 DPA, as discussed above, based solely on the loss of control of their personal data,[60] and the data subjects represented in the claim were found to have the same interest for the purposes of C.P.R. 19.6; it also exercised its discretion under C.P.R. Part 19.6(2) to allow the representative claim to proceed.[61] Depending on the decision of the Supreme Court, Lloyd can therefore take the claim to trial: this decision would allow him to serve proceedings out of the jurisdiction and gives some encouragement, if successful, to quasi-class claims of this nature which would attract compensation running into millions. A further similar claim is reportedly currently being launched against Facebook: in *Facebook You Owe Us v Facebook UK* the claimant

[57] The claim was then settled: see Andrew Dunlop, "Damages for distressed data subjects: Google withdraws its appeal" (*Burges Salmon*, 21 July 2016) at https://www.burges-salmon.com/news-and-insight/legal-updates/damages-for-distressed-data-subjects-google-withdraws-its-appeal/.

[58] See *Google v Judith Vidal-Hall* [2016] Q.B. 1003: "It is accurate…[to find that] compensatory damages may be relatively modest (as they often are in claims for misuse of private information and breaches of the DPA)", at [139].

[59] [2020] Q.B. 747.

[60] It had been questioned whether "damage" had been suffered according to DPA 1998 s.13 and art. 23(1) Directive 95/46/EC to warrant compensation.

[61] See s.13 of the judgment: he made the claim on behalf of a class of more than 4 million Apple iPhone users, alleging that "Google secretly tracked some of their internet activity for commercial purposes…" at [1]. The Supreme Court heard the claim in April 2021; judgment is awaiting publication: UKSC 2019/0213.

group[62] is claiming that Facebook had allowed data to be collected in 2013-2014 and transferred to Cambridge Analytica without consent and without informing the data subjects, in violation of the first, second, fifth, sixth, seventh and eighth data protection principles of the DPA 1998. The group have stated that the data breach potentially affected one million UK users and 87 million worldwide.

This new possibility of allowing class claims against intermediaries clearly now offers the prospect of using compensation to create an effective privacy remedy, but only in BGI cases. Class claims have not yet been accepted under the tort, but the possibility of relying on an account of profits as well as damages was considered in *Google v Judith Vidal-Hall*;[63] so doing could clearly have deterrent value, given the very large profits, running into millions, that can be made from exploiting BGI,[64] the third instance of loss of control of private information from the Introduction. Received wisdom therefore to the effect that compensation is an inferior remedy in respect of misuse of private information may now need to be re-visited in the intermediary context, where it is an *active* participant in privacy-invasion, given the new potentialities for awarding much higher levels of compensation that are currently on the horizon.

III. The roles of injunctive relief and the "right to be forgotten" in the digital era

1. Introduction

Below, the roles performed by art. 17 GDPR and by injunctions are compared in recent cases concerning online privacy, in order to consider whether a more creative approach to their potentialities could be adopted, which also questions the distinctiveness of their roles. The remedy under data protection playing a role most closely equivalent to that of injunctions is the right "to be forgotten" under art. 17, which is generally seen, as far as publication, not storage, is concerned, as an *ex post facto* remedy only, and therefore as playing a role distinct

[62] See: https://www.lexology.com/pro/content/cambridge-analytica-class-action-filed-in-the-uk (*Lexology*, 2 November 2020). The data breach relates to a Facebook personality-quiz app, allowing access to information on millions of people beyond those downloading it. The Information Commissioner's Office has already issued a £500,000 fine against Facebook for the Cambridge Analytica data breach.

[63] [2016] Q.B. 1003.

[64] "The Defendant's misuse of the Claimants' Private Information…[means] the Defendant has made a substantial profit….for which the Claimants seek an account", at [21, Appendix] "…the Defendant makes an annual profit of billions of dollars from the DoubleClick service…[which]…provides subscribing advertisers with a service called AdSense…subscribing advertisers provide AdSense with browsing information received…due to use of the DoubleClick ID Cookie relating to…individual browsers visiting their websites", at [6.1]-[6.2].

from that of an injunction. It has been assumed that injunctions are not available under the GDPR/DPA, but it will be contended below that that assumption could be challenged judicially, in the sense that art. 17 could be interpreted flexibly to perform a role similar to that of an injunction, to ensure its own efficacy and to create equivalence of remedial relief as between the tort and data protection. Equally, it will be argued that in relation to the online situations with which this article is concerned, the award of an injunction can play a role cognate with that of the right to erasure. Most importantly, it will be argued that recently the reach of injunctions has broadened in a range of highly significant respects, meaning that *both* remedies can be deployed against intermediaries in order to protect private information, thereby overcoming some of the most concerning threats to such information in the digital era. Further, their "shield" under the e-commerce Directive, as discussed above, will not apply once they have notice that an injunction or erasure is being sought,[65] while the 2002 Regulations only apply to pecuniary remedies, and allow for other relief under s.20.

2. Diminution in the value of injunctions as traditionally envisaged in the digital age?

The availability of injunctions as a remedy under the tort is well established.[66] Received wisdom among judges and privacy lawyers finds that injunctions rather than damages/compensation provide the remedy with the greatest capacity to preserve informational autonomy,[67] and that notion was firmly reiterated recently, in the traditional context of misusing private information by publishing it without consent.[68] The dispute has traditionally been between the media party which wishes to secure the often-transient newsworthy nature of the information, and the claimant, who wants to preserve its private nature by seeking interim relief to ensure that the information in question does not enter the public domain,[69] since if it does a final trial of the action would be rendered almost otiose.[70]

---

[65] See *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2019] Q.B. 344 in relation to de-listing.

[66] See: *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] UKSC 26; [2016] A.C. 1081; *Ntuli v Donald* [2010] EWCA 1276; [2011] E.M.L.R. 10.

[67] See: *PJS*, at [41],[43]; *Douglas v Hello! Ltd (No.3)* [2005] EWCA Civ 595; [2006] Q.B. 125 at [257]-[259]; R. Wacks, *Privacy and Media Freedom* (Oxford: OUP, 2013), p.21; H. Fenwick and G. Phillipson, *Media Freedom Under the Human Rights Act* (Oxford: OUP, 2006), pp.662-666; A.F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), pp.34-35.

[68] See *ZXC v Bloomberg LP* [2019] E.M.L.R 20 "Although the ECtHR has held that damages are capable of being an effective remedy in art. 8 claims (*Mosley v UK* App. No. 48009/08 (ECHR, 10 May 2011); EMLR 1 [120]), this does not displace the recognition in domestic law that damages in misuse of private information claims are unlikely to be an adequate remedy," at [137].

[69] See: *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] A.C. 1081; *Ntuli v Donald* [2011] E.M.L.R. 10 at [48]. See *ZXC* [2019]: "the practical reality in privacy cases [is] frequently, the fate of the interim injunction application determines the whole claim", at [137].

The s.12(3) Human Rights Act (HRA) legal framework for awarding interim injunctions[71] was not only devised with those mass media considerations in mind, but also with the intention of affording the media greater protection than appeared to have been available under the pre-HRA test.[72] The wording of s.12(3), providing that publication can be restrained before trial *only* if the "applicant is likely to establish that publication should not be allowed",[73] obviously presupposes that something identifiable as a "publication" could occur – but *enabling* disclosure in the public domain via social media has now been found to be covered.[74] If, however, an injunction was sought in respect of the collection of browser-generated information by a social media platform or search engine with a view to its disclosure to other controllers for private commercial gain, it appears unlikely that s.12(3) could be found to apply,[75] since "publication" has not occurred.

Clearly, contentions as to the value of injunctions rely on finding that they are effective in practice, and their efficacy has obviously been placed under strain recently due to the rise in the dissemination of private information online,[76] and also for the practical reasons discussed below. The problem is that injunctions are aimed at providing the privacy claimant with control over their private information, but it has been considered until recently that such control cannot be exerted over all potential privacy-invaders, usually online. The Supreme Court in *PJS*[77] took the view that despite widespread disclosure of the information in question online, grant of the injunction against identifiable newspapers published in England was not entirely futile,[78] and was normatively justifiable.[79] But, although the distress occasioned by

---

[70] "Where the hearing….involves confidential information that may be harmed by publicity"; see Procedure Rules, Part 39(2): https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part39#39.2.

[71] See *American Cyanamid v Ethicon Ltd* [1975] A.C. 396; [1975] 1 All E.R. 504. S.12(3) HRA was enacted to set a slightly higher threshold for injunction awards: see *Cream Holdings Ltd v Banerjee and Others* [2004] UKHL 44; [2005] 1 A.C. 253.

[72] The Court of Appeal in *PJS* confirmed that s.12(3) had "raised the bar" as to proof needed to secure an interim injunction: *PJS v News Group Newspapers Ltd* [2016] A.C. 1081 [4], a finding that was not disputed by the Supreme Court.

[73] "…courts will be exceedingly slow to make interim restraint orders where the applicant has not satisfied the court he will probably ('more likely than not') succeed at trial.…": *Cream Holdings Ltd v Banerjee and Others* [2005] 1 A.C. 253 at [22]. See also *NPV v QEL and ZED* [2018] EWHC 703 (Q.B.); [2018] E.M.L.R. 20.

[74] See *CG v Facebook Ireland Limited and McCloskey (Joseph)* [2015] N.I.Q.B. 11.

[75] In *Google v Judith Vidal-Hall* [2016] Q.B. 1003the defendant had stopped the conduct complained of by the time the Particulars of Claim were served, and destroyed the relevant data, so the injunction claim was not pursued: at [12,iv].

[76] See e.g.: C. R. Campbell, "Death By Birdsong: Has Twitter Sealed the Coffin on Britain's Privacy Injunction" (2012) 41 *Georgia Journal of International and Comparative Law* 187; T. Manu and R. F. Moreno, "Is Social Media Challenging the Authority of the Judiciary? Rethinking the Effectiveness of Anonymised and Super Injunctions in the Age of the Internet" (2016) 18(32) *Journal of Legal Studies* 39.

[77] *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] A.C. 1081.

[78] At [45],[47].

further publication of the information would have been fairly – not entirely – similar[80] if such publication had been anticipated largely via non-identifiable online posters, possibly outside the jurisdiction,[81] a finding of the futility of seeking to pursue such actors via an injunction would probably have appeared inevitable at the time. Individual bloggers may host their websites on out-of-jurisdiction servers in an attempt to escape the jurisdiction of England and Wales and to make it more difficult and expensive for injunctions to be levelled against them; in the US, the First Amendment would prevent any privacy injunction being enforced, while injunctions awarded in England may be disregarded in the other UK jurisdictions.

Even where a media body or an online poster is identifiable and within the jurisdiction, it appears that potential claimants have been abandoning tortious actions as ineffectual once the information in question has become widely available online,[82] or due to the perception that even if granted the injunction would be ineffective due to the likelihood that postings of the information might well occur outside the jurisdiction. These problems probably explain in part why few injunctions have been awarded in recent years,[83] despite the very widespread dissemination of private information online. But, as discussed below, the courts are beginning to address them.

3. The operation and role of the "right to be forgotten" under the GDPR

The idea underlying the "right to be forgotten" ("the right to erasure") arising under the GDPR art. 17, partly cognate with that underlying injunctions, is that it avoids the distress

---

[79] "[where] the court is in a position to prevent some of that intrusion and distress…it may…maintain that degree of protection" [represented by an injunction]: *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] A.C. 1081 at [29]. See G. Horton "Injunctions and public figures: the changing value in injunctions for privacy protection" [2021] *Journal of Media Law* https://doi.org/10.1080/17577632.2021.1889866.

[80] Publication of the information in national newspapers was seen as more damaging than publication online: *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] A.C. 1081, at [29]. See also *Goodwin v NGN Ltd* [2011] EWHC 1437 (Q.B.); [2011] E.M.L.R. 27 (Q.B.D.).

[81] See T. Manu and R. F. Moreno, "Is Social Media Challenging the Authority of the Judiciary? Rethinking the Effectiveness of Anonymised and Super Injunctions in the Age of the Internet" (2016) 18(32) *Journal of Legal Studies* 39 at 62. It is clearly possible to search for content hosted on servers outside the English and Welsh jurisdiction, by e.g. using "Spanish Google" (see Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [2014] Q.B. 1022).

[82] Due to re-sharing of information available on social media. Some *en masse* breaching of injunctions was clearly intended to undermine specific injunctions. See: J. Agate, "Battle lines drawn: privacy injunctions following CTB et al" [2011] *Entertainment Law Review* 212 at 213); T. Manu and R. F. Moreno, "Is Social Media Challenging the Authority of the Judiciary? Rethinking the Effectiveness of Anonymised and Super Injunctions in the Age of the Internet" (2016) 18(32) *Journal of Legal Studies* 39 at 62; A. Thierer, "The Pursuit Of Privacy In A World Where Information Control Is Failing" (2013) 36(2) *Harvard Journal of Law and Public Policy* 409.

[83] E.g. in 2020 8 interim injunction applications were granted: Ministry of Justice, "Civil Justice Statistics Quarterly: Jan-June and July-Dec 2020": www.gov.uk.

and other harms suffered by the data subject whose private information remains available.[84] To that end art. 17(1) takes a fairly uncompromising approach; it dictates that the "data subject shall have the right to obtain from the controller the erasure of personal data concerning him/her *without undue delay* and the controller shall have the obligation to erase personal data" if one of several grounds applies, including a withdrawal of consent or that the data has been unlawfully processed.[85] The right can be invoked by a data subject[86] who contacts the data controller to request deletion; if the controller refuses the request, the data subject can challenge the controller's refusal to comply, by seeking to escalate the matter to a court for judgment, as occurred under the previous regime in *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner).[87] Objections would normally be on the grounds of one of the exemptions under art. 17, including freedom of expression (art. 17(3)(a)), compliance with a legal obligation/a task carried out in the public interest (art. 17(3)(b)).[88] In such a case, the court would examine the legality of the controller's refusal to comply with the erasure request and civil fines can be levied where a deletion request is unlawfully refused.[89] The wording of art. 17 clearly does not imply that there is a requirement that the data has already been disclosed or that disclosure is threatened; thus erasure is available where, as discussed below, under s.12(3) HRA injunctive relief would not appear to be. Intermediaries are not protected from art. 17 requests via the "safe harbours" under the e-commerce Directive[90] if their role is not purely passive,[91] and in any event once they have had notice.[92] Article 17 requires that for information to be deleted, that must first be

[84] E.g. employers often now conduct online search checks on job applicants: see, e.g.: S. Driver, **"**Keep It Clean: Social Media Screenings Gain in Popularity" (*Business News Daily*, 23.3.2020): https://www.businessnewsdaily.com/2377-social-media-hiring.html. Persons may seek to have spent convictions forgotten, as in *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2019] Q.B. 344. See: V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2009); D. Solove, "Speech, Privacy and Reputation on the Internet" in S. Levmore and M. Nussbaum (eds), *The Offensive Internet* (Cambridge: Harvard University Press, 2010).

[85] Art. 17(1)(a)-(d) GDPR. Grounds also include: the data subject objects to the processing pursuant to art. 21(1) or 21(2), and there are no overriding legitimate grounds for the processing.

[86] The identifiable individual to whom the information relates: art. 4(1).

[87] [2019] Q.B. 344.

[88] See also art. 17(3)(c),(d),(e). The controller could also refuse deletion on the grounds of the "journalistic exemption", discussed below.

[89] Art. 83(5)(a),(b).

[90] In e.g. *CG v Facebook Ireland* [2015] N.I.Q.B. 11 an injunction was obtained.

[91] Directive 2000/31/EC may potentially place limits on intermediary liability for transmission of data under art. 17 GDPR if the service provider's activity is "of a mere technical, automatic and passive nature" (e-Commerce Directive, Recital 42). But while such limits can operate to bar a claim for damages/compensation, they do not prevent the grant of injunctive relief "to terminate or prevent an infringement". This wording appears in relation to: I.S.P.s as "mere conduits" (art. 12(3)); caching information (art. 13(2)); I.S.P.s hosting information (art. 14(3)), and is reflected in s.20 2002 Regulations.

[92] See art. 14.

requested by a data subject; the intermediary would at that point have notice as to the disputed material.

4. Comparing the roles of the two remedies

Given the ease with which data erasure can be obtained, in comparison with the hurdles to be overcome in obtaining an injunction, the objective of minimising distress due to further disclosures of private information is more likely to be achieved in practice under the GDPR/DPA. It is usually more straightforward for a claimant to approach a website (particularly one run by a large conglomerate such as Facebook)[93] to request data deletion, or a national Data Protection Authority, as opposed to mounting a potentially lengthy and expensive tort action to seek to obtain an interim injunction and, if it is granted, then awaiting a court action in the hope that it will be maintained.[94] An injunction must be awarded by a judge, whereas erasure can be sought without judicial involvement. Erasure also covers a wider range of interactions with private information, including its storage, involving the specified forms of misuse. The right therefore appears to provide a more cost-effective, wider, rapid (no "undue delay") and accessible route to redress for data subjects.[95]

But a drawback of the right to erasure, as opposed to reliance on injunctive relief, is that – at face value – it cannot provide the equivalent of such relief in relation to threatened disclosures, since in *that* situation it operates as an *ex-post* remedy. The traditional position under the tort has been that the grant of an injunction *before* the personal information has been disclosed, or fully disclosed, means that the information will be more likely to retain its private quality.[96] In the first and second situations envisaged in the Introduction, if erasure was requested, the data in question would already be accessible, so the information would already be in the public domain, meaning that informational autonomy would already have been compromised.

The right of erasure can therefore be found to play a somewhat different role from that of an injunction where private information was at one point clearly in the public domain, explaining why de-listing as the previous equivalent of the right (very similar to requesting

[93] E.g. Facebook is readily contactable, see: https://www.facebook.com/help/; https://www.facebook.com/help/263149623790594; https://www.wikihow.com/Contact-Facebook.
[94] Once it had already been granted urgently, to preserve a state of stasis.
[95] If the request is not challenged by the controller under an exempting ground.
[96] See e.g. *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] A.C. 1081, at [41],[43].

erasure, but requiring court action) has been found to have particular applicability in relation to criminal convictions. A point has been found to arise at which, for the purposes of privacy protection, convictions can be found to have faded into the past, and therefore de-listing is applicable, whereas an injunction would be, under traditional analysis, less likely to be obtained since the conviction would probably be viewed as having entered the public domain already. These contentions are illustrated by *NT1 and NT2 v Google LLC (Intervenor: The Information Commissioner)*:[97] the claims were brought under both the tort[98] and the DPA 1998 on the basis that Google had provided links via personal name searches to the spent fraud-related convictions of two business-men, who wanted them to be expunged. NT2 succeeded in his de-listing request;[99] an injunction was not sought, possibly because its potential role could be satisfied by de-listing,[100] or given that the information was already in the public domain. It had been clear since *Google Spain*[101] that claims for data protection by way of de-listing (now taking the form of erasure requests) can succeed against intermediaries as data controllers.

Tortious claims for injunctions have been successful against social media platforms. *CG v Facebook Ireland Limited and McCloskey (Joseph),*[102] concerned sensitive private information about CG's previous convictions in 2007 for a number of sex offences. McCloskey ran a Facebook page termed "Keeping our Kids Safe from Predators 2" on which he posted comments and the comments of others about CG, identifying CG and to an extent the area he lived in. CG successfully sued both Facebook Ireland Ltd and McCloskey in relation to a series of these posts, alleging inter alia that they constituted a misuse of private information under both data protection and the tort. A mandatory injunction ordering Facebook to take down all the pages in question was awarded and that finding was undisturbed on appeal. There had also been an earlier judgment against both defendants in a case brought by a different convicted sex offender, in relation to a page entitled "Keeping Our Kids Safe from Predators".[103] Facebook in the earlier case, it was found, had misused the

[97] [2019] Q.B. 344, especially at [111],[130],[168].
[98] At [172],[226].
[99] Greater harm to his family life was found to arise due to the availability of the information: *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2019] Q.B. 344 at [216]-[218],[222(3)].
[100] At [227].
[101] Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [2014] Q.B. 1022. The case also concerned name-based searches: at [98].
[102] [2015] N.I.Q.B. 11.
[103] *XY v Facebook Ireland Ltd* [2012] N.I.Q.B. 96.

information by failing to delete it, and although the information was already in the public domain, an interim injunction was awarded.

In *J20 v Facebook Ireland*[104] the Plaintiff complained about a series of postings on Facebook, mainly couched in insulting terms, and including photographs of the claimant taken without consent. The postings were given added sensitivity due to the Irish context; the Plaintiff was accused of being a "loyalist bigot" and of ignoring his children because they were Catholics. At the time of this action, the Plaintiff had already obtained an emergency interim injunction requiring Facebook to take down the pages in question, and an injunction in relation to future similar publications on Facebook. Facebook then removed the offending pages. In that instance injunctive relief played the same role as in future erasure requests could do as far as the *published* information was concerned, but the potential preventive role of art. 17 in relation to *threatened* publication is more complex, as addressed below.

5. More flexible approaches: convergence of the roles of both remedies in the digital era?

The assumptions made about the distinctive roles of erasure and injunctions should now be questioned if their value is to be enhanced in the digital age. It is now often the case, especially due to online disclosures, that the information has partially entered the public domain regardless of the injunction since it is usually assumed that it cannot prevent disclosures by posters outside the jurisdiction, or before it can be obtained. Thus, in *PJS (Appellant) v News Group Newspapers Ltd (Respondent)*,[105] concerning disclosures of private information, the injunction was maintained, not to prevent disclosure of the information, since that had already occurred, mainly online, outside the jurisdiction, but to prevent *further* disclosure, and to prevent it in the mainstream media.[106] The role of the injunction was accepted in that instance as shifting from protecting privacy to minimising distress, as the Supreme Court made clear. The Court focused on the further *harms* caused by disclosure to the claimant and his family,[107] rather than merely considering whether the information had lost its private quality due to previous disclosure – a highly significant re-envisaging of the role of injunctions in the digital age. The decision indicated that in the digital age the traditional notion that injunctions are more valuable than damages since they can operate to

[104] (2016) N.I.Q.B. 98, at [5],[55],[56].
[105] [2016] A.C. 1081.
[106] See K. Yoshida, "Privacy injunctions in the internet age – PJS" (2016) 4 E.H.R.L.R. 434, at 435.
[107] *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] A.C. 1081 at [1],[44],[45],[63],[74]. See O. Butler, "Confidentiality and Intrusion: building storm defences rather than trying to hold back the tide" [2016] C.L.J. 452 at 452-453.

prevent private information from ever entering the public domain may need to be reviewed: their role may now often be one of harm-reduction once the information is already available online. The objectives of the right to erasure, therefore, and those underlying injunctive relief under the tort, are in some respects already beginning to align with each other more closely where the information in question has already been disclosed, meaning that the more flexible remedy – an injunction – may be available to claimants in positions similar to those of NT1 and NT2 or Mosley,[108] or where the defendant is out of the jurisdiction, as discussed below.

More significantly, there may be circumstances predisposing a claimant who is seeking erasure, as more rapidly and readily available than an injunction, to seek it although the information, or part of it, has *not* been disclosed already. The claimant may be seeking to keep specific facts, such as allegations of sexual abuse or family-linked information likely to have a severe impact on a child,[109] out of the public domain, meaning that the erasure right would only be fully effective if it could operate before the information in question is fully or partially disclosed. Merely seeking erasure after disclosure might not be viewed as sufficient to address the distress that would potentially be caused. If a controller has gathered and stored personal data on a private database it would appear that the right is still operable if the data subject knows that the private information is held but it has not yet been published or disclosed. Assuming that one of the conditions under art. 17 applied, the data subject could send an erasure request prior to disclosure, with which a court might later seek to compel the data controller to comply. As discussed below, however, this possibility would appear to apply in practice only to data deemed non-journalistic due to s.176 DPA 2018.

The argument would be that if the retaining of informational control – the objective of art. 17 – would be left unsatisfied in a particular case, the court should move to read in the potential to obtain relief – relief equivalent to that which would have been available via an injunction - under the art., relying on arts. 7 and 8 of the EU Charter, as occurred in *Lloyd v Google LLC*, albeit in that instance in relation to compensation.[110] Such an argument could also draw on s.3 HRA and art. 8 ECHR, bearing in mind that arts. 7 and 8 of the Charter reflect art. 8, to reinterpret art. 17 and other relevant provisions of the UK GDPR[111] and DPA to ensure the

[108] See *Mosley v Google* [2015] C.M.L.R. 22.
[109] Such as the example from *Re S* [2004] UKHL 47; [2005] 1 A.C. 593.
[110] [2020] Q.B. 747 at [41]-[42],[70].
[111] Art. 79 GDPR "Right to an Effective Judicial Remedy Against a Controller or a Processor"; art. 82 "Right to Compensation and Liability".

efficacy of the erasure right. The contention under s.3 would be that although the Strasbourg privacy jurisprudence, such as in particular *Mosley*,[112] does not appear to provide a basis for demanding that relief equivalent to injunctive relief should be made available in England and Wales beyond its current availability under the tort, the domestic courts could be asked to adopt this interpretation of art. 17, going "beyond" Strasbourg, mainly on the basis that the margin of appreciation doctrine is operative at Strasbourg[113] but not domestically.[114] Clear support from Strasbourg is not available, but would not be needed, although a recent minority Opinion accepted that online disclosures can be particularly damaging to the effective exercise of the right to respect for private life under art. 8,[115] and the Council of Europe took that stance unequivocally in 2020.[116] If this argument was accepted, which would be encouraged by the wording of art. 17, the role of erasure in relation to the first two situations outlined in the Introduction would quite clearly resemble that undertaken by injunctions, meaning that in future data subjects could rely on art. 17 in relation to certain non-"journalistic" threatened disclosures without necessarily engaging in court action.

In some circumstances a possible solution to the problem of the undermining of injunctions by online postings would involve relying on both art. 17 and the tort, operating in combination, even where anonymous posters and/or posters outside the jurisdiction were involved. Combining a claim for a grant of an injunction against the publisher of private information with an erasure request aimed at the tech companies where the intermediaries they control are enabling unconsented-to access to private information, could have some impact in reversing the trend towards abandoning the possibility of seeking injunctive relief.

---

[112] *Mosley v UK* App. No. 48009/08 (ECHR, 10 May 2011).

[113] See: *Von Hannover v Germany (No.2)* App. No.s 40660/08 and 60641/08 (ECHR, 7 February 2012); *Von Hannover v Germany (No.3)* App. No. 8772/10 (ECHR, 19 September 2013); *Couderc and Hachette Filipacchi Associes v France*, App. no. 40454/07 (ECHR, 12 June 2014); *Axel Springer AG v Germany* App. No. 39954/08 (ECHR, 7 February 2012).

[114] Domestic courts have taken this stance under art. 8 already: *Campbell v MGN Ltd* [2004] 2 A.C. 457 determining that art. 8 could impose an obligation to adhere to it on private actors, was decided before the same conclusion was reached in *Von Hannover v Germany*, App. No. 59320/00 (ECHR, 24 September 2004); the House of Lords has found that it can extend the range of interests protected under art. 8, although no decision at Strasbourg could be relied on: *In Re P and others (AP) (Appellants) (Northern Ireland)* (2008) UKHL 38; [2009] 1 A.C. 173. In *R (on the application of Nicklinson and another) v Ministry of Justice* [2014] UKSC 38; [2015] A.C. 657 it was found: "[where the Court had already found that the matter was within the member states' margin of appreciation] the national courts…must decide the issue for themselves, with [little] guidance from…Strasbourg…", both at [70].

[115] Opinions of Judges Wojtyczek and Kūris in *Fürst-Pfeifer v Austria*, App. No.s 33677/10 and 52340/10 (ECHR, 17 May 2016).

[116] See: https://www.coe.int/en/web/data-protection. See also EU Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law - 2018 Edition* (Luxembourg: EU Publications Office, 2018).

For example, in a situation resembling that in *Bloomberg*,[117] but where the information regarding the criminal investigation was being posted on social media, and was also available via Google, an injunction could be sought against the online news organisation, while in a concurrent action an art. 17 claim could be pursued against the online intermediaries as data controllers.[118] That could represent an effective strategy, although only if the spread of the information had remained fairly limited. Such requests, if complied with, could limit the continued availability of the information, and therefore would render the award of the injunction more meaningful.

A further prior restraint possibility arises as a result of the "Right to Object" in art. 21 GDPR; its exercise can lead to a right to restriction (under art. 18(1)(d) GDPR, "Right to Restriction of Processing") which bears some similarity to the impact of an emergency interim injunction, while the relative merits of the objection on the part of a data subject are verified - whether the legitimate grounds of the controller override those of the data subject. It also appears arguable from the wording of art. 21 that processing could be objected to leading to its restriction where it has not yet taken place but may do in future; for example, in the third situation from the Introduction, if a data controller such as Google has collected BGI and is about to disclose it to a third party company for gain, the data subjects could exercise the right to object against Google but possibly also against that third party, to prevent the anticipated processing, relying on art. 18(1)(d).

6. The defendant/data controller is out of the jurisdiction

The UK GDPR has extra-territorial scope under art. 3, applying to processing of personal data within or outside the EU, if the controller or processor is within the Union; in a range of circumstances it also applies to such processing where the data subject is within the EU, regardless of whether the controller is also within the EU.[119] In *Google v Judith Vidal-Hall*[120] the Court of Appeal found that proceedings could be served against Google in the US for

[117] *ZXC v Bloomberg LP* [2021] Q.B. 28.
[118] That situation bears some resemblance to *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2019] Q.B. 344, and *J20 v Facebook Ireland* (2016) N.I.Q.B. 98, although those instances concerned convictions.
[119] The CJEU in C-507/17 *Google LLC v CNIL* ECLI:EU:C:2019:772 at [72] accepted the possibility of a "worldwide de-referencing order in the future". See further: EDPB's *Guidelines 3/2018 on the Territorial Scope of the GDPR* 12.11.19; C. Hopkins, "Territorial scope in recent CJEU cases: Google v CNIL/Glawischnig-Piesczek v Facebook" (*Inforrm*, 9 November 2019), https://inforrm.org/2019/11/09/territorial-scope-in-recent-cjeu-cases-google-v-cnil-glawischnig-piesczek-v-facebook-cathryn-hopkins/.
[120] [2016] Q.B. 1003, at [6]-[11].

breach of the DPA 1998, so the same stance would be likely to be taken under the UK GDPR. Article 3 GDPR applies: (1) "to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not"; or, where the establishment of the controller/processor was outside the EU, (2) "to the processing of personal data of data subjects…in the Union by a controller or processor not established in the Union, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union".

The GDPR, including art. 17, therefore clearly potentially applies, in quite wide-ranging circumstances, to the processing of the personal data of a UK data subject by a publisher or intermediary outside the EU. The claim can be brought in the UK courts by a UK citizen even if the controller/processor is not based in a member state (art. 79(2)). Valuable findings as to the GDPR's territorial reach were made in the recent case of *Soriano v Forensic News and Others*[121] which concerned a claimant who wished to bring an action in the UK courts relying on the GDPR (and other legal avenues, including misuse of private information) against a US-based investigative journalism website, *Forensic News*; so the claimant needed the court's permission under C.P.R. Practice Direction 6B to "serve out". The case in part turned on the issue of the GDPR's jurisdiction, set out in art. 3. The claimant attempted, but failed, to establish that one of the three grounds in art. 3(1) and 3(2) applied. That was because, firstly, the controller's physical place of business and staff were in the US, and centrally targeted an American audience (the fact of its UK/EU readership was not found sufficient to satisfy art. 3(1)), so *Forensic News* had no *establishment* in the EU;[122] secondly, the court found that although someone in the EU had *once* bought a product from the website that would be insufficient to satisfy art. 3(2)(a),[123] and in any event such offering of goods and services must relate to "core activities" of the controller; thirdly, the monitoring which *could* fall within art. 3(2)(b) – "the behavioural profiling that informs advertising choices" - was found not to be *related to* the processing which was the subject of the complaint.[124] While the GDPR claim therefore failed, and the findings took a fairly restrictive approach to the

[121] [2021] EWHC 56 (Q.B.). See R. Hopkins "Overseas websites and the GDPR's reach" (*Panopticon Blog*, 19 January 2021).
[122] At [64].
[123] *Soriano v Forensic News and Others* [2021] EWHC 56 (Q.B.) at [66].
[124] At [68].

interpretation of art. 3, the consideration of the three methods of establishing its territorial reach indicated that on slightly different facts a number of ways of establishing such reach are available.

The position as regards extra-territorial scope under the tort is governed by Practice Direction 6B which supplements s.IV of the Civil Procedure Rules Part 6.[125] If an injunction is aimed at identifiable publishers or other actors misusing, or potentially misusing, private information on or offline *within* the jurisdiction, it can have an impact in minimising intrusion, as in *PJS*.[126] The problems of protecting private information where posters disclosing the private information are out of the jurisdiction have frequently been canvassed, and clearly such disclosure also undermines any injunction obtained against within-jurisdiction actors.[127] But, very significantly, the problem of bringing proceedings to enable the removal of access to the offending material in such circumstances could now be partly overcome, if the privacy concern arises due to postings on social media, or via provision of links to the information, by proceeding by way of the tort and seeking an injunction and damages against the intermediaries in question. That has already been found to be possible in relation to defamation,[128] but was also accepted in relation to misuse of private information, in the significant findings in *Google v Judith Vidal-Hall*,[129] on the basis, under Practice Direction 6B, that although the intermediary in question, Google, was US-based, the tortious *impact* took place within the jurisdiction.[130] The claimants successfully argued that there was a "serious issue" to be tried, that there was "a good arguable case" that the case came within the ambit of C.P.R. P.D. 6B, that it was appropriate that an English court should hear the case, and that "in…the circumstances, the court ought to exercise its discretion to permit

[125] Paragraph 3.1 Practice Direction 6B permits service without court permission in cases where: "(2) A claim is made for an injunction ordering the defendant to do or refrain from doing an act within the jurisdiction; (9) A claim is made in tort where (a) damage was sustained within the jurisdiction; or (b) the damage sustained resulted from an act committed within the jurisdiction."
[126] *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] A.C. 1081.
[127] See: *PJS*; J. Rowbottom, "A landmark at a turning point: Campbell and the use of privacy law to constrain media power" (2015) 7(2) *Journal of Media Law* 170 at 184.
[128] See *Hegglin v Person(s) Unknown & Google Inc* [2014] EWHC 3793 (Q.B.); [2015] 1 Costs L.O. 65; the case was settled but it was found in the previous hearing that there was no jurisdictional bar to the grant of an injunction since the *impact* of the tortious acts arose in England (judgment of Mr Justice Bean, July 31, 2014). A recent Australian judgment found that in allowing access to defamatory material, Google should be accounted a publisher: *Defteros v Google LLC* [2020] V.S.C. 219 (30 April 2020).
[129] [2016] Q.B. 1003.
[130] Paragraph 3.1 of Practice Direction 6B paras 3.1(2) and (9) applied since the action in question was found to be a tort. The claimants were in England; the defendant was a US-registered corporation; thus, the claimants had to "obtain the permission of the court pursuant to C.P.R. 6.36" and Practice Direction 6B to serve proceedings on the defendant: at [6].

service of the proceedings out of the jurisdiction".[131] That decision concerned damages since the collection of the BGI had already ceased, but in principle an injunction could be awarded in that situation, of clear significance in relation to the second and third situations outlined in the Introduction, although as regards the second other intermediaries would still be free to host/provide access to the information. Clearly, this possibility has limits in relation to the first situation set out in the Introduction: an injunction awarded against one privacy-invader outside the jurisdiction would not prevent further publication by others outside England and Wales,[132] but in *ZXC v Bloomberg LP* that did not deter the court from granting one, partly on the basis that publication online had not been widespread.[133]

7. The poster/publisher of the information is unknown or problematic to identify

In fairly unusual circumstances an injunction can be sought against *publishers* of the information even where a number of non-identifiable posters are involved, as occurred in *AMP v Persons Unknown.*[134] A woman's phone, containing non-password-protected explicit photographs of the claimant,[135] was stolen, and eventually they were uploaded to a Swedish website hosting "BitTorrent" files.[136] Her name was connected to each image so that, when her name was searched online, those images appeared.[137] As regards curbing the spread of the information in England and Wales,[138] expert evidence was provided to the court[139] as to the nature of BitTorrent, to the effect that it would be possible to trace "seeders" (people who have downloaded pieces of the file, and, due to its programming, allowed the pieces to be re-uploaded, promulgating the data) using their I.P. addresses obtained from internet service providers.[140] Due to the design of BitTorrent, even if some of the seeders were outside the jurisdiction, the injunction was able to prevent enough fragments being uploaded to make a file, thereby preventing the spread of the data. Unsurprisingly, a reasonable expectation of

[131] [2016] Q.B. 1003, at [7]. The court granted permission to serve out on similar grounds in *Soriano v Forensic News and Others* [2021] EWHC 56 (Q.B.).
[132] Contempt-based sanctions are available for breach of an injunction under Contempt of Court Act 1981 s.2 *if* individuals undertake publication within the jurisdiction. The Joint Committee on Privacy and Injunctions has urged the Attorney General to be vigilant in pursuing actions against breaches of injunctions online: "Privacy and Injunctions", chapter 4, [104]: https://publications.parliament.uk/pa/jt201012/jtselect/jtprivinj/273/27307.htm.
[133] [2019] E.M.L.R 20, at [144 ii)]; Court of Appeal: [2020] EWCA Civ 611.
[134] [2011] EWHC 3454 (T.C.C.).
[135] At [4]-[5].
[136] *AMP v Persons Unknown* [2011] EWHC 3454 (T.C.C.) at [8].
[137] The claimant successfully removed some of the links to these images (in the US) using the US Digital Millennium Copyright Act.
[138] *AMP v Persons Unknown* [2011] EWHC 3454 (T.C.C.) at [16].
[139] By Andrew Murray, L.S.E.
[140] *AMP v Persons Unknown* [2011] EWHC 3454 (T.C.C.) at [9]-[15].

privacy was found[141] and, notably, the judge, to ensure that the claimant would not have to re-file her case, granted a general injunction against "persons unknown" – in other words, to a class of people who possessed any part of the file[142] - thereby addressing the problem of multiple anonymous postings.[143] Clearly, this decision turned on two factors that would not be present in a number of online instances of misuse of private information in the form of images – that BitTorrent had been relied on, as opposed to situations whereby images are uploaded in their *entirety* to different sites by multiple anonymous individuals online, and also a significant number of the "seeders" were within the jurisdiction.[144]

A further unusual situation arose in *DDF v YYZ*,[145] in which an injunction was obtained against an unknown defendant poster to restrain the threatened disclosure of the private information in question available via the photo-sharing service Instagram, and to prevent harassment on that service. The claimant also obtained an order for permission to serve the proceedings on the defendant via Instagram. The claimant did not know the real identity of the defendant, and the nature of the threats involved was found to mean that it would be just, convenient and appropriate that relief was granted before the defendant was alerted to the institution of the proceedings.

More significantly, an injunction can provide a degree of protection in instances of online misuse of private information where the privacy invader is not identifiable; an injunction could be sought against the intermediary that has enabled access to information posted anonymously, requiring that the offending pages should be removed.[146] Or an erasure request to the effect that the links to the information should be expunged could be sent to the intermediary in question.[147]

8. Free speech barriers to injunctions or erasure: media-friendly tests?

[141] At [24]-[28].
[142] The BitTorrent seeders.
[143] *AMP v Persons Unknown* [2011] EWHC 3454 (T.C.C.) at [19]-[21].
[144] The facts were particularly compelling: see A. Orlowski *The Register*, 12.1.12, https://www.theregister.co.uk/2012/01/12/amp_bittorrent_injunction/.
[145] 21.6.2015: https://www.5rb.com/news/injunction-ordered-served-via-instagram/.
[146] As in *J20 v Facebook Ireland* (2016) N.I.Q.B. 98; many privacy-invading comments posted were made anonymously.
[147] E.g. in *Mosley v Google* [2015] C.M.L.R. 22 the determination that Mosley had a viable claim under data protection was not dependent on identifying the original posters of the information.

The remedies discussed can only be deployed subject to the demands of free expression. The argument advanced in the academic literature to the effect that the legal framework and case-law surrounding the award of injunctions was designed with the mass media in mind,[148] and therefore could detrimentally affect the claimant whose privacy is invaded online by non-media bodies,[149] is bolstered to an extent by considering part of the wording and content of s.12(4)(a) HRA. It applies if a court is considering remedies, including the award of an injunction,[150] and provides that where "journalistic, literary or artistic material" is under consideration "the court must have particular regard to the importance of the Convention right to freedom of expression"; apparently designed to enhance the weight of media claims in privacy cases,[151] it is clearly media-centric in aspiration, as is the recent Strasbourg art. 10 jurisprudence that influences the weight accorded to such claims.[152]

A somewhat similar weight is given to free expression under the GDPR/DPA. Article 17(3)(a) GDPR provides an exception to erasure if the processing serves the freedoms of expression and information, while provision reflective of s.12(4) arises under schedule 2 Part 5 paragraph 26 DPA 2018, which provides that processing for the "special purpose" of journalism, means that "journalistic" material,[153] receives particular protection; if para 26 applies, listed GDPR provisions, including the "right to be forgotten", do not apply to the extent that the controller reasonably believes that the application of those provisions would be incompatible with the special purposes (para 26(3)). Further, under s.176 DPA 2018 if "the controller or processor claims, or it appears to the court" that the personal data is being processed only for the special purposes, and with a view to the publication, inter alia, of journalistic material, the proceedings must be stayed pending a determination by the Information Commissioner, a categorical provision which effectively prevents pre-

[148] See further G. Phillipson, "Press freedom, the public interest and privacy" in A. Kenyon (ed.), *Comparative Defamation and Privacy Law* (Cambridge: CUP, 2016).
[149] See: F. Brimblecombe and G. Phillipson, "Regaining Digital Privacy? The New 'Right to be Forgotten' and Online expression" (2018) 4(1) *Canadian Journal of Comparative and Contemporary Law* 1; J. Rowbottom, "A landmark at a turning point: Campbell and the use of privacy law to constrain media power" (2015) 7(2) *Journal of Media Law* 170.
[150] S.12(1): s.12 "applies if a court is considering whether to grant any relief which, if granted, might affect the exercise of the Convention right to freedom of expression".
[151] E.g. Jack Straw M.P. stated to parliament that inclusion of s.12(4) should mean that injunctions were only granted exceptionally: H.C. Deb., 2 July 1998, col 536.
[152] See: *Axel Springer AG v Germany* App. No. 39954/08 (ECHR, 7 February 2012); *Von Hannover v Germany (No.2)* App. No.s 40660/08 and 60641/08 (ECHR, 7 February 2012) at [38],[118]; in both instances there was a tenuous link between allowing publication and *genuine* public interests. See further G. Phillipson, "Press freedom, the public interest and privacy" in A. Kenyon (ed.), *Comparative Defamation and Privacy Law* (Cambridge: CUP, 2016) at p.153.
[153] Para 26(1)(a)-(d) covers journalistic, academic, artistic material.

publication restriction. A grant of a final injunction-equivalent *after* initial publication (s.176(1)(c)) of such material could, however, be dependent on the application of the public interest and compatibility tests laid down in Schedule 2.

The requirements of para 26 include the requirement that "the controller reasonably believes[154] that the publication of the material would be in the public interest", and under paragraph 26(4), in making that determination "the controller must take into account the special importance of the public interest in the freedom of expression and information". Article 85 provides that member states shall "by law reconcile the right to the protection of personal data…with the right to freedom of expression and information…". Under art. 6(f) a condition of processing is that a legitimate interest of the controller is being pursued, which can include the interest in free expression.

In recent cases, when the court is reaching the stage of balancing arts. 8 and 10 ECHR, in order to determine whether the privacy-protecting remedy should be awarded, under either data protection or the tort, it has been found that the same considerations informing the balancing act[155] would be determinative of the outcome under both regimes.[156] So doubtful or weak speech claims could potentially lead to denial of the remedies discussed. The Supreme Court in *PJS*,[157] however, found that the balancing exercise at the stage of considering interim injunctions must treat rights to privacy and free expression as having equal weight, despite s.12(4). The Court further found that a public interest factor of very low value – invading privacy to promote public debate about anti-social behaviour – was found to be unable to bar the award of an injunction.[158] Lord Mance further found that "kiss and tell stories" have no public interest value.[159] Similarly, close scrutiny of the strength of the art. 8

[154] Para 26(2)(b). For discussion of "reasonably believes" under the DPA 1998 s.32, see the Court of Appeal in *Campbell v MGN* [2002] EWCA Civ 1373; [2003] Q.B. 658.
[155] See Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [2014] Q.B. 1022; at [81],[97] it was found that a similar balancing act, as conducted at Strasbourg (already influencing the one under the tort), would apply to the interpretation and application of the previous Directive.
[156] E.g. in *Cliff Richard v (1) The British Broadcasting Corporation (2) South Yorkshire Police* [2019] Ch. 169 at [226] it was found: "I do not propose to consider [DPA issues]…the DPA claim….adds nothing to the privacy claim." Use of the balancing act as under the tort (where the exemption under s.32 was not found to apply) in respect of the provision equivalent to art. 6(f) DPA 2018 under the Data Protection Act 1998, Sched. 2, Condition 6(1), was affirmed as appropriate in *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2019] Q.B. 344 at [115],[132].
[157] *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] A.C. 1081 at [20],[33].
[158] At [22].
[159] *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] A.C. 1081 at [15].

and 10 claims arose in *ZXC v Bloomberg LP*[160] in the context of a claim for an injunction to prevent further reporting on a criminal investigation relating to business dealings; it was concluded that the expression in question had limited public interest value, and the issues at stake could be discussed without disclosing details specifically relating to the claimant: "A restriction on…publication…does not impinge upon the Defendant's ability to report generally on…issues of significant public interest concerning alleged corruption in the foreign country…".[161] Such determination to identify matters of genuine public interest if an award of an injunction or an erasure request is disputed is likely to apply now to Schedule 2 Part 5, paragraph 26(4) DPA 2018, and the other aspects of the GDPR speech-protective framework.

The recent tendency identified in the tort decisions on injunctions – to seek to identify genuine public interest value for s.12(4) purposes - appears to find echoes in recent decisions in which intermediaries have sought to rely on free expression arguments under the tort or the previous data protection regime. In, for example, *CG v Facebook Ireland Limited and McCloskey (Joseph),*[162] in respect of a claim for damages/compensation and an injunction, it was found that the public interest value of warning the public in polemical terms that the claimant had been a sex offender was minimal, or virtually non-existent, meaning that the privacy argument prevailed. The CJEU in *Google Spain* held that the search engine Google could *not* rely on the journalistic exemption under the 1995 Directive[163] and that was confirmed in *NT1 and NT2 v Google.*[164] That decision concerned links to criminal convictions; a degree of speech value was identified in terms of warning the public as to the implications for future business dealings of the claimants' previous convictions; in respect of NT2 the privacy claim, however, prevailed, by a small margin, due to the impact of the revelations on his family, meaning that his de-listing claim succeeded.[165] It may be suggested that the jurisprudence governing the speech-protective framework under the HRA s.12 appears to be accommodating to the online context; the courts, following the lead from *PJS*, are showing a determination to discard the previous media-friendly stance, rendering it less

[160] [2019] E.M.L.R 20 at [133]. The findings as to the balancing act were accepted on appeal: [2021] Q.B. 28.
[161] At [133].
[162] *CG v Facebook Ireland Limited and McCloskey (Joseph)* [2016] N.I.C.A. 54. (first instance: *CG v Facebook Ireland Limited and McCloskey (Joseph)* [2015] N.I.Q.B. 11).
[163] Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [2014] Q.B. 1022.
[164] *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2019] Q.B. 344 at [98]-[102].
[165] At [111],[130],[168].

likely that the tech companies could also take advantage of spurious "public interest" arguments. It appears likely that the equivalent framework under the GDPR/DPA will follow suit.

Claims in which search engines or social media platforms have collected personal data concerning consumer preferences (browser-generated information) to disclose for commercial profit would clearly favour privacy claimants, whether brought under the tort or data protection: the information would almost always have value only in terms of *private* gain;[166] not only would they fall outside the "journalistic exemption", but no plausible public interest value could be claimed.[167] It may be concluded tentatively – since decisions in the three categories of online privacy-invasion put forward in the Introduction to this article are only recently emerging – that reliance on spurious notions of "public interest" under the speech-protective frameworks of both the HRA and GDPR/DPA are not likely to present barriers to privacy protection, unless *genuine* public interest claims are present.

IV. Conclusions

This article has argued that rather than merely acquiescing to the power of the tech companies, the legislature, courts, and watch-dog bodies, including the Information Commissioner, are taking an expansive approach to utilising remedies under both the tort and data protection to seek to protect private information online, covering, in certain circumstances, the three instances outlined in the Introduction. Court action is reining in the power of the companies in encouraging class claims as in *Lloyd* under data protection and also in accepting that tortious claims can be served out of the jurisdiction, as in *Vidal-Hall* (in the third situation above). In a range of respects the new prospect of availability of art. 17 erasure requests and of expanding uses of injunctive relief or its equivalent mean that particularly powerful privacy-protecting remedies are showing some equivalence and are now of rising significance in the online privacy context, rendering protection for private information available in the second situation against intermediaries, bearing in mind that search engine activity is not deemed "journalistic". The level of protection provided for persons whose personal information has been posted online in breach of data protection and/or the tort (the first situation) is seeing an incremental augmentation, even, in some

[166] See e.g. *Google v Judith Vidal-Hall* [2016] Q.B. 1003 (under the previous DPA regime).
[167] In *Google v Vidal-Hall* freedom of expression arguments, understandably, did not feature.

circumstances, where anonymous or out-of-jurisdiction posters are concerned. Clearly, this article is speculative as regards the GDPR, a number of the decisions discussed are only at first instance or have only determined that a claim is viable: the jurisprudence under consideration here is in its infancy; this article represents an attempt to find coherence in the trends that are currently emerging. The privacy-protective framework discussed reflects global efforts to enable individuals to retain control over their private information online, rejecting the notion that privacy can no longer be viewed as a social norm in the digital era,[168] and the idea of the irresistibility of the monopoly power of the tech companies.[169]

Fiona Brimblecombe

Wallscourt Fellow in Law (Senior Lecturer), Bristol Law School, University of the West of England

Helen Fenwick

Professor of Law, Durham Law School, Durham University

[168] See B. Johnson, "Privacy is no longer a social norm, says Facebook founder": *The Guardian* (London, 11.1.2010): https://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

[169] Google has almost complete dominance of the search market; Facebook manages six of the top ten social media apps globally. See further R. Fernandez et al., "The financialisaton of Big Tech" (*SOMO*, December 2020): https://www.somo.nl/wp-content/uploads/2020/12/Engineering_Financial-BigTech.pdf.