

Protecting private information in the digital era: making the most effective use of the availability of the actions under the GDPR/DPA and the tort of misuse of private information

Abstract

Globally, enhanced data protection schemes are being introduced in the face of threats to privacy in the digital era. In England and Wales protection from one such threat – from unconsented-to disclosures of private information online - is covered by *both* the established tort of misuse of private information and a recently enhanced data protection scheme, arising under the GDPR, providing in particular the right to erasure. The *previous* scheme ran alongside the tort, in an uneasy relationship which until recently saw its marginalisation in the privacy context under consideration, with the result that the data protection jurisprudence in this context is impoverished, while the tort jurisprudence and scholarship has flourished. This article argues that merely noting that the two causes of action are available and may arise in the same claim provides a limited response. With the advent of the UK GDPR, and the rise in the dangers to protection of private information posed by the ‘tech’ companies, it presents a new argument in opposition to the two separate silos into which scholarship in this area has fallen, and, more importantly, in favour of the opportunities the two actions provide for addressing the range and variety of privacy claims, especially against online ‘intermediaries’, including from non-celebrities. To that end it probes the differences between the designs of the key elements of the two actions which might render one more apt or able to provide privacy protection, depending on the situation, than the other, especially in the online context. It also considers as a warning potentialities within both that could detract from their efficacy.

Key words

Misuse of private information, UK GDPR/DPA, free expression, intermediaries, ‘tech’ companies

Introduction

Globally, enhanced data protection schemes are being introduced in the face of threats to privacy in the digital era.¹ In England and Wales protection from one such threat – from unconsented-to disclosures of private information on or offline – is now covered by *both* the

¹ For example, India is following the model of the EU's General Data Protection Regulation (GDPR) in introducing the Personal Data Protection Bill 2019, allowing global digital companies to conduct business there under certain conditions, as is Sri Lanka in ‘The Framework for the Proposed Personal Data Protection Bill’ 2019; in both cases that stance is being taken, as opposed to following the isolationist framework of Chinese regulation which prevents global tech companies like Facebook and Google from operating within its borders.

established tort of misuse of private information and the recently enhanced data protection scheme under the General Data Protection Regulation 2016 (GDPR) (now referred to as the UK GDPR and relied on by the Data Protection Act 2018).² That somewhat anomalous situation – in which two causes of action appear to operate largely as fairly close equivalents - has subsisted for some time: the tort and the previous data protection scheme under the Data Protection Act 1998 (DPA)³ have run alongside each other for around twenty years, in an uneasy relationship which has until recently seen the marginalisation of the latter in the privacy context under consideration.⁴ The result has been that the data protection jurisprudence in this context is impoverished, while the tort jurisprudence and scholarship has flourished. The tort remained in general firmly in the ascendant where both causes of action were at stake, on the basis that the data protection claim would add little or nothing to the tort one.⁵ But the threat to protection of personal information is changing – it is now coming from the tech companies as much as from the traditional media bodies. The global rise in the volume of personal information online,⁶ including via ‘intermediaries’,⁷ means that a rise in the number of claimants challenging disclosures of such information when un-consented-

² Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (General Data Protection Regulation, hereafter GDPR) [2016] OJ L119/1 (27/4/2016).

³ Reflecting Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and of the free movement of such data [1995] O.J L 281, 31, Article 2(a) and Recital 26.

⁴ A number of claimants under the previous DPA 1998 regime brought the claim under both the tort and the DPA on the same set of facts as regards the information in question, but the judges focused mainly on the tort claim; see eg: *Campbell v MGN Ltd* [2004] 2 AC 457, 459 [32] (under DPA 1998, s 4(4)); *David Murray v Express Newspapers* [2007] EWHC 1908 (Ch) at [22]. See also n 5.

⁵ See eg *Sir Cliff Richard OBE v (1) The British Broadcasting Corporation (2) South Yorkshire Police* [2018] EWHC 1837 (HC) at [226]: ‘It will be noted that I have not included any issues arising under the DPA... That is because I do not propose to consider them. [Counsel] submitted that he was entitled to a verdict on the DPA claim, although he accepted that if he won on privacy then he did not need his DPA claim, which would not get him any more than his privacy claim and if he lost on privacy his DPA claim would not save him. In other words, it adds nothing to the privacy claim. In those circumstances I do not think it is necessary (or proportionate) for me to consider it, and I shall not do so’. In *ZXC v Bloomberg LP* [2019] EWHC 970 (QB) it was noted: ‘The Claimant accepted that, if he could not succeed with his claim in relation to the misuse of private information, he would not succeed in...the Data Protection Act claim’ [3]. See also n 16.

⁶ Eg in 2020 1.69 billion Facebook users logged on to Facebook and Instagram every day: see ‘Number Of Users Worldwide Statista’ (Statista, 2020) at <https://www.statista.com/statistics/490424/number-of-worldwide-facebook-users/#:~:text=This%20statistic%20shows%20the%20number,from%201.34%20million%20in%202014.> and ‘By The Numbers (2020): Stats, Demographics & Fun Facts’ (Omnicoagency.com, 2020) at <https://www.omnicoagency.com/instagram-statistics/> (accessed 8 October 2020). Websites may have huge readerships and followings, attracting many people from a range of demographics: see eg *Monroe v Hopkins* [2017] WLR 68, at [71(3)].

⁷ The term is used here only to denote entities that enable access to personal information online, gather and disclose it for gain, or host it, as opposed to publishing it, so it covers search engines and social media platforms. But see as to the complexity of the term: G. Dinwoodie, *Who are Internet Intermediaries?* (Oxford: OUP 2020).

to/unauthorised, under the tort and data protection, is already currently under way,⁸ prompting the following re-evaluation of the opportunities presented by the availability of both these areas of liability in the online context, and of their ability to protect persons from the forms of online privacy invasion that are the main subject of this article.

This article will focus on one particular aspect of the fundamental right to privacy, reflecting the value often viewed as at the core of informational autonomy, the preserving of control over unconsented-to disclosures of personal information. Online harm created by such loss of control includes the misuse of data due to its dissemination via social media platforms, and due to its gathering and then disclosure of data for commercial purposes.⁹ The view will be taken, in accordance with the general academic stance,¹⁰ that the preservation of such control lies at the heart of European informational privacy protection,¹¹ reflecting a concern that is especially engaged by the recent dramatic increase in such disclosures online.¹² Hence the focus of this article on the tort and on addressing such disclosures under the GDPR, including via the ‘right to be forgotten’ (Article 17), in order to answer to this aspect of a control-based notion of privacy.¹³ While other aspects of privacy protection under the GDPR, including

⁸ See for recent examples of claims, n 16 and n 39. Many de-listing requests are being made to Google relating to unconsented-to access to personal information: eg in *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2018] EWHC 799 (QB) it was noted that between the *Google Spain* decision (n 26) and 4 October 2017, a period of some 3½ years, Google had been asked to de-list almost 1.9m URLs or links to private information via named person searches.

⁹ In *Google v Judith Vidal – Hall* [2014] EWHC 13 (QB) it was the ‘subsequent use of that information’ – the browser-generated information – (at 1052) which was found to bring the situation within the area of tortious liability – and it is the disclosure of private information, whether to the public at large, or for commercial gain that is the subject of this article. It is significant that a court action on this basis has recently been launched in the UK: a 12-year-old girl, supported by the children’s Commissioner for England, is seeking to take legal action against the video-sharing app TikTok, claiming that the company collects and discloses children’s data unlawfully, to generate advertising revenue. Mr Justice Warby in the High Court has already granted the girl anonymity in bringing the claim on the basis that she might suffer significant harm via online bullying by TikTok users if her identity was known: *SMO (a child) by their litigation friend Anne Longfield v TikTok Inc and others* [2020] EWHC 3589 (QB), 30 December 2020.

¹⁰ See Westin’s seminal work, identifying four functions of privacy, including enabling the exercise of personal autonomy, emotional release, testing moral activities in communion with others, sharing intimacies (A.F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) 34-35). All these functions relate to choice and control over the audience for private information. See further: R. Wacks, *Privacy and Media Freedom* (Oxford: OUP 2013), 21; H. Fenwick and G. Phillipson, *Media Freedom Under the Human Rights Act* (Oxford: OUP 2006), 662-666.

¹¹ It should be noted that the right of erasure (the ‘right to be forgotten’) protects personality rights (in the sense of protecting both privacy and reputation) generally and so does not solely constitute a ‘privacy law’.

¹² See a number of the very recent cases considered here concerning unconsented to disclosure of private information, including at n 9, n 16. For discussion, see: P Bernal ‘*What Do We Know and What Should We Do About Internet Privacy?*’ (Sage 2020); P. Bernal *Internet Privacy Rights: Rights to Protect Autonomy* (CUP 2014); M. Mills, ‘Sharing privately: the effect publication on social media has on expectations of privacy’ (2017) 9(1) *Journal of Media Law* 45.

¹³ The harm has been accepted as consisting of the loss of control of personal data, without the need to prove a specific psychological harm or a diminution of welfare or financial loss; see: *Gulati v MGN* [2015] EWCA Civ

curbing the unconsented-to collection by state bodies of personal information online,¹⁴ checking the accuracy of such information or the security of its storage,¹⁵ are clearly relevant to the preservation of informational autonomy, they will lie outside its scope.

Where both causes of action could arise in the context of the same claim in respect of online privacy, claimants may be advised that reliance on one is more appropriate in their particular situation, or that it may be advantageous to proceed under both even though, obviously, they cannot ‘double-recover’.¹⁶ A key intention underlying the GDPR – to rein in the power of the tech companies to invade online privacy¹⁷ – contrasts with the intention underlying the design of the tort, originally designed largely in the context of such invasion by the traditional media; therefore in the digital era the GDPR will clearly not be as under-used in the privacy context under discussion as was the DPA 1998. This article envisages an increasing court-based reliance on both areas of liability in that era and foreshadows the nature of the jurisprudence that is beginning to arise, arguing that it is likely to provide privacy claimants with an enhanced ability to rely on the tort against online ‘intermediaries’. The tort jurisprudence in this specific privacy context is far more established than was the case under the previous data protection scheme, but its rooting largely, not wholly, in the intention to protect privacy from traditional media intrusion is now involving a change of approach; while clearly it will continue to provide some protection from such intrusion, its current and future role in relation to online privacy invasion now requires reflection, which this article seeks to provide. Judges confronted by both tort and data protection claims in this online privacy context will clearly proceed in a fact-sensitive manner, characteristic of common law

1291 [45]; see also *SMO (a child) v TikTok Inc*, n 9: ‘The damages claimed are for “loss of control of personal data”[2]. For some accounts of a control-based definition of privacy, see: R. Parker, ‘A Definition of Privacy’ (1973) 27 *Rutgers Law Review* 275, 276; C. Fried, ‘Privacy’ (1967) 77 *Yale Law Journal* 475; A. Westin, ‘The Origins of Modern Claims to Privacy’ in F. Schoeman (ed) *Philosophical Dimensions of Privacy* (Cambridge: CUP 1984); H. Nissenbaum, *Privacy in Context* (Redwood City: Stanford University Press 2009) 75; V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press 2009).

¹⁴ GDPR, Article 5(1)(b),(c).

¹⁵ *ibid*, ‘Principles relating to the processing of personal data’, (d) and (f), by way of example.

¹⁶ An example arose in *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2018] EWHC 799 (QB) at [43]: ‘The relationship between the laws of misuse of private information and data protection has been discussed on occasion. They are often considered to lead to the same conclusion, for much the same reasons.’ See also to similar effect *Lloyd v Google LLC* [2019] EWCA Civ 1599 [53].

¹⁷ See Recital 6 GDPR: ‘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 in order to pursue their activities’.

reasoning, adapting the key elements of the tort to a context radically different from that within which the tort was originally forged.¹⁸ That is already beginning to occur.¹⁹

Against that back-drop, this article will argue that merely noting that the two causes of action are available and may arise in the same claim provides a limited response. With the advent of the UK GDPR, and the rise in the dangers to protection of private information posed by the ‘tech’ companies, it presents a new argument in opposition to the two separate silos into which scholarship in this area has fallen, and, more importantly, in favour of the opportunities the two actions provide for addressing the range and variety of privacy claims, especially against online ‘intermediaries’, including from non-celebrities. To that end it probes the differences between the designs of the key liability-creating elements of the two actions which might render one more apt to provide privacy protection, depending on the situation, than the other, especially in the online context, and considers as a warning potentialities within both that could detract from their efficacy.

The legal context under the ECHR and EU Charter of Fundamental Rights

The Court of Appeal in *Lloyd v Google LLC*²⁰ 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’.²¹ That regime influences these two somewhat coterminous areas of law by way of both the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights, given that a number of the relevant rights align.²² It is well established that Strasbourg jurisprudence is relevant to the interpretation and application of Union laws²³

¹⁸ 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, 187.

¹⁹ See in particular the claims referred to in n 16 (*NT1 and NT2 v Google LLC*) and n 222.

²⁰ [2019] EWCA Civ 1599. The claim was heard by the Supreme Court in April 2021, but the judgment has not yet been made available: UKSC 2019/0213. That significant case concerned a challenge to the collection of browser-generated information to disclose to a third party for commercial gain.

²¹ *ibid*, at [53].

²² Where they do so the EU Charter Article 52(3) provides that the meaning and scope of both are to be taken to be the same. See further: W. Weib, ‘Human Rights in the EU: Rethinking the Role of the European Convention on Human Rights After Lisbon’ (2011) 7(1) *European Constitutional Law Review* 64, 64-67; F. Brimblecombe, ‘The Public Interest in Deleted Personal Data? The Right to be Forgotten’s Freedom of Expression Exceptions Examined Through the Lens of Article 10 ECHR’ (2020) 23(10) *Journal of Internet Law* 1, 15.

²³ See: N. O’Meara, ‘“A More Secure Europe of Rights?” The European Court of Human Rights, the Court of Justice of the European Union and EU Accession to the ECHR’ (2011) 12(10) *German Law Journal* 1813, 1814; C. Eckes, ‘EU Accession to the ECHR: Between Autonomy and Adaption’ (2013) 76(2) *MLR* 254, 254.

due to inter-court comity between the Court of Justice of the EU (COJ) and the European Court of Human Rights (ECtHR).²⁴ Both courts regularly cite the other's judgments and look to each other for guidance, in some instances the COJ taking the ECtHR's more experienced lead when adjudicating upon aligned rights.²⁵ In *Google Spain*²⁶ the Advocate General in his Opinion found that since Article 7 of the Charter of Fundamental Rights [respect for private life] is 'in substance identical to article 8 [ECHR]' it must be duly taken into account 'in the interpretation of the relevant provisions of the [previous] Directive, which requires the member states to protect *in particular* the right to privacy'.²⁷ Further, he found that 'in conformity with article 52(3) of the Charter, the case law of the Court of Human Rights on article 8 [ECHR] is relevant both to the interpretation of article 7 of the Charter and to the application of the Directive in conformity with article 8 [protection of personal data] of the Charter'.²⁸ Strasbourg's interpretations of 'private or family life'-based information under Article 8(1) will therefore influence the interpretation of Articles 7 and 8²⁹ of the Charter of Fundamental Rights, which will now influence the interpretation of the GDPR. The same clearly applies to the influence of Article 10 ECHR, highly relevant in this privacy context to the interpretation of both the tort and GDPR/DPA and to the interpretation of its counterpart, Article 11 of the Charter (protecting freedom of expression).

Thus, even after 'Brexit', the interpretation of the UK GDPR, as a retained provision following the end of the post-Brexit transition period under the EU (Withdrawal) Act 2018, will still be influenced by interpretations based on the relevant Article 8 and 10 ECHR jurisprudence. Such jurisprudence had an influence on the interpretation of the previous data protection scheme via both domestic decisions,³⁰ and pre-'Brexit' COJ decisions which took account of Articles 7 and 8 of the Charter.³¹ Clearly, the indirect influence of the Charter

²⁴ O'Meara *ibid*, at 1815.

²⁵ See T. Pavone, 'The Past and Future Relationship of the European Court of Justice and the European Court of Human Rights: A Functional Analysis' M.A Programme in Social Sciences, University of Chicago (28th May 2012) 1.

²⁶ Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [2014] WLR 659, ECLI:EU:C:2014:317; the Opinion of Advocate General Jääskinen of 25 June 2013.

²⁷ *ibid* at [114].

²⁸ *ibid* at [115].

²⁹ Article 8(1): 'Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'. Obviously the GDPR now provides that basis.

³⁰ See eg n 16.

³¹ See in particular n 26.

post-‘Brexit’ in domestic law is yet to become fully apparent,³² but Articles 7, 8 and 11 were based on pre-existing general principles of EU law and should therefore remain unaffected by the removal of the Charter.³³ Since Articles 7 and 11 have equivalents in Articles 8 and 10 ECHR, which have effect in domestic law via the Human Rights Act 1998 (HRA), that provides a further basis for their continuing domestic impact and influence on the interpretation of the GDPR/DPA. The design of the tort has also been shaped by the Strasbourg Article 8 and 10 jurisprudence. But, despite these commonalities in human rights terms, some differences between the two causes of action emerge in relation to the scope of their privacy protection but much less so in relation to the protection they provide for freedom of expression, as will be discussed.

‘Private life’ information – differences between its recognition under the tort and the GDPR

Disclosing/facilitating online actors; threats of intermediaries to private information

Questions as to *which* online actors are susceptible to attracting liability under the tort are beginning to be addressed, whereas that issue is less problematic under the GDPR. Online blogging, or postings on social media including personal information clearly amount to data-processing.³⁴ The hosting of unconsented-to third party disclosures of personal information on social media platforms such as Facebook, and the creation of links to such information via search engines, are covered by the GDPR/DPA since such intermediaries are also viewed as data controllers³⁵ and within scope of liability if their role is not purely passive.³⁶ A partial

³² Under the EU (Withdrawal) Act 2018, s 5(4) the Charter ‘is not part of domestic law on or after exit day’, but its status for a period will depend on the transitional provisions; the status of decisions of the COJ will depend on the harmonisation provisions, but they will still influence domestic law in relation to retained law. See for discussion C. Barnard, ‘So Long, Farewell, Auf Wiedersehen, Adieu: Brexit and the Charter of Fundamental Rights’ (2019) 82(2) MLR 350-366, especially 360 onwards.

³³ They would be expected to be unaffected, in line with the EU (Withdrawal) Act 2018, s 5(5) and Sched 1(2). The government has acknowledged in its right-by-right analysis that Articles 7,8 and 11 of the Charter were pre-existing general principles of EU law: see ‘Charter of Fundamental Rights of the EU’ (2017) 24-25 at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664891/0512_2017_Charter_Analysis_FINAL_VERSION.pdf (accessed 8 October 2021).¹⁰

³⁴ See eg *The Law Society and others v Kordowski* [2014] EMLR 2 at [82].

³⁵ There has previously been debate over who or what can be found to be a data controller, but it is now apparent that the tech companies owning social media platforms are viewed as data controllers under the GDPR (that was the case under the previous scheme, and it is also the stance taken under the GDPR by the European Data Protection Board: see eg Guidelines 8/2020 on the targeting of social media users, adopted 2nd September 2020); see Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] (ECJ) ECLI:EU:C:2018:388, accessible at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0210> (accessed 8 October 2021).¹⁰ in which Facebook

parallel could be drawn with the provision regarding operators of web-sites in section 5(2) Defamation Act 2013 providing a defence if it was not ‘the operator who posted the statement on the website’. The position under the tort is more complex and currently developing: it also clearly covers the online *publisher* of the information,³⁷ who may often utilise such platforms for publication, and it is now apparent, although not yet firmly established, that the platform *itself* can incur tortious liability if it has notice of the content and therefore could not utilise an intermediary defence under the E-Commerce Directive (it ceased to apply from January 2021).³⁸ Search engines which have *only* provided links to information are not currently covered by the tort, but once the engine has decided to maintain

was found to be a (jointly) responsible data controller (alongside those who operated a Facebook page). Also see Court of Justice of the European Union, ‘The administrator of a fan page on Facebook is jointly responsible with Facebook for the processing of data of visitors to the page’ (Press Release No. 81/18, 2018) at <https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180081en.pdf> (accessed [8 October+2 November 2021](#)⁹). See under the previous regime, determining that search engines can be data controllers: Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [2014] W.L.R 659; *Mosley v Google* [2015] EWHC 59 (QB); *GC, AF, BH, and ED v Commission nationale de l’informatique et de Libertes (CNIL), Premier ministre, and Google LLC* 24 September 2019. See also *Lloyd v Google LLC* [2019] EWCA Civ 1599, concerning a claim under the DPA 1998 since the defendant had collected information about the claimant’s internet usage to disclose for gain.

³⁶ Intermediaries might potentially be able to take advantage of their ‘shield’ under the E-Commerce Directive (Directive 2000/31/EC Article 14) where their role is merely passive: the Directive may place limits on intermediary liability for transmission of data under Article 17 GDPR if the service provider’s activity is “*of a mere technical, automatic and passive nature*” (Recital 42, E-Commerce Directive). Hosting providers will lose the benefit of the Article 14 exemption if, upon obtaining actual knowledge of illegal activity or information, or awareness of facts or circumstances from which the illegal activity or information is apparent, they fail to act expeditiously to remove or disable access to the information. Article 17 requires that for information to be deleted, that must be first be requested by a data subject; the intermediary would at that point have notice as to the disputed material and so would appear to lose its shield. See further G. de Gregorio, ‘The E-Commerce Directive and GDPR: Towards Convergence of Legal Regimes in the Algorithmic Society?’ (EUI Working Paper RSCAS 2019/36, 2019) at [RSCAS 2019/36 The e-Commerce Directive and GDPR: Towards Convergence of Legal Regimes in the Algorithmic Society?](#) (eui.eu) (accessed [8 October+24 December 2021](#)⁹).

³⁷ See: *Rocknroll v News Group Newspapers Ltd* [2013] EWHC 24 (Ch) at [25]; *AMP v Persons Unknown* [2011] EWHC 3454. The notion of social media as a more ephemeral form of internet-use, as compared to setting up a blog or posting an article on a newspaper’s website, representing a lawless area of the internet where ‘anything goes’, was put to bed in the defamation case of *Monroe v Hopkins* [2017] EWHC 433 (QB), [2017] WLR 68 [54]-[62]; over a thousand estimated views of a defamatory tweet (as well as other forms of engagement online) were deemed to create ‘substantial’ disclosure, enough to cause reputational harm. The interest at stake in relation to privacy does not in contrast require ‘substantial’ disclosure, so unconsented-to disclosure of private information on social media, viewed by a small number of persons – or possibly only one – would appear to be capable of attracting tortious liability.

³⁸ See ‘The e-Commerce Directive and the UK’, Department for Digital, Culture, Media and Sport, 5.1.21, updated 18.1.21. In *CG v Facebook Ireland Limited and McCloskey (Joseph)* [2015] NIQB 11, CG had been convicted in 2007 of a number of sex offences. Mr 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 and others, identifying CG and to an extent the area he lived in. CG successfully sued Facebook Ireland Ltd and McCloskey in relation to a series of these posts, alleging inter alia that they constituted a misuse of private information. There had 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” (*XY v Facebook Ireland Ltd* [2012] NIQB 96). Facebook in the 2015 case, it was found on appeal (*CG v Facebook* [2016] NICA 54), had misused the information by failing to delete it; all the circumstances had to be taken into account in deciding whether an ISP had actual knowledge of the unlawfulness of the material; Facebook appeared to have such knowledge due to the earlier action; a defence under the E-Commerce Directive therefore failed.

links despite a request to remove them on privacy grounds, tortious liability could potentially arise (*Townsend v Google*).³⁹ That has now been found to be the case where the engine has *collected* browser-generated information with a view to its disclosure for private gain – in *Google v Judith Vidal – Hall*.⁴⁰

In the digital era, therefore, protection for private information under the tort is receiving more expansive interpretations of its scope - extending liability from the traditional media (post-2000), to online publishers (around 2010 onwards), and now also to online intermediaries, where the intermediary's role is more than a purely passive one. But while the tort is now beginning to adapt itself to the online environment in potentially applying to intermediaries, as well as publishers, the discussion below questions whether the nature of the jurisprudence affecting the current determinations as to whether information is 'private' – linked to an extent to determinations regarding the traditional media - could potentially play a part in inhibiting the creation of tort liability in respect of some disclosures of private information online, depending on the precise situation. In so far as that is the case, the GDPR/DPA would provide the more appropriate cause of action for some privacy claimants.

Contrasts between remedial relief and regulatory aspects of the two schemes: influence on design

The lack of injunctive relief under the DPA 1998, also the case – at face value - under the GDPR/DPA, but its availability under the tort, meant on the one hand post-2000 that the tort offered a more effective response to privacy-invasion,⁴¹ but on the other that the prospect of

³⁹ In *Townsend v Google Inc & Google UK Ltd* [2017] NIQB 81 the plaintiff made a request for Google Inc. to de-list seven of the 12 previously notified URLs because they indicated that he was a sex offender. The judge found that the tort could potentially apply but on the facts no reasonable expectation of privacy was found [31]-[32]; the claim also failed under the DPA 1998 [36]: see text to n 184 below. In contrast, in *Mosley v Google* [2015] EWHC 59 (QB) the High Court ruled that Max Mosley's claim under the tort against Google in respect of links to private information would not succeed, without explaining why that would be the case, but found that he had a viable claim against Google under the DPA 1998, s 10, [55].

⁴⁰ [2014] EWHC 13 (QB) 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 [3]; it therefore concerned an instance of potential disclosure of private information.

⁴¹ Clearly, such relief may be fairly hard to utilise in practice in relation to online disclosures of private information, especially relevant in the *traditional media* context. See eg: K. Yoshida, 'Privacy injunctions in the internet age – PJS' (2016) 4 *European Human Rights Law Review* 434; G. Phillipson, 'Max Mosley goes to Strasbourg: Article 8, claimant notification and interim injunctions' (2009) 1(1) *Journal of Media Law* 73; C. Hunt, 'Strasbourg on Privacy Injunctions' (2011) 70(3) *Cambridge Law Journal* 489. Awards of injunctions are now rare: three of the proceedings (of five) for a new interim injunction at the High Court in January-June 2020 were granted. In the previous six months (July-December 2019) six new interim privacy injunction proceedings took place, and all of these were granted. See 'Civil Justice Statistics Quarterly: April to June 2020' (*Ministry of*

prior restraint engendered some caution in judges in determining its parameters. Such caution did not, however, encourage a reliance by courts on data protection, as opposed to the tort.⁴² The regulatory aspects of both regimes tended in the same direction, in the sense of providing a greater incentive to turn to the courts where the tortious claim was against the press: the Information Commissioner had significant powers to fine data controllers,⁴³ which have now been enhanced,⁴⁴ while the regulatory aspect of the tort regime was and is significantly weaker and of more limited application. Previously operated by the toothless Press Complaints Commission, it now relies on the privacy code policed by the Independent Press Standards Organisation (IPSO),⁴⁵ with statutory recognition.⁴⁶ Judicial awareness of the weakness of press self-regulation as a means of protecting privacy appears to have had an influence on the genesis of the tort, and on its subsequent design, although signs of caution are still apparent. Thus, a determination to rein in the power of the traditional media to invade privacy, and yet a concern to protect media freedom, runs through the earlier jurisprudence establishing the test for ‘private’ information. The specific tests that emerged to establish liability under the tort⁴⁷ were, therefore, largely designed to target the behaviour of the traditional media, especially newspapers; as Rowbottom puts it, the tort was ‘forged’ with traditional mass-media actors in mind,⁴⁸ as exemplified in the seminal case of *Campbell v MGN* in 2004, between Naomi Campbell and the *Daily Mirror*, which named the new tort.⁴⁹ This variation in remedial relief and in regulation may partly explain the preference, until

Justice, 2020) at <https://www.gov.uk/government/publications/civil-justice-statistics-quarterly-april-to-june-2020/civil-justice-statistics-quarterly-april-to-june-2020#privacy-injunctions4> (accessed ~~8 October 20~~ ~~November~~ 2021~~9~~).

⁴² See n 5.

⁴³ They arose under ss 55A-55E DPA 1998. The powers now arise under the DPA 2018, Parts 5 and 6, and Schedules 12-16. See also GDPR, Article 51.

⁴⁴ See DPA 2018, s 157 and GDPR, Article 83(5)(b), providing for ‘administrative fines of up to 20,000,000 Euros, or, in the case of an undertaking, up to 4 % of the total worldwide annual turnover...’. But there is some evidence that these powers are currently under-used: see M. Burgess, ‘MPs slam UK data regulator for failing to protect people’s rights’ (*Wired*, 2020) at <https://www.wired.co.uk/article/ico-data-protection-gdpr-enforcement> (accessed ~~8 October 24~~ ~~December~~ 2021~~9~~).

⁴⁵ See (<https://www.ipso.co.uk/editors-code-of-practice>, accessed ~~8 October 24~~ ~~December~~ 2021~~9~~). For discussion, see P. Wragg, *A Free and Regulated Press: Defending Coercive Independent Press Regulation* (Oxford: Hart 2020). The privacy aspects of the Code monitored by OFCOM for broadcasting are also relevant as representing a further part of the regulatory regimes for press and broadcasting operating alongside the tort.

⁴⁶ See text to n 128.

⁴⁷ The Court of Appeal in *Google Inc v Judith Vidal – Hall* [2015] EMLR 15, [2015] EWCA Civ 311 recently confirmed that the action takes the form of a tort. See J.Y.C. Mo, ‘Misuse of private information as a tort: The implications of *Google v Judith Vidal – Hall*’ (2017) 33 *Computer Law and Security Review* 87.

⁴⁸ 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, 187.

⁴⁹ *Campbell v MGN Ltd* [2004] 2 AC 457 at [14] (Lord Nicholls). It was found that in light of courts’ obligations under the Human Rights Act 1998 s 6, there is an English action against unauthorised disclosure of private information which should be referred to as the tort of ‘misuse of private information’ – also at [14].

recently, for relying on the tort rather than the DPA 1998, resulting in a richer tort-related, but also largely press-focused, privacy jurisprudence.

Determining that information is ‘private’ under the tort: a traditional media-focused design?

In *Campbell*, the House of Lords focused, not on the confidentiality of the personal information in question, but on the invasion of privacy in Article 8 terms its publication represented,⁵⁰ leading Rowbottom to find that the Lords had moved from a confidence-based discussion to a human rights assessment, focusing upon autonomy and dignity.⁵¹ Subsequent developments in the design of the tort, however, saw it depart from that focus, diluting the human rights’ assessment via degrees of absorption of traditional media interests, taking account of the somewhat symbiotic relationship celebrities often have with the press. Since the tort emerged due to a re-contouring of the breach of confidence doctrine based on the courts’ duty under section 6 HRA to abide by the European Convention on Human Rights, it might have been expected that Article 8, with its accompanying jurisprudence, would form the primary focus.⁵² While that jurisprudence has clearly had a bearing,⁵³ the interpretation of the key domestic test as to a ‘reasonable expectation of privacy’, which has in effect become a ‘reasonable sensitivities’ test,⁵⁴ has become largely dependent on the development of a number of traditional media-focused sub-tests: the precise relationship between satisfying these convoluted and cumbersome tests and showing the engagement of Article 8 was initially left largely unarticulated.⁵⁵ They include: consideration of the attributes of the claimant, the activity in question, and the place at which it was happening, the nature and purpose of the intrusion, the location of the photographs (if photographs are involved), the absence of consent, the effect of publication on the claimant, and the circumstances in which and the purposes for which the information came into the hands of the publisher.⁵⁶

⁵⁰ See further: Rowbottom n 48; G. Phillipson, ‘Transforming breach of confidence? Towards a common law right of privacy under the Human Rights Act’ (2003) 66 MLR 726; S. Deakin, A. Johnson and B. Markesinis, *Tort Law* (6th ed, Oxford: OUP 2012) 844.

⁵¹ Rowbottom, *ibid*, 171.

⁵² Under the Human Rights Act 1998, s 2.

⁵³ See, in particular, *McKennitt v Ash* [2006] EWCA Civ 1714 at [37-49].

⁵⁴ See *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457 at [134-142, per Baroness Hale] as regards the test. It evolved into asking what “a reasonable person of ordinary sensibilities would feel [in all the circumstances] if he or she was placed in the same position as the claimant and faced the same publicity:” *Terry and persons unknown* [2010] EWHC 119 (QB) [55].

⁵⁵ The Strasbourg Court, however, later began to incorporate similar tests into the relevant jurisprudence; see *Von Hannover v Germany (No.2)* App nos 40660/08 and 60641/08 (ECHR, 7 February 2012).

⁵⁶ See: *David Murray v Express Newspapers* [2007] EWHC 1908 (Ch) and [2008] EWCA Civ. 446 at [24], [36], [52]; *Terry (previously “LNS”) v Persons Unknown* [2010] EWHC 119 (QB) [55]; *Weller v Associated*

From the tort's very inception, therefore, judges began demonstrating a concern to adopt a cautious stance in relation to (traditional) media freedom, a concern which had previously appeared to preclude – for the most part – the transformation of breach of confidence into a tort of misuse of private information.⁵⁷ It appears that some judges had in mind the desirability of creating an inbuilt leeway at this first stage of a privacy analysis which would aid in giving credence to a finding at the second one (discussed below) that the privacy claim was too 'weak' to overcome the media one.⁵⁸ That may in part explain why the domestic judges, while paying lip service to recontouring the tort with the Strasbourg jurisprudence in mind,⁵⁹ have not absorbed the *Von Hannover*⁶⁰ principle of covering *all* information related to an adult's private/daily life into domestic law:⁶¹ had they done so, some privacy claims would almost inevitably have prevailed since virtually no free speech-based justification would have been available at the next stage of the argument, as the Strasbourg Court found in that instance.

A ready fit between these factors, developed to determine that information is 'private', but clearly created mainly with the traditional media, and its relationship with celebrities in mind, is not apparent in respect of most disclosures of personal information online by individuals⁶² or made possible by intermediaries. Therefore mismatches or misalignments potentially could arise if those factors were applied to such online privacy invasion. For example, the locational factor may be hard to evaluate or may be merely irrelevant, as in *CG v Facebook*

Newspapers Ltd [2015] EWCA 1176; first instance: [2014] EWHC 1163 (QB), [2014] EMLR 24 [16 onwards]; *ETK v NGN* [2011] Civ 439 [10]. This range of considerations was affirmed in 2018 in *Sir Cliff Richard OBE v (1) The British Broadcasting Corporation (2) South Yorkshire Police* [2018] EWHC 1837 (HC) at [276], where the Court also made reference to the ECtHR case of *Axel Springer AG v Germany* App no 39954/08 (ECHR, 7 February 2012) [89-95] which includes analysis of the above factors.

⁵⁷ See G. Phillipson and H. Fenwick, 'Breach of Confidence as a Privacy Remedy in the Human Rights Act Era' (2000) 63 MLR 660.

⁵⁸ That occurred in the cases of both *Terry* (previously "*LNS*" v *Persons Unknown* [2010] EWHC 119 (QB)) and *Ferdinand v MGN* [2011] EWHC 2454 (QB): the information in both instances concerned romantic and sexual relationships; therefore it was of an intimate quality and would obviously have been viewed as information relating to private life under Article 8(1). In both instances the judges were hesitant in finding that a reasonable expectation of privacy arose, indicating that, although it did, the test was only satisfied in quite a borderline fashion; in both the court went on to find that due to the findings as to the balancing act between the media and privacy interests at stake, the claims failed.

⁵⁹ See *McKennitt v Ash* [2006] EWCA CIV 1714 at [8-11] on accepting such re-contouring.

⁶⁰ App no 59320/00 (ECHR, 24 September 2004) at [13]. While it was accepted in *McKennitt* *ibid* that the tort should absorb the relevant Strasbourg Article 8 jurisprudence, the decision stopped short of accepting that all details relating to daily life would attract a 'reasonable expectation of privacy'.

⁶¹ See *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457 at [154]: Baroness Hale found that an unconsented-to photograph of Naomi Campbell popping out to buy milk would not count as 'private' information.

⁶² See eg *AMP v Persons Unknown* [2011] EWHC 3454.

Ireland Limited and McCloskey (Joseph),⁶³ as may the matter of consent, where, for example, the claimant herself had originally played a part in uploading personal material to a platform such as Facebook, aimed at a small number of friends, but where she did not consent to its wider dissemination. The factors concerning the ‘nature of the intrusion’ and use of photographs were clearly devised with the journalistic practice of covert photography in mind, again often a problematic factor to apply in the online domain.

The personal, but apparently innocuous, information at stake in *Von Hannover*⁶⁴ is not covered domestically as regards *adults* under the ‘reasonable expectation’ test,⁶⁵ contrary to the impact of sections 6 and 2 HRA combined, and to the finding in *McKennitt v Ash* to the effect that the courts should absorb the Strasbourg jurisprudence into the common law to shape the tort.⁶⁶ In that respect the notion of private information under the tort is not fully in line with the more expansive conception under Article 8, and also contrasts strongly with the stance taken under the GDPR – below - which, unsurprisingly, shows a more ready tailoring to online privacy protection.

‘Personal data’ under the GDPR/DPA: the broadest possible conception of ‘personal information’

On its face, the contrast between the idea of private information under the GDPR/DPA and the cumbersome test of establishing a ‘reasonable expectation of privacy’ could hardly be more stark. The GDPR/DPA relies on a far more transparent, and much lower, threshold requirement; information must amount to ‘personal data’ relating to the individual person in question. Article 4(1) GDPR categorises personal data as ‘*any* information relating to an identified or identifiable natural person (‘data subject’);⁶⁷ an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier, and an

⁶³ [2015] NIQB 11.

⁶⁴ *Von Hannover v Germany*, App no 59320/00 (ECHR, 24 September 2004) at [13]; e.g., shopping trips were covered, at [13] since the judgment found that a number of activities in public places could still be deemed to be private; see also n 75.

⁶⁵ Innocuous daily life activities engaged in by *children* appear to be covered; see: *David Murray v Express Newspapers* [2007] EWHC 1908 (Ch) and [2008] EWCA Civ 446; *Weller v Associated Newspapers Ltd* [2015] EWCA 1176; first instance: [2014] EWHC 1163 (QB); [2014] EMLR 24.

⁶⁶ [2006] EWCA CIV 1714 [8-11].

⁶⁷ Under the DPA 2018 s 4(2), (5) the GDPR’s definition applies to processing under the Act.

extensive range of identification modes are listed.⁶⁸ It is immediately apparent that there is *no* definition of the term ‘personal’ under the GDPR, echoing the stance under the 1995 Directive;⁶⁹ it is only necessary that the information is *capable* of relating to an identifiable natural person and does so relate. Matters therefore that can be classed as personal data are apparently without limit, subject to that *one* requirement: the emphasis is, in contrast to the emphasis of the test under the tort, not on the *nature* of the information but on the means of identifying a ‘natural person’ that it relates to, thereby excluding, for example, a robot or a company.⁷⁰ In contrast to the test under the tort, sensitivities of the data subject as regards the information, or their basis for seeking erasure, are irrelevant for Article 4(1) purposes, although the GDPR also recognises the category of ‘sensitive personal data’, requiring further protection.⁷¹

One caveat to the above, however, arises in the sense that there appears to be a disconnect between this concept of ‘personal data’ and the necessity that it is being ‘processed’; if it is not being ‘processed’ under the GDPR definition of processing⁷² it does not attain the status of being ‘personal data’. Verbal communication, whether via a phone or face to face, does not, according to a recent ruling under the previous data protection regime,⁷³ count as ‘processing’, even where, aside from that limitation, the data would clearly count as ‘personal’. Since this article is concerned mainly with online disclosures that limitation is not of significance for its purposes, but questions could be raised as to its basis, given that in *this* respect the scheme may not be coterminous with Article 8 ECHR, and possibly of narrower

⁶⁸ They include under Article 4(1): ‘a name, an identification number, location data [including GPRS data], an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’. The new scheme provides a more contemporary, technology-based account by including the notion of an ‘online identifier’ as evidence which could render data personal, demonstrating the acceptance of the EU Commission that technology had evolved to a stage where it is common to trace an internet user by utilising their IP address. See D. Brennan, ‘GDPR series: personal data – an expanding concept’ (2016) *Privacy & Data Protection* 12, 13. Also see Case C-582/14 *Breyer v Germany* [2016] (ECJ) ECLI:EU:C:2016:779, at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582> (accessed ~~8 October~~ ~~13 November~~ 2021¹⁰). Recital 26 of the GDPR provides elaboration as to the requirement of identifying a natural person: ‘account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly’.

⁶⁹ Directive 95/46/EC. See: M.J. Taylor, ‘Data Protection: Too Personal to Protect?’ (2006) 3(1) *SCRIPT-ed* 72, 75; P. De Hert and V. Papakonstantinou, ‘The proposed Data Protection Regulation replacing Directive 95/46/EC: a sound system for the protection of individuals’ (2012) 28(2) *Computer Law & Security Review* 130, 183.

⁷⁰ In that respect the ambit of Article 8(1) could be broader than the ambit of ‘personal data’ under the GDPR; in *Societe Colas Est v France* (2002) App No 37971/97 at [41] it was found that a company could have a right to respect for its private life under the Article, but that instance only concerned a physical search of the premises.

⁷¹ GDPR Article 9; Recitals 51-56; for definitions, see Article 4(13),(14),(15).

⁷² See Article 4(2).

⁷³ *Scott v LGBT Foundation* [2020] EWHC 483 (QB) [55].

scope than the tort. Further, certain instantaneous communications immediately deleted, connected to an identifiable person online, and hosted by, for example, Snapchat⁷⁴ would count as ‘personal data’ despite being quite closely cognate to offline verbal communication.

Apart from the matter of verbal communication, this account of ‘personal data’ under the GDPR, relying *only* on the connection of information to an identifiable person, clearly covers, but goes beyond, information relating to ‘private or family life’, ‘the home or correspondence’, the terms used in Article 8(1) ECHR. It covers matters that under Article 8 would not be deemed ‘private’ because it entirely disregards the distinction introduced in *Von Hannover* by the Strasbourg Court between a person’s public and private life, a distinction obviously of most relevance to celebrities and other well-known figures.⁷⁵ Thus the Princess of Monaco’s (the claimant in *Von Hannover*) public life duties, such as opening a new civic building, would be covered under Article 4(1) of the GDPR, but not under Article 8(1) ECHR, while her daily/private life activities would be covered under Article 8,⁷⁶ but not under the tort.⁷⁷ But for the purposes of covering information that would *in reality* be likely to be the subject of erasure requests or compensation, it is the area of convergence between Article 4(1)’s account of personal data and the area of private life-linked information covered by Article 8(1) that is significant, an area that is currently of greater breadth than the area covered by the tort.

Implications of the narrower conception of ‘private information’ under the tort

The explanation for the difference between the tort and GDPR in respect of information that counts as ‘private’ clearly lies in the origins and objectives of the two schemes. Given the nature of the general scheme under the GDPR/DPA, intended *inter alia* to enable control of the processing of personal data by the tech companies⁷⁸ as well as state bodies, including data

⁷⁴ Snapchat, accessible at <https://www.snapchat.com/> (accessed ~~8 October 23~~ ~~November 2021~~ 10). The communications can be retrieved. It is possible to ‘screenshot’ images received and therefore save them onto mobile devices, but the sender is notified.

⁷⁵ In *Niemietz v Germany* (1993) 16 EHRR 97, the Strasbourg Court stated: ‘The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of “private life”,’ at [29]; but the examples of personal information from *Von Hannover* [2004] EMLR 21 – shopping trips, at [13], eating in a restaurant, at [11] – and from *Von Hannover v Germany (no 2)* [2012] EMLR 16 concerning a skiing trip, at [17], were the result of the Court’s delineation under Article 8(1) of the outer limits of the ‘private life’ of a public figure, as opposed to their ‘public life’-linked information.

⁷⁶ *ibid*, [2004] EMLR 21.

⁷⁷ See n 61.

⁷⁸ See n 17.

that might have significance on various bases in the future, including economic ones, its adoption of an account that relies only on contrasting humans with non-human entities is unsurprising. It obviously had no need to carry the traditional media-related baggage associated until recently with the test devised under the tort, and it therefore relates more closely to the core value of informational autonomy.

As discussed above, the Strasbourg Article 8 jurisprudence is relevant to the application of the GDPR in conformity with Article 8 of the EU Charter, while the tort has also been interpreted, to an extent, in conformity with Article 8 ECHR, under the HRA. The type of information that is significant in terms of protecting privacy online clearly often differs from information mainly relating to celebrities that has frequently been at issue under the tort until recently. In particular, information relating to non-celebrities as to previous spent convictions or more controversial previous appointments accessible via a search engine,⁷⁹ social media platform or website, could have an impact on a person's work and/or family life. Such 'public life' information would clearly fall within Article 4(1) and could also receive added protection.⁸⁰ It would probably also fall within Article 8(1), since the public life/private life distinction from *Von Hannover* would tend not to apply to online privacy-intrusion pertaining to the 'public life' information⁸¹ of *private* or semi-public figures, bringing them more readily within Article 8(1) at Strasbourg. But it would now *also* fall within the ambit of the tort, following a number of online decisions involving intermediaries, including *NT1 and NT2 v Google*, depending in some circumstances on the impact availability of the information could

⁷⁹ Much of the information in the following instance was of that nature, and concerned private or semi-public figures: in *GC, AF, BH, and ED v Commission nationale de l'informatique et de Libertes (CNIL), Premier ministre, and Google LLC* 24 September 2019 AF wanted search results removed identifying him as previously holding a post as a public relations officer for the Church of Scientology. BH requested deindexing of articles linking him to contemporaneous investigations into the funding of political parties. ED requested such de-indexing to mentions of a prison sentence of seven years and ten years judicial supervision for sexual assaults on children under 15. All the requests had been denied. GC had requested domestically that a link to a satirical photomontage depicting her in an illicit relationship with a politician should be removed from search returns. The links included special categories of personal data (now covered by Article 9 GDPR). In a preliminary ruling the Court found that the prohibition imposed on other controllers of processing data caught by Article 8(1) and (5) of Directive 95/46 (previously covering special categories of data), subject to the exceptions laid down there, would also apply to the search engine. In the face of this ruling one possibility is that Google seeks to rely on Article 85 GDPR; see text to n 155.

⁸⁰ If previous employment revealed political opinions, religious or philosophical beliefs it could count as sensitive personal data under Article 9 GDPR; criminal convictions would fall within Article 10 (see s10(5) DPA 2018).

⁸¹ In *M.L. and W.W. v. Germany* (application nos. 60798/10 and 65599/10) judgment of 28th June 2018 information as to the applicants' previous convictions was made available on a website run by a radio station; the Court accepted that the information counted as 'private' under Article 8(1) but did not disturb the conclusions reached domestically: in the balancing of the Article 8 and 10 interests at stake the domestic court had found that the Article 10 interest prevailed.

have on the claimant's family, as well as private, life.⁸² The requirement under the tort test, following *Von Hannover*, that the information relates to an individual's private/daily life, as opposed to their public one, but *also* has some added sensitivity,⁸³ clearly does *not* render it inapplicable to information relating to previous convictions, available online via search engines or otherwise. That might also be found to apply in future to other past life information of sensitivity to the claimant available on or offline. The courts clearly are *not* currently struggling to apply the 'reasonable expectation of privacy' test in the online context, to individuals, but also intermediaries.

But that added requirement of sensitivity *does* currently preclude reliance on the tort in relation to apparently innocuous private life information relating to public, and probably, private figures, whereas such information would be covered under both Article 4(1) and Article 8. The current conception of private information under the tort therefore renders it inapplicable, as currently interpreted, to a range of information posted or accessible online, related to private/daily life. Apparently innocuous information such as, for example, images posted on social media of a private figure drinking in a bar, might – albeit not as a necessary requirement – have sensitivity for that person due, for example, to their religious background, but it is not clear that it would count as private information under the tort, although it would obviously fall within Article 4(1) GDPR, and probably within Article 8 ECHR.

A reconfiguring therefore of the 'reasonable expectation of privacy' test, re-evaluating the basis and value of the factors discussed, to create a somewhat better fit with the online context, may eventually find a place within the jurisprudence. Given the volume of personal information online, including browsing data, that may be misused without consent, the likelihood of claims arising under both the tort and GDPR is increasing, and this article considers a number of very recent instances, arising under the previous data protection regime.⁸⁴ In future, where the tort potentially applies in the online context, especially where the claim is brought by a private figure against a private actor, pressure might be placed increasingly on courts to re-evaluate the tort test for private information, in terms of re-

⁸² See *NT1 and NT2 v Google LLC* (n 16). It was found as regards NT1 that he had no reasonable expectation of privacy: the information regarding his previous convictions was found to be 'public' information [171]; in contrast, NT2 was found to have such an expectation [224], mainly due to the impact that the availability of the information could have on his family life since he had young children [226]. See further text to n 212. See also *CG v Facebook Ireland Limited and McCloskey (Joseph)* Neutral Citation No. NICA 54; [2015] NIQB 11.

⁸³ See n 61.

⁸⁴ See in particular n 16 and n 213.

thinking the requirement of added sensitivity,⁸⁵ in order to enhance the efficacy of the tort in that context, and ensure compatibility with Article 8 ECHR.

Finally fully discarding the public domain doctrine under the tort in the digital era?

Design and (current) decline of the tortious 'public domain' doctrine

It has in the past been the case that a further hurdle must be overcome to establish a 'reasonable expectation of privacy' under the tort: the notion of 'public domain' has evolved in the jurisprudence, mainly with the traditional media in mind, as a potential bar to finding that the expectation exists.⁸⁶ The doctrine would be particularly problematic in relation to protecting privacy online, *but for* its recent decline in significance, prompted by the increase in online disclosures. The doctrine traditionally stated that if the personal information is already known to the public (to an extent that a court deemed significant) then the information has lost its private quality and so should no longer be protected.⁸⁷ Butler finds that the doctrine clearly derives from the 'all or nothing' analysis in breach of confidence actions,⁸⁸ while Wragg observes that a heavy reliance on the doctrine in the tortious context would align the tort more closely with such actions.⁸⁹ Such concerns, however, are to an extent misplaced: even in judgments prior to, or following closely on, the process of transformation of breach of confidence into the tort,⁹⁰ the doctrine was *not* applied in an absolutist fashion.⁹¹

⁸⁵ That requirement can be traced back to Baroness Hale's comment in *Campbell* to the effect that a photograph of the claimant merely shopping would not count as private information (see n 61). However, the comment was technically only obiter, and was made prior to the findings as to daily life private information in *Von Hannover* [2004] EMLR 21 (n 75). The example given above of images posted online without consent of an individual drinking in a bar would not necessarily have added sensitivity, unless, for example, he/she had claimed to be a reformed alcoholic.

⁸⁶ See *Douglas v Hello! III* [2005] EWCA Civ 595, [2006] QB 125 at [105]: 'In general...once information is in the public domain, it will no longer be...entitled to the protection of the law of confidence...The same may generally be true of private information of a personal nature'.

⁸⁷ For example, the focus of the court in *Terry and persons unknown* [2010] EWHC 119 (QB) and *Ferdinand v MGN* [2011] EWHC 2454 (QB) was on the number of people to whom the claimants had disclosed their affairs/the number who were aware of them. Given the relatively low numbers in question, the information was not found to be in the public domain. See for the previous position under the doctrine of confidence: *Attorney General v Guardian Newspapers Ltd (No 2)* (1990) 1 AC 109.

⁸⁸ Simplistically, the information either is or is not found to be confidential: O. Butler, 'Confidentiality and Intrusion: building storm defences rather than trying to hold back the tide' (2016) *The Cambridge Law Journal* 452, 453.

⁸⁹ P. Wragg, 'Privacy and the emergent intrusion doctrine' (2017) 9(1) *Journal of Media Law* 14, 17.

⁹⁰ See *Attorney General v Guardian Newspapers Ltd (No2)* (1990) 1 AC 109 which found that a small amount of disclosure of the information would not destroy its confidential quality. In *Douglas and Zeta Jones and ors v Hello!* [2001] 2 All ER 289 the fact that a large number of guests had observed the appearance of the couple at

Nevertheless, the doctrine has not yet been *entirely* discarded, and reliance on it as traditionally understood could clearly work to negate a tortious claim in respect of information disclosed online.⁹² The potential for the rapid and widespread dissemination of personal information online clearly sits uneasily with some of the references to public domain in the earlier tort jurisprudence, which has focused mainly on persons who happened to be in a public place at the time. Finding that disclosure to small numbers who happened to be present would not negate the private quality of the information⁹³ could readily be taken to imply conversely that more *widespread* dissemination of the information online *would* do so.

Lack of doctrinal 'fit' especially in the online context

Judgments under the tort before the judgment of the Supreme Court in *PJS* (discussed below),⁹⁴ concerned mainly or partly with disclosures online, have to an extent followed the trends apparent from the offline case-law in seeking to determine whether an element of privacy still exists despite prior online publication. But some unarticulated awareness of the difficulty and inaptness of applying the public domain doctrine in that context has been apparent.⁹⁵ In *Martin and Ors* publication to a private Facebook account (where viewers were controlled) was not found to have placed the information in the public domain,⁹⁶ whereas in *Rocknroll v NGN* the focus was on both intrusion and the degree of disclosure:⁹⁷ the initial

the wedding did not preclude the finding that the information remained confidential/private. Similarly, in *Browne v Assoc Newspapers* [2008] QB 103 information disseminated to a circle of family and friends was distinguished from its publication in a newspaper.

⁹¹ There has also been a reluctance to allow the newspaper in question to take advantage of its own disclosure of the information: widespread disclosure of the information in that circumstance was not deemed to create a bar to establishing the reasonable expectation in *Max Mosley v News Group Newspapers Limited* [2008] EWHC 1777 (QB).

⁹² That may explain the decision in *Mosley v Google* [2015] EWHC 59 (QB). The High Court ruled that Max Mosley had a viable claim against Google, at [55], under the data protection scheme, but not under the tort, in respect of links created by Google to sexually explicit information concerning Mosley.

⁹³ See in particular: *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457; *David Murray v Express Newspapers* [2007] EWHC 1908 (Ch) and [2008] EWCA Civ. 446. At Strasbourg, see: *Peck v United Kingdom* App no 44647/98 (ECHR, 28 January 2003); *Von Hannover v Germany*, App no 59320/00 (ECHR, 24 September 2004). Also see P. Wragg, 'Privacy and the emergent intrusion doctrine' (2017) 9(1) *Journal of Media Law* 14, 16.

⁹⁴ *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] UKSC 26.

⁹⁵ In *AMP v Persons Unknown* [2011] EWHC 3454 the intimate images of the claimant were uploaded to a free online media hosting service for the sharing of images. They were then also uploaded to a Swedish site hosting BitTorrent files; they had clearly been viewed by a large number of persons, but the public domain issue did not feature in the decision that a reasonable expectation of privacy arose.

⁹⁶ *Robert Gordon Martin and Heather Elaine Martin and Ors v Gabrielle Giambrone P/A Giambrone & Law, Solicitors and European Lawyers* [2013] NIQB 48.

⁹⁷ *Rocknroll v News Group Newspapers Ltd* [2013] EWHC 24 (Ch), at [20]-[25].

post was to a friend's private Facebook account and, until changes in the privacy settings, it could be viewed by his approximately 1500 friends, but not by the general public; no internet search would have located it. It was determined that there was still something private left to protect despite the reposting of the information to the more public platform, since its publication in a national newspaper – which had acquired the photographs from the Facebook posting – was found to be likely to create a greater intrusion on the claimant's privacy. A somewhat similar stance, but *purely* in the online context, was taken in *CG v Facebook Ireland Limited and McCloskey (Joseph)*⁹⁸ in which a photograph of the claimant and information about his past as a sex offender were posted on Facebook pages, attracting there very hostile comments. Although the previous court case had been reported on, and the pages could be accessed by a large number of persons since privacy settings were not imposed, a reasonable expectation of privacy *was* found to arise, and the judges appeared to accept on appeal – although this was not clearly articulated – that the material need not be viewed as being in the public domain.⁹⁹

The lack of 'fit' between the doctrine and the likelihood of disclosures of personal information online in the digital era has more clearly led to its erosion as a result of the Supreme Court's decision in *PJS*.¹⁰⁰ The case, which concerned a celebrity couple's engagement in extra-marital sex, effected a clear departure from reliance on the traditional public domain analysis. The Supreme Court was concerned with reinstating the injunction,¹⁰¹ but the findings would *also* apply to the 'reasonable expectation' test. The information in question was deemed to retain a 'private' quality:¹⁰² the doctrine was *not* found to preclude finding that the information retained its ability to create intrusion, despite its very widespread

⁹⁸ [2015] NIQB 11.

⁹⁹ *CG v Facebook* [2016] NICA 54. Hugh Tomlinson QC submitted on behalf of the claimant, referring only to the *reporting* of the case: 'In any event it is clear that information which is in the public domain can, through the passage of time, recede into the past and become part of a person's private life' [30], and this appeared to be accepted by the court. In *Reachlocal UK Ltd v Bennett and Ors and Mason v Huddersfield Giants Ltd* [2013] EWHC 2869 (QB), concerning claims in defamation and confidence from a company, the issue was not clearly dealt with, but the court did not appear to consider that 'tweets' viewed by thousands should be considered to be in the public domain for the purposes of the confidence claim.

¹⁰⁰ *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] UKSC 26.

¹⁰¹ It had already been accepted that, despite the widespread disclosure of the information, it retained its quality of being 'private'. The Court reinstated the claimant's interim injunction: *ibid* at [71] (Lord Neuberger).

¹⁰² That was although it had been the subject of several articles outside the jurisdiction and had been widely disseminated online in the US, Scotland and Canada. There was an abundance of US reportage on the rumours and on the subsequent judgements. See, for example, a US article concerning the case on a website, 'Pop Goes the News' (19 May 2016), which deployed a disclaimer stating that the blog was not bound by the injunction since it was confined to the English and Welsh jurisdiction, at <https://popgoesthenews.com/2016/05/19/uk-supreme-court-upholds-ban> (accessed 18 October 2021).

disclosure on and offline in a number of jurisdictions. Rather than focussing mainly on the *extent* of its dissemination, the Court considered the further *harm*, in terms of intrusiveness, that would arise due to its further publication in the English and Welsh press,¹⁰³ bearing in mind the ‘greater influence, credibility and reach, as well as greater potential for intrusion of revelations in the press as compared with the internet...’.¹⁰⁴ That contention was doubted by Lord Toulson who argued that the Law Lords should not be seen as ‘out of touch with reality’ since the ‘world of public information is interactive and indivisible’,¹⁰⁵ but it formed part of the ratio of the judgment,¹⁰⁶ which undeniably represented a shift in the stance taken by the domestic courts to the public domain doctrine, of particular significance in relation to protection for privacy online.¹⁰⁷ Butler finds that the ‘shift from confidentiality or secrecy to intrusion permitted the court to move from a rather abstract notion of the “public domain” to a more concrete notion of the *harms* that disclosure in a particular location and medium would do to the claimant and his family.’¹⁰⁸ That is also the position under the GDPR, but it is only relevant at the stage of considering competing freedom of expression and information claims, *not* at the stage of identifying ‘personal data’.¹⁰⁹

Entirely abandoning the ‘public domain’ notion: remaining differences between the tort and GDPR?

¹⁰³ n 94, at [68] (Lord Neuberger).

¹⁰⁴ *ibid* at [69] (Lord Neuberger); see further Butler n 88, 454.

¹⁰⁵ *PJS* n 94, at [89].

¹⁰⁶ *ibid* at [88] and [89] respectively.

¹⁰⁷ The intimate nature of the information may also have played a part – intimacy may in general have the ability to persuade courts to take a generous view of the public domain notion on the basis, it appears, that the greater its intimate quality, the more likely it is that a court would find that harm has been and would be caused by its disclosure, the situation in *PJS*. Information already to an extent in the public domain, but of a particularly intimate nature (in one case, consisting of a sex tape: *Contostavlos v Mendahun* [2012] EWHC 850) can still attract liability. See K. Hughes, ‘Publishing Photographs Without Consent’ (2014) 6(2) *Journal of Media Law* 180. Mead has suggested that the focus on intrusion may also imply that the more intimate the information the greater the harm that might be expected to arise from its disclosure in a particular medium or location, bearing in mind the intimate nature of the information at stake in *PJS*, but the Supreme Court did not expressly advert to that possibility. The information in *PJS*, relating to sexual trysts, was inherently private in nature: see D. Mead, ‘A socialised conceptualisation of individual privacy: a theoretical and empirical study of the notion of the “public” in MoPI cases’ (2017) 9(1) *Journal of Media Law* 100, 126.

¹⁰⁸ Butler n 88, 453 [emphasis added].

¹⁰⁹ That stance was adopted in the *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*, adopted by the European Data Protection Board on 7 July 2020: ‘The rights of the data subjects will prevail, in general (referring to COJ, Case C-131/12, judgment of 13 May 2014, paragraph 99; COJ, Case C-136/17, judgment of 24 September 2019, paragraph 53) [over] the interest of Internet users in accessing information through the search engine provider’. However, [the Court] identified several factors that may influence such determination ‘[including] the nature of the information or its sensitivity, and especially the interest of Internet users in accessing information’ [48].

There is no express reference to the prior dissemination of the personal data under Article 4(1) GDPR in relation to disclosures of personal information on or offline. Information already widely disclosed still retains the *status* of ‘personal data’, whereas under the tort, as discussed, dissemination of the information was found in the earlier case-law to be able to overcome the expectation of privacy, rendering the information non-private and so precluding the need to balance its private nature against free expression interests. Even after *PJS* that notion may possibly linger on, where publication in the traditional media, as opposed to online publication, is *not* in question. The ruling in *PJS* related to the greater harm that would be done by *press* disclosure, both online and offline, in England and Wales. The *PJS* principle, however, surely demands a focus on the harm that could still be caused by further disclosure, without necessarily demanding that the harm should arise only via *press* disclosure; that has already been accepted, impliedly, in relation to purely online disclosures.¹¹⁰ If, for example, the threat to privacy arose due to named person searches,¹¹¹ or possibly from more popular websites, and/or ones that had, in terms of a reputation for reliability, attained a standing approaching that attributed to newspapers in *PJS*, it would appear that the harm-based principle from that judgment could be found to apply.

It is contended that attempts to apply this doctrine in the online context should now be clearly and definitively abandoned in seeking to identify a ‘reasonable expectation of privacy’. Discussion of degrees of dissemination in that context, involving, for example, seeking to count the number of views of a tweet, approaches the farcical, while the question of the dissemination of the information has now divorced itself so comprehensively from any plausible meaning of the term ‘public’ as to render that term redundant. Reliance on the harm-based principle from *PJS* to find that information retains a claim for protection even where it has already been extensively disclosed online, departing from the stance taken as to online dissemination in *RocknRoll*, would enhance the tort’s ability to protect privacy online effectively. A clearer adoption of such a harm-based test under the tort would still mean that its stance differed from that under the GDPR since the acquisition of the status of ‘personal data’ does *not* depend on considering the harm that disclosures could cause, but it *would*

¹¹⁰ See n 98 and n 211.

¹¹¹ As in Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [2014] WLR 659; in *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2018] EWHC 799 (QB), the Court found: ‘The CJEU was surely right to point out in *Google Spain* that information distribution via [internet search engines] ISEs is inherently different from and more harmful than publication via source websites’ [151]. Clearly, the search could find links to information from various sources, including from online press or broadcasting coverage.

mean that widespread prior disclosure of the information would in the circumstances discussed have no more impact on its ‘private’ quality than it would on its ‘personal’ one under the GDPR.

There is no reference to the prior disclosures of their own personal information by data subjects under the GDPR Article 4(1). Article 17 was also clearly designed to avoid distinguishing between personal data initially disclosed to the controller by the individual it relates to, and data uploaded initially by a third party or the controller. It states that ‘the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay’ where one of a number of grounds applies,¹¹² including the situation in which the data subject ‘withdraws consent on which the processing is based’,¹¹³ which would include instances in which subjects changed their minds after initially disclosing the personal information online themselves.¹¹⁴ As a result, the fact of such initial disclosures by a data subject, or the provision of the specific information at issue by him/her to a third party who discloses it, has no effect on its status as personal data, or mean that the right to erasure ceases to apply.

Conclusions

It is clear from the above that the presence of information in the public domain does not now usually adversely affect the prospects of success under the tort. The notion of taking account of the extent to which the information is already in the public domain is *not* entirely absent from the GDPR/DPA. But that notion *only* arises at the stage of considering competing free speech claims: the data *can* be disclosed if the journalistic ‘exemption’,¹¹⁵ which can cover non-media actors, as discussed below, applies to its processing. The public interest value of the data is relevant in determining whether the ‘exemption’ applies and the Independent Press Standards Organisation’s Editor’s Code (IPSO’s) is relevant to determining whether a public

¹¹² The grounds are set out in Article 17(1) (a)-(f).

¹¹³ Article 17(1)(b); it continues: ‘according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing’.

¹¹⁴ Similarly, DPA 2018, Part 3, Chapter 3, s 47(4) (applying the right to erasure specifically in the law enforcement context) does not differentiate between the persons who initially uploaded the data, sub-section 4 simply stating that ‘a data subject may request the controller to erase personal data or to restrict its processing’.

¹¹⁵ Under DPA 2018 Sched 2 Pt 5 para 26. See pp 00 below for discussion.

interest in the information in question exists;¹¹⁶ so doing includes considering whether the information is in the public domain,¹¹⁷ and/or consideration of the data subject's 'own public disclosures of information'.¹¹⁸ The Code has no legal status,¹¹⁹ and its influence on judicial decisions is, as discussed below, variable, but this aspect of the exemption accords some traction to public domain notions under the DPA, and since IPSO's code is also relevant to public interest arguments under the tort, under section 12(4)(b) HRA, the same point applies. Under the tort the extent to which the information is already publicly known has also become a relevant factor in balancing Article 8 concerns against the demands of Article 10.¹²⁰ The differences between the two causes of action in this respect can be viewed as minimal in the sense that under both the question whether the information was in the public domain, or had previously been disclosed by the claimant, should usually now be relegated to the free expression stage of the argument - below.¹²¹

The speech/privacy 'balancing' acts under the tort and under the GDPR/DPA

Introduction

The so-called speech/privacy 'balancing act' under the tort, undertaken once it has been established that the information in question is private, is conducted as a parallel proportionality analysis under Articles 8(2) and 10(2) ECHR:¹²² each right is seen as creating a potentially justifiable interference with the other one. That balancing act is expected to be conducted in the same way under the GDPR since that was accepted under the previous data

¹¹⁶ See the reference to the 'Editors' Code of Practice' under Data Protection Act 2018, Sched 2, Pt 5, para 26(6)(c); this appears to refer to IPSO's Code of Practice (at <https://www.ipso.co.uk/editors-code-of-practice>, accessed 8 October 2021).

¹¹⁷ IPSO's Code, under 'Public Interest', clause 3 provides: 'The regulator will consider the extent to which material is already in the public domain or will become so'.

¹¹⁸ IPSO's Code clause 2(ii) provides: 'In considering an individual's reasonable expectation of privacy, account will be taken of the complainant's own public disclosures of information....'.

¹¹⁹ It has statutory recognition in the HRA s12(4)(b), and, as indicated, under the DPA 2018 (n 125).

¹²⁰ See n 139.

¹²¹ Their lack of traction at the *privacy* stage is implicit in *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2018] EWHC 799 (QB); it was found in relation to both the tort and the previous data protection scheme: 'The two interviews which NT2 now seeks to delist were given and published with his actual consent. That consent has now been withdrawn' [220]. The information at issue had also been available to a large number of users of Google (unquantified). Nevertheless, NT2 succeeded under both causes of action.

¹²² As found in *Re S (a child)* [2005] 1 AC 593; it was termed the 'ultimate balancing act' [17], per Lord Bingham.

protection regime.¹²³ The GDPR, as discussed above, must also be interpreted and applied in conformity with the EU Charter of Fundamental Rights,¹²⁴ meaning that Article 11 must be balanced against both Articles 8 and 7 of the Charter. Since the interpretation of the Charter relies on the Strasbourg jurisprudence,¹²⁵ the balancing act under the GDPR appears likely to echo the one conducted under the tort, which itself relies on the relevant ‘balancing’ Strasbourg jurisprudence.¹²⁶ It is generally agreed in the academic literature, however, that some of the earlier tort jurisprudence as to conducting the ‘balancing act’ is unsatisfactory since it was largely (not wholly) developed with traditional media rather than purely free speech concerns in mind.¹²⁷ But given the recently increased likelihood of claims against individuals and intermediaries, aimed at protecting privacy online, the discussion will argue for the desirability of a clearer focus on public interest demands, at times involving some departure from the established tort expression jurisprudence when conducting the balancing act under the GDPR/DPA, and indeed under the tort itself, of particular applicability in the online context.

The design of the balancing act under the tort

All aspects of the ‘balancing act’ under the tort have been strongly criticised. The notion of ‘balancing’ has in itself attracted criticism, both for its lack of clarity and for its reliance on a metaphorical reference to weighing scales that does more to obscure than illuminate the exercise apparently being undertaken.¹²⁸ The focus of the exercise has also been found, in

¹²³ See *NT1 and NT2* (n 16) [115]: ‘...the exercise the Court must undertake in this context is an assessment of proportionality (see Morland J in *Campbell v MGN Ltd* [116-117]) involving essentially the same Article 8/Article 10 “ultimate balancing test” as prescribed by *In re S (Murray v Express Newspapers)* [2007] EWHC 1908 [76]’.

¹²⁴ See 2000/C 364/01. *Lindqvist v Aklagarkammaren I Jonkoping* (C-101/01) November 6, 2003 [87].

¹²⁵ See Article 52(3) of the Charter and Case C-400/10 *PUJMcB v LE* [2010] ECLI:EU:2010:582. See also Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [3], and n 132.

¹²⁶ Under the Human Rights Act 1998, ss 2 and 6. See n 137 and n 139.

¹²⁷ See the later ‘footballer cases’, including *Terry and persons unknown* [2010] EWHC 119 (QB) at [55]. The judge adverted to Terry’s portrayal of himself via the media as in some sense ‘reformed’. In *Douglas v Hello!* [2001] 2 All ER 289 the sale of the couple’s privacy (pictures of the wedding) to a different magazine, persuaded the Court that their privacy interest had been down-graded in relation to the rival magazine’s contentions. In *Campbell* (n 49), the House of Lords accepted somewhat uncritically that there was a public interest in correcting the false image Campbell had previously portrayed to the media. See further G. Phillipson, ‘Press freedom, the public interest and privacy’ in A. Kenyon (ed), *Comparative Defamation and Privacy Law* (Cambridge: CUP 2016).

¹²⁸ See: R. Moosavian, ‘A just balance or just imbalance? The role of metaphor in misuse of private information’ (2015) 7(2) *Journal of Media Law* 196, 217: ‘Thus perhaps “balance” acts as a convenient fiction which overlays an inherently creative, subjective and, to some extent, inexpressible interpretive activity...’. Wragg has gone further and argued that the balancing exercise is so vague that it fails to give judges any tools with

some of the earlier cases involving journalism, to have come adrift from the free speech values recognised under Article 10,¹²⁹ appearing to tend to benefit the traditional media actor,¹³⁰ given the range of matters that have been deemed to bear a relationship to the public interest. Contrary pronouncements have emerged from, for example, Lord Hoffmann in *Campbell*, who found that the ‘relatively *anodyne* nature of the additional details [as to Campbell’s drug addiction and treatment] is in my opinion important and distinguishes this case from cases in which....there is a public interest...’.¹³¹ But the range and nature of the matters that the courts have quite frequently somehow found to create a public interest in the private information disclosed¹³² are quite staggering to privacy advocates. At their most highly tabloid-friendly mode, such matters have included the need to enable public debate about possible anti-social conduct,¹³³ and to allow newspapers to print private matters that the public feel some curiosity about, in order to ensure that a range of newspapers stay in business.¹³⁴ Not only have such factors quite often found purchase within the ‘balancing act’ in the earlier case-law, but, as Mead has pointed out, the term ‘public’ interest itself has not always been taken seriously since various *private* interests (such as a lascivious interest in the sex lives of the famous) have been elided with matters deemed to constitute the *public* interest.¹³⁵ The nature of the further linked sub-factors that have been identified also quite often show a traditional media-friendly tendency. Such factors have been found at

which to effect the balance. He similarly argues that the parallel analysis relies upon ‘abstract terms’ focussing on the negative effects on freedom of expression: P. Wragg, ‘Protecting private information of public interest: Campbell’s great promise, unfulfilled’ (2015) 7(2) *Journal of Media Law* 225, 234. Clearly, it can also be argued that a negative impact on privacy could also arise.

¹²⁹ See: E. Barendt, *Freedom of Speech* (2nd ed, Oxford: OUP 2007), F. Schauer, *Free Speech: A Philosophical Enquiry* (Cambridge: CUP 1982); H. Fenwick and G. Phillipson, *Media Freedom Under the Human Rights Act* (Oxford: OUP 2006) at 683 onwards. See also, for example: *Plon (Societe) v France* App no 58148/00 (ECHR, 18 May 2004): significant political speech, although relating to an individual’s private life, was accorded full recognition under Article 10; see also *Campbell v MGN Ltd* [2004] UKHL 22 at [117].

¹³⁰ See G. Phillipson, ‘Press freedom, the public interest and privacy’ in A. Kenyon (ed), *Comparative Defamation and Privacy Law* (Cambridge: CUP 2016). See also n 133.

¹³¹ *Campbell v MGN Ltd* [2004] 2 AC 457 at [60]. Lord Nicholls in that instance similarly found that disseminating information about the claimant’s attendance at Narcotics Anonymous meetings was of a ‘lower order’ than other forms of journalistic speech, such as political speech [*ibid.*, at 29].

¹³² These interpretations created for a period a renegeing on the finding that Articles 8 and 10 have equal value (as found in *Re S* [2004] UKHL 47 at [17], *Campbell ibid.*); findings in *Terry and persons unknown* [2010] EWHC 119 (QB) and *Ferdinand v MGN* [2011] EWHC 2454 (QB) implied that Article 10 may *de facto* take precedence over Article 8; that position was more clearly taken by the Court of Appeal in *PJS v News Group Newspapers* [2016] EWCA Civ 393, a position reminiscent of the English courts’ pre-HRA jurisprudence. But the notion that Article 10 has presumptive priority over Article 8 due to the HRA s 12(4) was eventually put to bed by the Supreme Court in *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] UKSC 26, at [33].

¹³³ *Ferdinand v MGN* [2011] EWHC 2454 (QB) and *Terry and persons unknown* [2010] EWHC 119 (QB).

¹³⁴ *A v B Plc* [2002] 3 WLR 542.

¹³⁵ D. Mead, ‘A socialised conceptualisation of individual privacy: a theoretical and empirical study of the notion of the “public” in MoPI cases’ (2017) 9(1) *Journal of Media Law* 100, 130.

Strasbourg, and then accepted in English cases such as *Weller*,¹³⁶ to include the celebrity or well-known status¹³⁷ of the claimant¹³⁸ and his/her ‘prior conduct’ as carrying weight on the Article 10 side of the balance;¹³⁹ if they are present, the privacy interest may in effect be down-graded. The COJ has echoed that tendency in considering the application of Article 11 of the Charter of Fundamental Rights, guaranteeing freedom of expression, when it is balanced against Articles 7 and 8.¹⁴⁰

The need for a stricter approach to determinations as to the public interest was, however, signalled by the Supreme Court in *PJS*.¹⁴¹ The idea that the public interest could encompass allowing the media to disclose private facts in order to enable debate as to possible anti-social behaviour, one of the broadest possible traditional media-friendly factors envisaged, was finally firmly rejected¹⁴² as a matter that could attract any weight on the Article 10 side of the balance. But a somewhat less weak ‘public interest’ had previously been found to inhere in revealing truths about celebrities’ private information, where they appeared to have misled the public, usually by presenting a false image.¹⁴³ The Supreme Court impliedly accepted the

¹³⁶ *Weller v Associated Newspapers Ltd* [2015] EWCA 1176; first instance: [2014] EWHC 1163 (QB), [2014] EMLR 24.

¹³⁷ See: *Von Hannover v Germany (No.2)* App nos 40660/08 and 60641/08 (ECHR, 7 February 2012) at [108-113]; *Von Hannover v Germany (No.3)* App no 8772/10 (ECHR, 19 September 2013); *Axel Springer AG v Germany* App no 39954/08 (ECHR, 7 February 2012) at [101].

¹³⁸ It was accepted in *Rocknroll v News Group Newspapers Ltd* [2013] EWHC 24 (Ch) at [15] that a person with a role in national affairs would have a reduced expectation of privacy.

¹³⁹ In *Couderc and Hachette Filipacchi Associes v France* App no 40454/07 (GC, 10.11.15), prior conduct was viewed as a guiding principle for the balancing exercise at [93], and further at [130]; the findings implied that prior conduct *would have* been considered as a balancing factor here (it has its own sub-heading) but the Grand Chamber found that there was no material on the file which was ‘itself sufficient to enable it to take cognisance of or examine the Prince’s previous conduct with regard to the media’, at [130]. It was, however, found that ‘the mere fact of having cooperated with the press on previous occasions cannot serve as an argument for depriving a person discussed in an article of *all* protection’, at [130] (emphasis added).

¹⁴⁰ See Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [2014] WLR 659 [81], [97]: ‘the interest of the public in having [the information in question] is an interest which may vary, in particular, according to the role played by the data subject in public life...’. That stance was adopted in the Guidelines 5/2019 on *The criteria of the Right to be Forgotten in the search engines cases under the GDPR*, adopted by the European Data Protection Board on 7 July 2020: ‘the interest of the public in having that information [is] an interest which may vary, in particular, according to the role played by the data subject in public life’ [47].

¹⁴¹ n 94, at [22]. See also Lady Hale’s definition of public interest in *Jameel v Wall St Journal* [2006] UKHL 44, where she excludes ‘vapid tittle tattle’ about footballers from the definition: [147].

¹⁴² It was previously rejected in *Mosley Max Mosley v News Group Newspapers Limited* [2008] EWHC 1777 (QB) at [127]: Mr Justice Eady found ‘...it is not for the state or for the media to expose sexual conduct which does not involve any significant breach of the criminal law....It is not for journalists to undermine human rights, or for judges to refuse to enforce them, merely on grounds of taste or moral disapproval’. The same argument was also rejected on the facts in *Rocknroll v News Group Newspapers Ltd* [2013] EWHC 24 (Ch): ‘nothing in the [lawful] conduct of the claimant which the Photographs portray gives rise to any matter of genuine public debate, however widely drawn is the circle within which such matters may genuinely arise’, at [33].

¹⁴³ See: *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457; *Terry and persons unknown* [2010] EWHC 119 (QB).

validity of that factor as apparently having a connection with the ‘public interest’, but concurred with the Court of Appeal’s view that it did not apply in the instance in question, since no false image had been presented.¹⁴⁴ That finding is clearly open to criticism on the basis that the Court took account, not of a matter of real value in free speech terms, especially in terms of audience-based justifications, but of a factor strongly linked to the somewhat symbiotic relationship between celebrities and the traditional media:¹⁴⁵ acceptance of the false image argument was reaffirmed without providing a defence of its connection with free speech values.¹⁴⁶ The argument from truth could apply but in a low level form, given that little value attaches to the knowledge that a celebrity takes drugs; it hardly needs pointing out that this is a press-friendly argument since in general the press seeks – for obvious reasons – to target celebrities for reporting, and celebrities are highly likely to have attracted, and sought, publicity in the past.

A general determination was, however, evident in *PJS* to focus closely on the severity of the privacy intrusion, as compared with the flimsiness of the free speech arguments;¹⁴⁷ its stance was then echoed in the very close focus on the severe impact on the claimant of the intrusion into his private life evident in *Cliff Richard*;¹⁴⁸ the privacy argument prevailed in the face of Article 10 arguments that had some plausible connections with the public interest.¹⁴⁹ The objective of re-focusing the tort somewhat more clearly on such connections was evident to an extent in *PJS*, and that re-focusing would also now be expected to become apparent in

¹⁴⁴ *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] UKSC 26, 1091 [14]: the Supreme Court supported an aspect of the Court Appeal’s decision (*PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] EWCA Civ 100) in finding that ‘there was no false image to require correction by disclosure of the claimant’s occasional sexual encounters with others.’

¹⁴⁵ Nevertheless, the Supreme Court in *PJS* (n 94) showed a strong awareness of the lack of significance in Article 10 terms that would in general attach to celebrity gossip: ‘But, accepting that Article 10 is not only engaged but capable in principle of protecting any form of expression, this type...is at the bottom end of the spectrum of importance...it may be that the mere reporting of sexual encounters of someone like the appellant, however well known to the public, with a view to criticising them *does not even fall within the concept of freedom of expression under Article 10 at all...*’ at [24] (emphasis added).

¹⁴⁶ *ibid* at [14].

¹⁴⁷ In particular, see Lord Mance’s forceful final paragraphs in *PJS* (n 94): 1104-1105, at [44-45].

¹⁴⁸ *Sir Cliff Richard OBE v (1) The British Broadcasting Corporation (2) South Yorkshire Police* [2018] EWHC 1837 (HC): ‘Sir Cliff felt trapped in his own home, and he felt despair and hopelessness leading, at times, to physical collapse. At first he did not see how he could face his friends and family, or even his future’, at [233]. That decision bears some similarity to the one in *Prince Charles*: on a possibly unique set of facts a fairly strong free speech argument, based on the value of political expression, was rejected in the face of a privacy argument weaker than the one in *Cliff Richard (HRH Prince of Wales v Associated Newspapers)* [2006] EWCA Civ 1776; the defendant publishers (a large newspaper corporation) sought unsuccessfully to argue that the fact that the Prince was lobbying democratically elected ministers was of public interest since, as heir to the throne, he was expected to be politically neutral; at [123-124].

¹⁴⁹ *ibid*. Mr Justice Mann considered the notion of public interest at length; the disclosure that Cliff Richard was being investigated for historical sexual abuse did have legitimate public interest value, but it was also noted that a point of relevance concerned the motivation of the BBC in making the disclosure [279-280].

relation to speech/privacy balancing under the GDPR. But the possibility that a *stronger* focus on free speech values might arise in relation to privacy claims under the GDPR/DPA and tort is also canvassed below.

The GDPR/DPA protective framework for freedom of expression and information

Under Article 7 of the previous Data Protection Directive,¹⁵⁰ echoed under the DPA 1998 Schedule 2 paragraph 6, a condition of processing was that a legitimate interest applied; one such interest arose (Article 7(f)) if ‘the processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)’. That wording is largely, not wholly, reproduced under Article 6(f) GDPR; a key change is that special protection is provided for children as data subjects, and in that respect Article 6(f) is in alignment with the tort wherein such protection has already been established.¹⁵¹ The legitimate interests under Article 7(f) were found in *Google Spain* to include the interest in serving freedom of expression and information.¹⁵² But since in relation to the right to erasure under Article 17, a specific provision, Article 17(3)(a), refers to processing serving those freedoms, a processor against whom the right is claimed would tend to rely on that provision rather than on the legitimate interests exception. The free expression jurisprudence discussed below refers to Article 7(f) under the previous Directive since Article 17 was a clarifying introduction in the GDPR; nevertheless, it is highly probable that that jurisprudence will be relied on under the GDPR since it will also be interpreted in accordance with the Strasbourg speech/privacy balancing jurisprudence. So that jurisprudence will determine the impact of Article 17(3)(a), which provides: ‘(3) Paragraphs 1 and 2 [the right to erasure/‘to be forgotten’] shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression...’.¹⁵³ The term ‘to the extent that’ invites consideration of the speech/privacy balancing act. Under the GDPR, alongside the protection for freedom of expression specifically applying to the right of erasure, there is also a potential or apparent

¹⁵⁰ Directive 95/46/EC.

¹⁵¹ See n 65.

¹⁵² n 26. The COJ spoke of striking ‘a fair balance’ between ‘the legitimate interest of internet users potentially interested in having access’ to the information and ‘the data subject’s fundamental rights under articles 7 and 8 of the Charter’: [81].

¹⁵³ Text in square brackets added.

difference between the data protection scheme and the tort: freedom of expression¹⁵⁴ finds a further layer of protection applying to processing generally in the form of the journalistic ‘exemption’.

The current iteration of the ‘journalistic exemption’

Article 85 GDPR 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, including processing for journalistic purposes’,¹⁵⁵ and invites member states to detail derogations.¹⁵⁶ The ‘journalistic’ aspect of the GDPR/DPA expression-protective framework arises under Schedule 2 Part 5 paragraph 26 DPA 2018, which provides that journalism is a ‘special purpose’,¹⁵⁷ and ‘the 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)). The exemption would not therefore apply if, in seeking to follow a journalistic purpose, a belief that a data protection principle could therefore be disapplied was found to be unreasonable,¹⁵⁸ a requirement that could exclude a range of actors from the exemption, including traditional media bodies. Paragraph 26(2) provides, based largely on the journalistic exemption that arose under section 32 Data Protection Act 1998, that the exemption applies to the processing of personal data carried out for the special purposes if ‘(a) the processing is being carried out with a view to the publication by a person of journalistic....material’. Before considering the further requirements needed to satisfy the exemption, it is important to seek to establish the meaning likely to be attributed to ‘journalistic purposes’ under the DPA 2018, but it should

¹⁵⁴ Freedom of expression includes ‘free access to information’ according to the Guidelines 5/2019 *on the criteria of the Right to be Forgotten in the search engines cases under the GDPR*, adopted by the European Data Protection Board on 7 July 2020, at 11.

¹⁵⁵ Article 85(1).

¹⁵⁶ *ibid.*, (2).

¹⁵⁷ Para 26(1)(a).

¹⁵⁸ See *True Vision Productions v IC* (EA/2019/0170), hearing: 23 and 24 November 2020. The Information Commissioner had issued a monetary penalty notice to the broadcast production company, imposing a penalty of £120,000, which related to recording, both video and audio, in most of the examination rooms at Addenbrooke’s Hospital through CCTV cameras and microphones, with the key purpose that the recording would capture the moment of diagnosis when the mother learned that her baby had died. It was found that the fact of recording was not fully brought to the attention of the mothers in question, and they did not give consent to it. The judge considered that ‘a belief that it was impossible to comply with the data protection principles without referring to, or hinting at, the real purpose of the recording’ [23] was a reasonable belief (because it related to the key journalistic purpose of the film) so far as obtaining ‘explicit consent’ under Schedule 3 DPA 1998 was concerned [25]. But the judge found that ‘it was not reasonable to believe that collecting the data required could only be achieved in a way that was incompatible with the principle of fairness’ [26] because hand-held cameras could have been used. The exemption did not therefore apply.

be noted that content deemed non-journalistic could fall within one of the other special purposes.¹⁵⁹

The 2018 Act fails to state whether the speech of citizen (non-professional) journalists is covered by the exemption, or to proffer a definition of ‘journalistic’, although it is notable that the general term ‘controller’ rather than ‘journalist’ is used in paragraph 26. The wording of the exemption was also widened somewhat under the current regime, removing the previous requirement that data had to be processed for journalistic purposes *alone*, thus making it more likely that non-journalists could fall within it.¹⁶⁰ The COJ in *Google Spain* held that the search engine Google could *not* rely on the exemption under the 1995 Directive,¹⁶¹ but nevertheless left open the possibility that website hosts/social media platforms could rely on it in certain circumstances.¹⁶² The pivotal issue, following the COJ findings in *Satamedia*, is likely to be whether content seeks to transmit ‘information’ or ‘ideas’ to the public; the COJ also found that the notion of ‘journalistic’ under the previous Directive should be construed broadly.¹⁶³ The court in the English case of *Sugar* found that ‘journalism’ should *only* encompass the discussion of ‘current affairs’,¹⁶⁴ but the significant decision in *NT1 and NT2*, relevant to the ‘right to be forgotten’, provided some guidance on this issue under the previous scheme,¹⁶⁵ which adopted a broader stance. Lord Justice Warby accepted that the journalistic exemption has a ‘broad’ reach under EU law, and held that ‘the concept extends beyond the activities of media undertakings and encompasses other

¹⁵⁹ Para 26(1)(b)-(d) covers academic, artistic or literary special purposes.

¹⁶⁰ Under the old regime data had to have been processed for journalistic purposes *alone* (with no additional motives); that is no longer the case. See: Data Protection Act 1998, s 32; N. Cain and R. Carter-Coles, ‘GDPR and the Data Protection Act 2018 – how do they impact publishers?’ (*RPC*, 2018) at <https://www.rpc.co.uk/perspectives/data-and-privacy/gdpr-and-the-data-protection-act-2018/> (accessed ~~8~~14 ~~November~~October 2021~~9~~).

¹⁶¹ See n 26; the decision referred to Directive 95/46/EC. In *NT1 and NT2* (n 16) at [98]-[102] the judge reiterated that search engines do not fall within the exemption. See further F. Brimblecombe and G. Phillipson, ‘Re-gaining Digital Privacy? The New ‘Right to be Forgotten’ and Online expression’ (2018) 4(1) *Canadian Journal of Comparative and Contemporary Law* 1, 34-35.

¹⁶² *ibid.*, at [85].

¹⁶³ See Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECR I-09831, ECLI:EU:C:2008:727 at [61]. See [56]: ‘In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary, first, to interpret notions relating to that freedom, such as journalism, broadly...’. See further: F. Brimblecombe and G. Phillipson *ibid.*; A. Flannagan ‘Defining ‘journalism’ in the age of evolving social media: a questionable EU legal test’ (2012) 21(1) *International Journal of Law and Information Technology*, 1-30.

¹⁶⁴ *Sugar v BBC* (and another) [2012] 1 WLR 439. See also H. Tomlinson, ‘The “journalism exemption” in the Data Protection Act: Part I, the Law’ (*Inform*, 2019) at <https://inform.org/2017/03/28/the-journalism-exemption-in-the-data-protection-act-part-1-the-law-hugh-tomlinson-qc/> (accessed ~~8~~14 ~~October~~November 2021~~9~~).

¹⁶⁵ *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2018] EWHC 799 (QB). Although the case was decided under the DPA 1998, there is a high degree of overlap between the journalistic exemption under both Acts, as mentioned above.

activities, the object of which is the disclosure to the public of information, opinions and ideas.’¹⁶⁶ That was clearly a very generous reading of the extent of the exemption; he sought, however, to place a constraint on its scope, but of a fairly imprecise nature, finding that not ‘every’ role involving distributing information and ideas could be viewed as journalism, since so doing would ‘elide the concept of journalism with that of communication.’¹⁶⁷ That caveat placed on his earlier comments was clearly intended to indicate that the exemption does not necessarily extend to *any* processing conveying ideas or information (bearing in mind that links created by search engines have been found to be outside the exemption). But it fails to create any clear distinction between journalistic and other communicative expression. His generous reading had previously been echoed by the Information Commissioner,¹⁶⁸ and also in findings in *The Law Society and others v Kordowski*¹⁶⁹ under the previous regime; the court was clear that a private individual can engage in internet journalism: ‘Journalism that is protected by s32 involves communication of information or ideas to the public at large in the public interest’, an interpretation clearly potentially consistent with the importance of free expression in general.¹⁷⁰

The main emphasis under the 2018 Act, from the findings above, is likely to be placed, not on the term ‘journalistic’, but on the public interest value of the expression or information.¹⁷¹ Given those findings as to ‘journalistic’, that term, under the current iteration of the exemption, appears to be unlikely to operate frequently in an exclusionary fashion, and to add little to the other requirements of para 26, which include the requirement that ‘the controller reasonably believes¹⁷² that the publication of the material would be in the public interest’. Under paragraph 26(4), in making that determination, ‘the controller must take into account

¹⁶⁶ *ibid* at [98].

¹⁶⁷ *ibid*.

¹⁶⁸ ‘We accept that individuals may be able to invoke the journalism exemption if they are posting information or ideas for public consumption online, even if they are not professional journalists and are not paid to do so.’ ‘ICO guidance Data Protection and Journalism: A Guide for the Media’ (Information Commissioner, 2014) at <https://ico.org.uk/media/about-the-ico/consultations/2029/consultation-response-summary-dp-and-journalism-a-guide-for-the-media.pdf> (accessed ~~8 October~~ ~~24 December~~ 2021~~9~~).

¹⁶⁹ [2014] EMLR 2. The High Court found that the exemption was inapplicable in relation to a website set up by an individual to name and shame ‘solicitors from hell’ because the communications to the public at large lacked ‘the necessary public interest’.

¹⁷⁰ *ibid*, at [99].

¹⁷¹ So finding might clearly tend to undermine the notion of ‘journalistic’ speech as distinctive: see Brimblecombe and Phillipson, (n 161) 35-37.

¹⁷² Para 26(2)(b). For discussion of ‘reasonably believes’ under the DPA 1998 s 32, see the Court of Appeal in *Campbell v MGN* [2003] QB 658. A clear parallel could be drawn with section 4(1) Defamation Act 2013, providing: ‘It is a defence to an action for defamation for the defendant to show that (a) the statement complained of was, or formed part of, a statement on a matter of public interest; and (b) the defendant reasonably believed that publishing the statement complained of was in the public interest’.

the special importance of the ‘public interest in the freedom of expression and information’. The term ‘reasonably’ obviously indicates that a purported belief that publication is in the public interest without substance would not satisfy this requirement. While the exemption therefore apparently relies on establishing objective and partially subjective elements, if the requirements under paragraphs 26(4) and (3) are satisfied, it appears to be likely, with the probable exception of search engines, that the ‘journalistic purposes’ element would also be. The need for a reasonable belief of the controller in the public interest value of the information would exclude online intermediaries in some circumstances; if there was no evidence that an intermediary had taken cognizance of such value, the exemption could not apply.¹⁷³ The requirement as to taking such cognizance, however, could be satisfied in some circumstances by search engines, and their exclusion from the exemption has been questioned.¹⁷⁴

The wording of the requirement under paragraph 26(4), taken at face value, could mean that there is a public interest in the mere fact of expression in itself, regardless of establishing a separate specific interest. The tort jurisprudence has had to confront a similar provision under section 12(4) of the HRA which requires that ‘The court must have particular regard to the importance of the Convention right to freedom of expression’. That provision receives some reinforcement since the court is also required to ‘take account of a relevant privacy code’ in relation to ‘journalistic material’,¹⁷⁵ and IPSO’s code finds that there is a public interest in freedom of expression itself.¹⁷⁶ But the tort jurisprudence, influenced by Strasbourg, has *not* taken the stance that the mere fact of expression, without more, creates a public interest. Had it failed to reject that stance, the speech/privacy balancing act would have been tipped towards favouring Article 10 over Article 8.¹⁷⁷ So if paragraph 26(4) DPA is interpreted consistently with that aspect of the tort jurisprudence that would prevent the exemption from

¹⁷³ See *CG v Facebook Ireland Limited and McCloskey (Joseph)* Neutral Citation No. NICA 54; [2015] NIQB 11. In *NT1 and NT2* (n 16) Google refused to de-list links to previous convictions of one of the claimants, on the basis that they ‘relate to matters of substantial public interest to the public regarding [that claimant’s] professional life’, [8]. But at [102] it was found: ‘There is no evidence that anyone at Google ever gave consideration to the public interest in continued publication of the URLs complained of...’. Thus it was found that the exemption did not apply to Google.

¹⁷⁴ In *Townsend v Google Inc & Google UK Ltd* [2017] NIQB 81 it was claimed on behalf of Google Inc. that ‘to ask the question as to whether a search engine is journalism is to ask the wrong question. Rather the enquiry should be whether the material is journalistic material’, at [60].

¹⁷⁵ Section 12(4)(b).

¹⁷⁶ n 45, at paragraph 2.

¹⁷⁷ It was established in *Re S (a child)* [2005] 1 AC 593 and *Campbell v MGN Ltd* [2004] UKHL 22, despite the provision of section 12(4) HRA, that the Articles must be treated as of equal weight. That was reaffirmed by the Supreme Court in *PJS* (n 94), at [33]. See in contrast text to n 127.

applying to *any* expression processed for ‘journalistic purposes’ – a specific further public interest would have to be identified. In considering that interest the fact that the disclosure of private information was carried, for example, on a non-journalistic website of similar standing to that of a serious, well-regarded newspaper,¹⁷⁸ could be taken into account, on the basis that an objective of the entity in question was to play a significant informative role in a democracy, aiding democratic self-governance.¹⁷⁹ As Coe puts it, ‘media freedom [need not] be a purely institutional privilege; it can apply to any actor[s]’.¹⁸⁰ In this context that would arguably be the case if, for example, such online actors conformed to certain requirements associated with, but not confined to, professional journalism, such as checking sources. Online material fulfilling such requirements could be found to be more likely to satisfy the public interest demands of the exemption. Placing the emphasis on the public interest requirement of the exemption may tend to elide it with other aspects of the speech protective framework of the GDPR/DPA. But it would avoid the possibility that the mere invocation of the term ‘journalistic’ in para 26 would place media-created, privacy-invading material in a privileged position, given that such material does not usually make the contribution to the market-place of ideas,¹⁸¹ to furthering democracy or the search for truth, that originally underpinned the idea of media privilege, recognised in Article 11(2) of the EU Charter of Fundamental Rights and at Strasbourg.¹⁸² But given the range of online actors that may now fall within the exemption, the idea of such privilege may now require a re-evaluation in order to cover expression of media *and* non-media actors of genuine public interest.

Expression outside the exemption under the GDPR/DPA

Some online privacy-invading expression might be found to fall outside the exemption due *inter alia* to failing the public interest test, so it could be covered by Article 85, Article 6(f), or under Article 17(3)(a) (where the right of erasure is sought). At first glance it is hard to

¹⁷⁸ Communications associated with the traditional media, as is well established, have occupied a privileged position in the speech jurisprudence of a number of jurisdictions; see J Oster ‘Theory and doctrine of “media freedom” as a legal concept’ (2013) 5 *Journal of Media Law* 57-78.

¹⁷⁹ See: Barendt n 129 above, p 18; *Bergens Tidande v Norway* (2001) 31 EHRR 16 at [48].

¹⁸⁰ P. Coe ‘Re-defining ‘media’ using a media-as-a-constitutional-component concept: an evaluation of the need for the ECtHR to alter its understanding of ‘media’ within a new media landscape’ (2017) 37(1) *Legal Studies* 25-53, at 51.

¹⁸¹ For discussion, see eg J. Gordon ‘John Stuart Mill and the “Marketplace of Ideas”’ (1997) 23(2) *Social Theory and Practice* 235-249.

¹⁸² It states: ‘freedom and pluralism of the media shall be respected’. The Strasbourg Court has also recognised a privileged position of the media; see eg: *Lingens v Austria* (1986) A. 103 at [42]; *Goodwin v UK* (1996) 22 EHRR 123, at [39]; *Perna v Italy* (2004) 39 EHRR 28; *Armonienė v Lithuania* [2009] EMLR 7, at [39].

conceive of an online processing of private information that would *not* convey information or ideas - potentially attracting the exemption - but would still have some value in free expression or information terms. Thus the role of the more general provisions could potentially be minimised. But the exemption would not apply if there was no evidence that an online intermediary had adverted to the public interest value of the expression, since paragraph 26(2)(b) would not be satisfied and, if the exclusion of search engines from the exemption is maintained, it would not apply even where they had so adverted.¹⁸³ In such instances expression of some value could be covered under Article 17(3)(a) (in the case of an erasure request) or under the general provisions and would have weight in the balancing act. An example in which the exemption was not found to apply is provided by *Townsend v Google Inc & Google UK Ltd*:¹⁸⁴ the plaintiff had requested that Google Inc. should de-list seven of twelve previously notified URLs because they indicated that he was a sex offender.¹⁸⁵ The claim failed, partly due to the speech value of the expression¹⁸⁶ as put forward on behalf of Google, given the principle of open justice, and the value of enabling the public to gain access to information of significance, facilitating, for example, public debate as to rehabilitation of sex offenders.¹⁸⁷

Similarities between the 'balancing act' under the tort and that under the GDPR/DPA expression-protective framework

The requirements of free expression and information under the GDPR, Article 85, Article 17(3)(a), Article 6(f), and paragraph 26(4) DPA, are likely to be interpreted consistently with Article 10 ECHR,¹⁸⁸ as discussed above, which also influences the interpretation of Article

¹⁸³ See the findings in *NT1 and NT2* (n 16) which could be taken to imply that the exemption could apply if there was evidence that a search engine had adverted to the public interest.

¹⁸⁴ [2017] NIQB 81.

¹⁸⁵ The argument was put forward under Condition 6, Schedule 2 of the DPA 1998.

¹⁸⁶ It was found that there was a clear public interest in open justice and a clear right to freedom of expression (at [61]). The processing was found to be warranted, which meant that there was no triable issue as to the Plaintiff's entitlement to rely on his section 10 DPA notice and therefore no breach of the sixth principle (at [64] – [65]). (The claim failed under the tort on the basis that when a conviction became spent under the Rehabilitation of Offenders Act that was 'usually' the point at which it might recede into the past and become part of a person's private life. But the Court found that the term 'usually' permitted 'facts and circumstances which may take the case out of the usual either one way or the other' (at [32]), and did not find that there was a basis for finding that it had become part of his private life). See also n 39.

¹⁸⁷ A similar conclusion was reached in *CG v Facebook* [2016] NICA 54 at [43]: 'We agree that with the passage of time the protection of an offender by prohibiting the disclosure of previous convictions may be such as to outweigh the interests of open justice. In principle, however, the public has a right to know about such convictions'.

¹⁸⁸ That was the stance taken under the DPA 1998, s 32: see *Campbell v MGN Ltd* (CA) [2003] QB 658 at [133]-[138].

11 of the EU Charter of Fundamental Rights.¹⁸⁹ Strasbourg has reiterated, albeit in a somewhat tokenistic fashion, due to the impact of the margin of appreciation doctrine,¹⁹⁰ that to justify disclosures of private information identification of a genuine public interest is needed, which must be distinguished from matters that the public feel an interest in.¹⁹¹ Only the former is deemed capable of adding weight to the Article 10 argument. It would appear then that merely establishing that the public would display curiosity as to the information in question would be insufficient to satisfy the GDPR/DPA free expression requirements.¹⁹²

Where relevant, the GDPR/DPA balancing act is likely to be conducted as it would be under the tort,¹⁹³ in the sense that the relevant arguments under Articles 8 and 10 ECHR are weighed with close intensity against each other on an equal footing. The stance that the English courts will take when balancing Article 8 and 10 rights under the GDPR/DPA framework protecting expression and information is fairly predictable; while they may take account of guidance from national Data Protection Authorities across Europe,¹⁹⁴ and the

¹⁸⁹ See text to n 125.

¹⁹⁰ See: *Von Hannover v Germany (No.2)* App nos 40660/08 and 60641/08 (ECHR, 7 February 2012); *Von Hannover v Germany (No.3)* App no 8772/10 (ECHR, 19 September 2013); *Axel Springer AG v Germany* App no 39954/08 (ECHR, 7 February 2012).

¹⁹¹ See *Couderc and Hachette Filipacchi Associes v France* App no 40454/07 (ECHR, 12 June 2014) at [100]. Although there was a public interest in knowing of the existence of the illegitimate child when Prince Albert was unmarried, the Court found: ‘The Court has also emphasised on numerous occasions that, although the public has a right to be informed, and this is an essential right in a democratic society which, in certain special circumstances, can even extend to aspects of the private life of public figures, articles aimed solely at satisfying the curiosity of a particular readership regarding the details of a person’s private life, however well-known that person might be, cannot be deemed to contribute to any debate of general interest to society’. However, although the Strasbourg Court noted in that instance that sex lives, even of public figures, are an inherently private matter (at [99]) and are often deserving of Article 8 protection, the claimant’s Article 8 rights did not ultimately prevail. See also *Von Hannover v Germany (No.2)* (n 190) at [114]. As to the ‘public interest’ requirement under the DPA 2018 journalism exemption, Tomlinson finds: ‘the provision contemplates a “public interest” justification for processing of a similar type to that required to justify the publication of private or confidential information: a belief that the public will be interested in the story or that publication of stories of that type is necessary for the economic viability of the publisher will *not be enough*’: ‘The “journalism exemption” in the Data Protection Act: Part I, the Law’ (*Inform*, 2019) at <https://inform.org/2017/03/28/the-journalism-exemption-in-the-data-protection-act-part-1-the-law-hugh-tomlinson-qc/> (accessed [8 October 2021](#)).

¹⁹² Such a claim would not appear to provide a ‘compelling’ basis under Article 21(1) for continued processing, under Article 6(1): there must be ‘compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject...’.

¹⁹³ The use of the balancing act as under the tort in respect of the provision equivalent to Article 6(f) 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) [2018] EWHC 799 (QB), at [115], [132]. In Case C-131/12 *Google Spain SL and another v Agencia Española de protección de Datos (AEPD) and another* [2014] WLR 659 [81], [97] it was found that a similar balancing act would apply to the interpretation and application of the previous Directive. See also n 125 above.

¹⁹⁴ Articles 51–67 of the GDPR set out an enhanced role for national Data Protection Authorities, encouraging different authorities to work together and to insist on implementing rules. See: P. De Hert and V. Papakonstantinou, ‘The proposed Data Protection Regulation replacing Directive 95/46/EC: a sound system for

European Data Protection Board (EDPB), it is highly probable that they will be drawn towards relying on the ‘balancing’ jurisprudence relating to the previous DPA regime, and developed to a greater extent under the tort.¹⁹⁵ The guidance provided so far by the EDPB on this matter is of a general nature, leaving open a great deal of leeway for interpretation.¹⁹⁶ The term ‘public interest’ is also obviously open to interpretation: it might appear that the traditional media-friendly stance at times taken under the tort, as discussed above, could permeate the future GDPR/DPA expression jurisprudence.¹⁹⁷ In the *traditional media* context on or offline that is likely to be the case - the courts’ conception of the public interest elements under the GDPR/DPA is likely to be informed by the factors relied on under the tort, and possibly could lead to the under-use of the new data protection scheme, as occurred under the DPA 1998.¹⁹⁸ The public interest could be found to include, conceivably, ‘information as giving an account of a particular mode of living’,¹⁹⁹ but more probably reliance might be placed on the ‘role model’ argument, which was not rejected in *PJS*, and the ‘correcting false impressions’ notion,²⁰⁰ since it received express acceptance from the Supreme Court. But it is argued below that where private actors, including intermediaries, misuse private information online, the forthcoming speech jurisprudence is likely to show some fairly marked departures from acceptance of public interest factors of doubtful value in speech terms under both data protection and the tort.

A closer focus on free speech and information values under the GDPR/DPA and tort in the online context?

While the ‘public interest’ factors on the Article 10 side of the balance already established under the tort jurisprudence could influence the balancing act under the GDPR/DPA, they would be less relevant where the data controller is a non-journalist and the private

the protection of individuals’ (2012) 28(2) *Computer Law & Security Review* 130, 138; L. Costa and Y. Poullet, ‘Privacy and the Regulation of 2012’ (2012) 28 *Computer Law & Security Review* 254, 255.

¹⁹⁵ As argued in Brimblecombe and Phillipson, n 161.

¹⁹⁶ See n 140.

¹⁹⁷ Tomlinson (n 164) sees it as probable in relation to the exemption under the DPA 2018 that the English courts will look to the tort jurisprudence to interpret it, as they did under the DPA 1998.

¹⁹⁸ It has been found in a number of instances offline that nothing would be gained benefitting either claimant, from engaging in the balancing act under the DPA 1998, than would have been obtained under the tort: see n 4 and n 5 above.

¹⁹⁹ This position was accepted in *Von Hannover (No.3)* App no 8772/10 (ECHR, 19 September 2013). But this notion sits very uneasily with the stance as to weak public interest arguments taken in *PJS* (n 94); it is to an extent cognate with the disapproved-of notion of using private information to enable a debate about possible anti-social behaviour (text to n 94).

²⁰⁰ See further Brimblecombe n 22.

information does not relate to a high profile public figure.²⁰¹ That clearly also applies to the interpretation of the ‘public interest’ element of the journalistic ‘exemption’ since it covers speech published or hosted by such actors.²⁰² The ‘public interest’ factors identified tended to be linked to interests of the traditional media and so would clearly have a less ready application outside that context. If such factors have in reality merely been used at least partly as a proxy for promoting media freedom by enabling the traditional media to satisfy public curiosity as to celebrities’ private lives, then they should be discarded in interpreting the speech protective framework under the GDPR/DPA, since it was designed and developed with freedom of expression and information rather than the interests of the traditional media in mind. Early and tentative intimations of such a discarding in the online context are currently becoming apparent under data protection *and* the tort, giving rise to the prospect of interpreting the Article 10 aspect of the balancing act in a manner that involves a closer scrutiny of real connections with free speech, as opposed to traditional media, concerns.²⁰³ The possibility of such scrutiny found some expression in the significant case of *NT1 and NT2 v Google*.²⁰⁴

The claims were brought under both the tort²⁰⁵ and the DPA 1998, so the balancing act was conducted in relation to both causes of action; as far as the DPA claim was concerned, free expression and information arguments were adverted to under the 6th condition for lawful processing,²⁰⁶ now echoed in Article 6(f) GDPR.²⁰⁷ The personal data in question could be accessed via personal name searches to links operated by Google;²⁰⁸ the links were to the spent fraud-related convictions of two business-men, who wanted them to be expunged. Relying on the balancing act developed under the tort,²⁰⁹ the court found that NT1’s de-

²⁰¹ Article 29 of the previous Directive established a Working Party on the Protection of Individuals with regard to the Processing of Personal Data which set out various criteria relevant to balancing privacy and expression claims; it included quite an expansive interpretation of ‘public figures’ which could include persons in business. Article 68 and Recital 139 of the GDPR confirmed the establishment of the European Data Protection Board (EDPB) to replace the Working Party; the EPDB is likely to accept the stance of the Working Party.

²⁰² See the comments of the Strasbourg Court on this point in *Ahmet Yildirim v. Turkey* (3111/10) November 18, 2012, at [56].

²⁰³ See eg as to the differences between the two: Chief Justice Brennan, ‘Address’ (1979) 32 *Rutgers Law Review* 173; P. Wragg, *A Free and Regulated Press. Defending Coercive Independent Press Regulation* (Oxford: Hart 2020).

²⁰⁴ *NT1 and NT2 v Google LLC* (Intervenor: The Information Commissioner) [2018] EWHC 799 (QB), especially at [111], [130], [168].

²⁰⁵ *ibid*, at [172] and [226].

²⁰⁶ Data Protection Act 1998 Sched 2, Condition 6(1).

²⁰⁷ See text to n 150.

²⁰⁸ The case followed the breakthrough decision in *Google Spain* (see n 26) which also concerned name-based searches [98].

²⁰⁹ n 193, at [115], [132].

listing ('erasure') request should not be sustained, on the basis that the public needed to know that he had past convictions for dishonesty in relation to business dealings/enterprise, since he was seeking to start up new companies, and was apparently attempting to give a false impression as regards his honesty in business dealings via postings 'cleansing' his image. So it appeared that there was a legitimate public interest in allowing information as to his convictions to remain online, accessible via Google, so that people were aware of who they were dealing with; the obvious implication was that he could demonstrate dishonesty in future business dealings. That finding tipped the balance in favour of expression and information, but only after an extensive discussion of the competing speech and privacy-based arguments.²¹⁰ The same balancing act was conducted in relation to NT2; although there was some evidence that he had also sought to present a somewhat distorted image to the public, and the information in question was available on more than one website, regardless of named person searches,²¹¹ a close focus on the true value of Google's free expression claim led to the finding that the privacy argument should prevail. It was found: 'there is just enough in the realm of private and family life to cross the threshold. The existence of a young, second family is a matter of some weight....The claimant's current and anticipated future business conduct does not make his past conduct relevant to anybody's assessment of him, or not significantly so.'²¹² In both instances a close focus on both expression and privacy was achieved and, although the case concerned the presentation of a false or distorted image to the public, the tort jurisprudence concerning such images, in the traditional media context, was not referenced. The findings would clearly now also be relevant under aspects of the GDPR/DPA protective framework for expression and information.

NT1 and NT2 indicates that the courts are ready to accept that since freedom of expression arguments under the GDPR/DPA or tort are applicable in instances of online disclosures of information outside the traditional media context, their interpretation reaches beyond that context, and need not be formulated with the traditional media in mind.²¹³ Since the

²¹⁰ It was stated (at [166(4)]): 'Freedom of expression has an inherent value, but it also has instrumental benefits which may be weak or strong according to the facts of the case'. The close focus on both Articles 8 and 10 involved lengthy consideration, extending from [136]-[172].

²¹¹ Google's public domain argument did not succeed; see in particular [220].

²¹² n 213, at [226].

²¹³ A further example of such a tort claim where the respondents were not mass media entities (and where the Data Protection Act was viewed as of relevance to the claim) arose in *CG v Facebook Ireland Limited and McCloskey (Joseph)* [2015] NIQB 11; in part the case concerned the expression value of a Facebook post from 2 private individuals concerning CG's conviction for sexual offences, in terms of open justice and warning

distraction of considering protection for freedom of the traditional media is removed, the scrutiny accorded to such arguments can focus more clearly on the question whether factors are present that have any genuine connection with free speech values. The expression at issue in *NT1 and NT2* clearly had little or no connection with supporting democracy or contributing to the market-place of ideas. Essentially, it related mainly to the private business interests of certain persons who might consider entering into dealings with either claimant: it had some informative value as far as such persons were concerned. It is therefore unsurprising that NT2's private and family life interests – although not very compelling - overcame the expression and information claim. In contrast, it was found that the impact on NT1's family life was merely speculative,²¹⁴ and the information itself was only doubtfully to be deemed 'private'.²¹⁵

Overall, therefore, given the shaping of the GDPR/DPA with the creation of stronger protection for personal privacy in mind, as compared with aspects of the design and development of the tort, with traditional media concerns often to the fore, expression claims may be subject to a stronger scrutiny to determine their real connection, if any, to protecting free speech rather than (quite often) press interests. The rise of claims concerning online privacy *outside* the traditional media context is *also* prompting a gradual change of direction under the tort, meaning that the body of expression jurisprudence arising in future, albeit sometimes under the established balancing act, is likely also to show such a connection, or, alternatively, to expose its weakness more readily. Speech jurisprudence in general *outside* the privacy context, arising in a number of jurisdictions, demonstrating connections with the classic free speech values, tends to arise mainly in media or public protest contexts and to concern matters of general interest.²¹⁶ The difficulty of finding such connections in relation to disclosures of private information has at times been obscured under the tort so far, since most (not all) of the key cases concern the press and high-profile public figures. But now that the focus of the jurisprudence is becoming more likely to concern online privacy intrusion by private actors or intermediaries, and therefore more often the public or private lives of private or semi-public figures,²¹⁷ the notion that connections can be found with the classic free

the public, as compared with CG's privacy interest (which prevailed), linked in part to the impact on his family life that he might face as a result of the postings. See further text to n 98.

²¹⁴ n 204, at [154].

²¹⁵ *ibid.*, at [140].

²¹⁶ See n 129.

²¹⁷ But see n 26, at [81], [97] as to the expansive definition of a 'public' figure adopted under the previous scheme, likely to be adopted under the GDPR; NT1 as a businessman was viewed on that basis as a public

speech values in privacy cases will be more readily exposed for the hollow argument that it usually is.²¹⁸ In such instances the balancing act itself would often merely be irrelevant since there would be nothing of value to place on the Article 10 side of the balance, as in, for example, instances giving rise to GDPR, and tort, claims in which search engines or social media platforms collect personal data concerning consumer preferences (browser generated information) to disclose for commercial profit.²¹⁹ The information would almost always have value only in terms of *private* gain; no plausible public interest value could be claimed.

Conclusions

This article has contended that the tort, together with the UK GDPR/DPA, is entering a new era in terms of privacy protection. Rather than frequently concerning confrontations between a celebrity and the press, the conflicts are now typically also between ordinary people, including children, and the tech companies. When such conflicts arise, including those referenced above, leading to judicial consideration of the applicability of one or both causes of action to misuses of private information online, often by intermediaries, they are providing the judges with an opportunity to affirm the applicability of the tort in this new context, one they are currently grasping with alacrity. Given that the GDPR and tort are ‘two parts of the same European privacy protection regime’,²²⁰ pressure might be placed on any defence of a lower standard of privacy protection provided by one of those parts - hence the argument canvassed here that the traditional media-linked checks built – to an extent - into the notion of a ‘reasonable expectation of privacy’ are already being discarded by courts in the online context. Possibly the reluctance to attach such an expectation to apparently innocuous personal information about an adult may in future be questioned when such information is posted and widely disseminated online. Discarding the crude notion of public domain – as

figure with a reduced expectation of privacy. That definition is in some tension with *Von Hannover v Germany (No 1)* (2005) 40 EHRR 1 [63] which identified a ‘fundamental distinction...between reporting facts capable of contributing to a debate in a democratic society and reporting details of the private life of an individual who does not exercise such functions.’

²¹⁸ See n 145.

²¹⁹ See for current examples, but arising under the previous data protection regime, n 9 and n 220. In both instances the value of the expression would self-evidently be negligible.

²²⁰ See *Lloyd v Google LLC* [2019] EWCA Civ 1599 at [53]. The claimant proceeded under the DPA 1998 alone, but the question of relying on tort case-law in relation to damages was pivotal on the basis that the remedies should not be less effective under data protection than under the tort: [Counsel for Lloyd argued] ‘that, if damages are available without proof of pecuniary loss or distress for the tort of misuse of private information, they should also be available for a non-trivial infringement of the DPA. Both claims are derived from the same fundamental right to data protection contained in article 8 of the Charter of Fundamental Rights of the European Union’ (at [6]).

has already occurred – is also consonant with the protection the tort is providing, and is able to provide, for informational autonomy online.

It might have been anticipated that the ascendancy of the tort and marginalisation of data protection in the privacy context under discussion that occurred until recently in the pre-digital era would be reversed under the GDPR/DPA. In other words, in the face of a scheme clearly tailored to the privacy-invading power of the tech companies, the tort's role in the online context would diminish. This article has sought to demonstrate that that is *not* the case. It has argued that there are differences between the two causes of action – in particular there is a disparity between the idea of private information under the GDPR as compared with that under the tort - but that they both provide effective opportunities for the privacy claimant to vindicate their claim, especially as there are signs that dubious public interest claims would be rejected under both. The differences may mean that such a claimant may turn to one cause of action as opposed to the other: for example, in relation to apparently innocuous private information. Also court action is not essential to invoke the right to erasure under Article 17, and in any event reliance on the GDPR may in some circumstances lead to a more rapid and less costly resolution of an online privacy claim against an individual or an intermediary. But it is concluded that the tort is already adapting very readily to the online context, and that the availability of both causes of action provides a wider range of opportunities for the vindication of online privacy claims than would be provided if only one of the actions was available. So there is room for optimism as to the ability of both causes of action to meet the challenges of confronting the privacy-invading potentialities of the tech companies in the coming years, satisfying in many instances the objective of guarding informational autonomy online.