FOUR

Routes to Remedy? The 'Right to Be Forgotten' as an Alternative Route to Redress

Introduction

Chapter 3 of this book has argued that, for a number of different reasons, English defamation law is currently unsatisfactory in protecting the reputation – and therefore personal dignity – of those defamed online, in light of the prevailing threat of defamation by *social media*, *AI tools* and *third-party posters* in the digital age. Defamation law is largely insufficient in this goal for two main reasons: firstly, the substance of the action in English defamation law is now increasingly difficult to make out, partly due to changes introduced by the Defamation Act 2013. Secondly, defamation law is not doing enough to tackle phenomena produced by technological advancements (such as defamation by *AI* and *third-party posters*). An increasingly liberal interpretation of the law in favour of claimants must be adopted in such scenarios if meaningful redress is to be achieved.

In particular, the serious harm threshold in s 1(1) of the Defamation Act 2013 can act as a significant obstacle to those defamed on the internet, as it raises the bar from the previous common law position, meaning that more claims will be struck out at this stage. As explained in Chapter 3, Part I, the judiciary's interpretation of s 1 as biased in favour of 'evidentiary' arguments means that it may be more challenging to meet this threshold if an individual is a victim of defamation online,

rather than by traditional mediums. The single publication rule in s 8 Defamation Act 2013 that limits defendant liability disadvantages all potential claimants, but particularly those who have been defamed on the web – as the internet has the unbridled potential to bring information from the distant past to the surface at any time. Defamation law is also ill-equipped to meet some of the technological issues raised by online defamation. It has been argued in the previous chapter that *defamation by AI tool* is a very real threat, looming heavily on the horizon given the incumbent Prime Minister's recent promise to integrate AI into daily lives.[1] If this fails to be taken seriously by the courts, then this will lead to a growing lacuna in the protection of reputation online. It has also been argued that the s 5 defence for operators of websites should be interpreted to include conglomerates such as Facebook and X in the *defamation by social media* scenario, to incentivize large social media websites to act in accordance with the annexed statutory regulations. However, it remains to be seen if the law is interpreted in the ways suggested by Chapter 3, particularly now that defamation law has 'swung' in favour of freedom of expression.[2] It is far from certain this will, in fact, happen.

Given the rather bleak picture painted for obtaining redress in such matters in defamation law, this book now turns to an alternate method of redress: UK data protection law, inherited from the EU. The *right to be forgotten* (RTBF), is a broad erasure mechanism that allows 'data subjects' to obtain the removal of their personal data on the internet, enshrined in Article 17 of the General Data Protection Regulation (GDPR).[3] The

[1] See 'Prime Minister sets out blueprint to turbocharge AI' (*GOV.UK*, 12 January 2025) www.gov.uk/government/news/prime-minister-sets-out-blueprint-to-turbocharge-ai accessed 23 January 2025.

[2] Alastair Mullis and Andrew Scott, 'The swing of the pendulum: Reputation, expression and the recentering of English libel law' (2012) 61(3) *Northern Ireland Legal Quarterly* 27.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing

GDPR lives on after Brexit in the UK jurisdiction as inherited (now domestic) law, termed the 'UK GDPR'. As has been recognized in an embryonic way by the English courts, both data protection law and defamation law work a twin purpose to protect different aspects of a claimant's private life and it is logical to consider both causes of action in tandem in cases of online libel.[4]

★★★

Part I: What is the right to be forgotten?

I. Background context

The GDPR is a revolutionary piece of law making, designed to champion data protection rights for individuals across Europe by setting a high standard in the form of an overarching regulation, transplanted directly into member state legislatures. European commissioners involved in drafting the GDPR commented that a goal of the EU in enacting the GDPR was for this to become a 'standard setter' for the protection of

of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) [2016] OJ L119/1 (27/4/2016).

[4] As was held in *Prince Moulay v Elaph Publishing* [2017] EWCA Civ 29. See Simon Brown, 'Case law: *Prince Moulay v Elaph Publishing*, Moroccan prince wins libel and data protection appeal against Arabic news publisher' (*Inforrm*, 7 February 2017) https://inforrm.org/2017/02/07/case-law-prince-moulay-v-elaph-publishing-moroccan-prince-wins-libel-and-data-protection-appeal-against-arabic-news-publisher-simon-brown/ accessed 25 May 2025. See also *Pacini & Anor v Dow Jones & Co Inc* [2024] EWHC 1709 (KB), where HHJ Parkes KC refused to strike out a defamation claim 'disguised' as a data protection claim [55] as per Jeevan Hariharan, 'Case comment: *Pacini v Dow Jones*, a call for appellate intervention on reputational harm damages' (*Inforrm*, 11 July 2024) https://inforrm.org/2024/07/11/case-comment-pacini-v-dow-jones-a-call-for-appellate-intervention-on-reputational-harm-damages-jeevan-hariharan/ accessed 25 May 2025.

personality interests in the digital age.[5] Aside from the desire to galvanize global change in robustly defending personal data, the drafting of the GDPR was also reactionary. It succeeded the previous data protection framework at EU level – the Data Protection Directive 1995 – which was increasingly seen as out of date due to the vast technological advancements between 1995 and 2012, the latter year being the time of the GDPR's first public release in draft form.[6] Two years after the EU Commission released its first lengthy draft of the GDPR, a seminal case was handed down by the Court of Justice of the European Union (CJEU): *Google Spain*.[7] The timing of the surprising ruling in *Google Spain* was most interesting,[8] as it came at a point when the RTBF, as included in the draft GDPR, was garnering hostility from legal commentators.[9] This was despite the fact the RTBF was far from an entirely new concept: France had already implemented a *droit à l'oubli* (a right to erasure) in its domestic law.[10] The right to private and family life and the right to control one's personal data are

5 Viviane Reding, 'The EU Data Protection Reform 2012: Making Europe the standard setter for modern data protection rules in the digital age' (22 January 2012) http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm accessed 18 June 2015.

6 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] OJ L 281, 31.

7 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.

8 Daniel Solove, 'What Google must forget: The EU ruling on the right to be forgotten' (*LinkedIn*, 13 May 2014) www.linkedin.com/pulse/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten accessed 23 January 2025.

9 See, for example, Meg L Ambrose and Jef Ausloos, 'The right to be forgotten across the pond' (2013) 3 *Journal of Information Law and Policy* 1.

10 Ibid 1.

also both codified in Articles 7 and 8 of the EU Charter of Fundamental Rights.[11]

One of the reasons that the RTBF enshrined in the draft GDPR 2012 had generated worldwide publicity was because European citizens did not believe the regulation's predecessor, the Data Protection Directive 1995, contained a right of erasure.[12] Indeed, a key motivating factor for the inception of the proposed regulation was to strengthen current insufficient data privacy rights and enhance a data subject's control over private information.[13] It was therefore surprising when the CJEU declared in *Google Spain* that a limited right to deletion already existed in EU law and could be found within Articles 6, 12 and 14 of the Data Protection Directive 1995.[14] Although the right within *Google Spain* manifested itself as a delisting of a search result on Google, the delisting right expounded in the judgment had the potential to be used in future cases to delete substantive personal data directly from websites. It is not an exaggeration to suggest that this judgment sent a shockwave through the worldwide legal community. Academics immediately responded to the judgment, a considerable amount of press coverage was generated and Google began to take measures to implement the ruling.[15]

Despite the significant publicity garnered, it is important to note that the CJEU *did not* create a generalized RTBF in the judgment of *Google Spain* in the same way that one exists to

[11] Charter of Fundamental Rights of the European Union (18/2/2000) OJ C 364/3, Article 7 and Article 8 www.europarl.europa.eu/charter/pdf/text_en.pdf accessed 23 January 2025.

[12] See (n 1).

[13] See Reding (n 5).

[14] See *Google Spain* (n 7) and Directive 95/46/EC (n 6).

[15] Paul Bernal, 'Are Google intentionally overreacting to the right to be forgotten?' (*Inforrm Blog*, 4 July 2014) https://inforrm.wordpress.com/2014/07/04/are-google-intentionally-overreacting-to-the-right-to-be-forgotten-paul-bernal/ accessed 30 January 2025.

this day in Article 17 GDPR. For the purposes of this book a RTBF is defined as a comprehensive personal data removal right, such as that enshrined within Article 17 GDPR (and UK GDPR). Rather, the CJEU construed a limited *deletion* right was present within the Data Protection 1995 (DPD '95). This deletion right was lifted from a combination of Articles 12 and 14 of the Directive. Article 12 of the DPD '95 predominantly relates to data removal in situations where data is outdated or inaccurate and Article 14 of the DPD '95 includes a 'right to object' to data processing on 'justified' grounds.[16] Despite its broad interpretation of the existing law, *Google Spain* did not create a generalized RTBF; in order to invoke *Google Spain*'s deletion right, a data subject must prove that the information is no longer relevant or that the data is inaccurate or excessive. In *Google Spain*, the CJEU adjudicated on three questions. Firstly, it was asked to decide whether a deletion right could be invoked within current EU data protection law.[17] Secondly, the court gave judgment upon whether the DPD '95 applied to Google as its company base was in the US (and not the EU).[18] Lastly, it ruled upon whether Google as a search engine could be construed as a 'data controller' for the purposes of the DPD '95.[19] Unexpectedly, the CJEU answered all three questions affirmatively.

Momentum grew after this shock ruling and the newly renamed 'right to erasure' (still a comprehensive RTBF) remained intact in Article 17 of the GDPR despite its passage through the EU legislative process, becoming enforceable in all member states – including the UK – in 2018. The 'right to erasure' in Article 17 is still widely referred to by its initial name in early GDPR drafts – the *right to be forgotten* – and as both names still accurately reflect the right, both will be used interchangeably in this book to refer to Article 17.

16 Directive 95/46/EC (n 6) Article 14 'The data subject's right to object'.
17 *Google Spain* (n 7) [92]–[93].
18 Ibid [60].
19 Ibid [38].

II. Article 17 GDPR

Article 17 allows 'data subjects' (identifiable individuals to whom information online relates)[20] to obtain from 'data controllers' (including website hosts, authors of a webpage or post and search engines)[21] deletion of personal data concerning themselves online. It also contains a requirement for controllers to contact third parties in relation to the replication or repetition of personal data that has been requested for deletion under Article 17(2). The right is broadly framed, with the mentioned roles loosely defined,[22] and does not require a threshold of seriousness to be met to invoke the right.[23] Article 17 appears to apply both to information initially uploaded to the internet by a data subject themselves and personal information uploaded by a third party. A limitation on the right is in the form of Article 17(3)(a), which contains an exception relating to the exercise of freedom of expression of the data controller,[24] as well as the GDPR's journalism exemption in the form of 'special purposes'.[25] Article 17 states:

> 1. The data subject shall have the right to *obtain from the controller the erasure of personal data* concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

[20] UK GDPR, Article 4(1).

[21] See *Google Spain* (n 7), where the CJEU found that search engine Google could constitute a data controller, and see UK GDPR, Article 4(7).

[22] UK GDPR, Article 4.

[23] As opposed to a defamation claim brought under the Defamation Act 2013, s 1.

[24] UK GDPR, Article 17(3)(a).

[25] EU GDPR, Article 85.

(a) the personal data are *no longer necessary* in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject *withdraws consent* on which the processing is based 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;
(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation under domestic law;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1);
[(g) the personal data have been processed as a result of an allegation about the data subject –
(i) which was made by a person who is a malicious person in relation to the data subject (whether they became such a person before or after the allegation was made),
(ii) which has been investigated by the controller, and
(iii) in relation to which the controller has decided that no further action is to be taken.]

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
   (a) for exercising *the right of freedom of expression* and information.[26]

In relation to Article 17(1)(b), an erasure right could become engaged in a scenario where consent to processing has initially been given by data subject and subsequently revoked, with no time limit in operation.[27] In the case of an online publication of potentially defamatory personal information, an individual could argue that they revoke any previous consent they may have given to that information being processed (for example, the prior use of a social media website in the *defamation by social media* scenario). In the event they gave no prior consent to its processing, an individual could claim that the false and defamatory personal data has otherwise been unlawfully processed, which would be particularly relevant if the false and defamatory personal data was uploaded to the internet by a third party, in according to Article 17(1)(d), in the *third-party poster* scenario. A person defamed online could also require erasure of the personal data on the grounds of objecting to the information's processing according to Article 17(1)(c).[28] The UK GDPR has extraterritorial effect, as it applies to

[26] UK GDPR; emphasis added. Note Article 17(1)(g) was added by the Victims and Prisoners Act 2024, s 31. This addition therefore does not appear in the EU GDPR or Article 17 as originally enacted. A further paragraph was also added to Article 17 UK GDPR by s 31, that details a 'malicious person' is one who has been convicted of one of a number of offences as set out by s 31(5) against a given victim, including harassment and stalking. See s 31(3) of the Act for more details. The impact of this section is to therefore expand Article 17 and to further protect victims of harassment and stalking. This expansion is to be welcomed, although it is not a central concern of this book.

[27] As this would, it is submitted here, come under the remit of Article 17(1)(a).

[28] This works in conjunction with Article 21 UK GDPR, the 'right to object'.

those 'offering goods or services to individuals in the UK';[29] such a service could be offered by, for example, a social media website which may be domiciled outside of the UK. As such, it is an extremely powerful erasure right, with a large scope – exactly what is necessary for tackling the multi-jurisdictional issue of online invasions of privacy – and in the case of this book – reputation.

There are, of course, a number of exemptions to Article 17's erasure right. Article 17 goes on to explain: 'Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information.'[30]

In terms of this book, the most pertinent exemption is Article 17(3)(a).[31] In this sense, there is a distinct similarity between defamation law and data protection law here: both the RTBF and a claim in defamation will chiefly be balanced against competing arguments that the publication (and continued access) of the personal information is in the public interest. How this balancing exercise should be conducted in relation to the RTBF will be returned to a later point in this chapter.

Finally, it is important to observe that a data controller's compliance with an Article 17 erasure request has a large motivating factor – the considerable sanctions possible under the UK GDPR (for non-compliance). Article 17 entails a fine of either £17,500,000 or 4 per cent of turnover according Article 83(5)(a) and (b).[32] The UK GDPR also notes that the decision to impose either the fine or the turnover tariff will depend on *whichever is higher*.[33] This is a considerable amount of money even for a large data controller such as Facebook or

[29] See the Information Commissioner's Office, 'The UK GDPR' https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/ accessed 30 January 2025. Also see UK GDPR, Article 3(1) and (2)(a).

[30] UK GDPR, Article 17(3); emphasis added.

[31] Also see EU GDPR, Article 85(1).

[32] UK GDPR.

[33] UK GDPR, Article 83(5).

Google and an inordinately large sum for a smaller corporation. Indeed, in Article 83's opening paragraph, the UK GDPR notes that one of the aims of the fines is to be 'dissuasive'.[34]

Now the groundwork has been set, this chapter will turn to a substantive comparison between the RTBF as a route to redress for those defamed online, in comparison to traditional English defamation law.

⋆⋆⋆

Part II: Can the 'right to be forgotten' provide a more effective remedy than English defamation law?

The comparison conducted here between English defamation law and the RTBF will be navigated by individual points pertinent to those seeking redress against false and potentially defamatory material on the internet.

I. Accessibility of redress

Despite the complex terminology that data protection law is couched in, the RTBF is a straightforward remedy. Ultimately, all an individual must do to assert their Article 17 erasure right is to contract a data controller and request the information's removal from the internet. In the case of the *defamation by social media* scenario, it is straightforward to ascertain who a potential controller is – either the website themselves or, alternatively, the person who has posted the offending statement in question. This is because Article 4(7) UK GDPR has a wide definition of 'data controller' as either an entity or a natural person that determines the processing of personal data – and processing, according to Article 4(2), catches almost all functions one could perform with information, such as 'structuring,

[34] UK GDPR, Article 83(1).

storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available'.[35] Similarly, if a person is defamed by an *AI tool* such as a chatbot on a AI website, one could contact the website as a controller for those purposes, or any third party who further disseminates the information online. This route to remedy is clearly not as lengthy, costly or complex as mounting a formal legal action in defamation. On instruction of a law firm to argue a case in defamation, the wait to trial in the English and Welsh jurisdiction would also likely be significant,[36] as both County Court and High Court waiting times in the wake of the COVID-19 pandemic are lengthy,[37] and prove a very real barrier to the sort of swift justice one would wish to obtain in defamation – as the longer the defamatory remark is able to percolate online, the more harm to reputation (and personal dignity) accrues. Conversely, to invoke the RTBF, all, in theory, an individual needs to do is to request the information's erasure from a data controller. This initial point of contact would be quick to make – those defamed online could likely make contact with a controller by email. There will, of course, be a waiting time between this request and any response, although large conglomerates such as Google now appear to have streamlined processes for such a request down to a fine art, with particular forms that need to be filled out by the data subject,[38] and specific teams responsible and

[35] UK GDPR, Article 4(2).

[36] See John Hyde, 'Litigants now wait 78 weeks for their County Court date' (*Civil Mediation Council*, 2023) https://civilmediation.org/78-weeks-wait-for-court-date/ accessed 24 January 2025.

[37] See ACSO, 'Record court waiting times mean UK has a third-rate justice system' (7 December 2023) https://acso.org.uk/news/202312/record-court-waiting-times-mean-uk-has-third-rate-justice-system accessed 24 January 2025.

[38] See Google, 'Legal help: Right to be forgotten overview' https://support.google.com/legal/answer/10769224?hl=en-GB accessed 24 January 2025.

dedicated to handling the requests.[39] Of course, if the data controller refuses to comply and the individual concerned is not satisfied with any explanation given for refusing the request (such as linked to a relevant exemption), the matter could then be referred to the UK's Information Commissioner's Office and ultimately be adjudicated in court – which would mean that the litigant would suffer the same lengthy wait times as they would pursuing an action in traditional defamation law. However, there is every chance that this will not happen – many erasure requests are straightforwardly upheld after a request is lodged, and it has been reported that Google has deleted approximately 2.5 million web links since 2014.[40] This option for a timely remedy of personal data erased (be it false and defamatory or otherwise) is something that defamation law, unlike the RBTF, simply cannot provide.

Further, the cost of litigation is another area where the RTBF will likely have an advantage for those seeking redress when defamed online, in comparison to an action in defamation law. The 'Wagatha Christie' defamation litigation in 2021 demonstrated the sheer cost of launching (and defending) a libel trial, 'with costs for both parties estimated to be in excess of 1 million'.[41] In the event that a defamation case is lost by a claimant – which, as demonstrated by the previous chapter, is always possible due to the many different hurdles a defamation claim can fall at – then a *defendant's* costs are

[39] Cohen Davis Solicitors, 'Right to be forgotten' https://arighttobeforgotten.co.uk/right-to-be-forgotten-google#:~:text=Between%20June%202014%20and%20November,to%20nearly%204%20million%20links last accessed 24 January 2025.

[40] See 'How many people in Europe use their "right to be forgotten" online?' (*Surfshark*, 28 February 2024) https://surfshark.com/blog/right-to-be-forgotten-requests accessed 24 January 2025.

[41] James Martin, 'High profile case shines light on expensive costs in defamation claims' (*Blacks Solicitors*, 16 May 2022) www.lawblacks.com/2022/05/16/high-profile-case-shines-light-on-expensive-costs-in-defamation-claims/ accessed 24 January 2025.

likely to be absorbed by the claimant as well as their own, as was the case for Rebekah Vardy in *Vardy v Rooney*. Ms Vardy was recently ordered to pay 90 per cent of defendant Coleen Rooney's legal costs on top of her own legal fees, Rooney's costs amounting to £1.8 million pounds[42] (an order she sought to challenge, although the matter is now settled).[43] This serves to show that lengthy costs disputes in defamation can also prolong defamation litigation and, somewhat ironically, generate even higher legal bills for an unsuccessful claimant. The peril of an ordinary individual seeking to fund an action in defamation, much less pay an opposing party's costs, is a powerful disincentive for individuals seeking to use defamation law to obtain a remedy. This is in contrast with the RTBF, where an initial erasure request can simply be made to a data controller – by either email, form or letter – free of charge. If the matter does not escalate to litigation, then no costs will be accrued. Contacting the UK's Information Commissioner's Officer (ICO) to obtain information is also free of charge, with the ICO potentially acting as an intervener if the matter were to be escalated to a court.[44]

Finally, the RTBF has the advantage of simplicity over any potential litigation in defamation law. The public are readily

[42] *Vardy v Rooney* [2021] EWHC 1888 (QB) and Julie Hamilton, '"How much?" Wagatha Christie trial back in the headlines' (*Morton Fraser Macroberts*, 8 October 2024) www.mfmac.com/insights/litigation-dispute-resolution/how-much-wagatha-christie-trial-back-in-the-headlines/#:~:text=The%20news%20of%20the%20%22sheer,have%20reached%20%C2%A31.8M accessed 24 January 2025.

[43] Adele Whaley and Kirstie Goulder, '*Vardy v Rooney*: The saga continues (the costs era)' (*Greenwoods*, 29 October 2024) www.greenwoods.co.uk/article/vardy-v-rooney-the-saga-continues-the-costs-era/ accessed 24 January 2025 and see Paul Glynn, 'Vardy must pay £1.4m of Rooney's "Wagatha" legal costs' *(BBC News*, 6 May 2025) https://www.bbc.co.uk/news/articles/c7939wwxd0jo accessed 23 July 2025.

[44] As was the case in *NT1 and NT2 v Google LLC (Intervenor: The Information Commissioner)* [2018] EWHC 799 (QB).

aware of their RTBF: as discussed earlier in this chapter, the *Google Spain* judgment handed down by the CJEU in 2014 achieved widespread academic, political and press attention across Europe, as well as Article 17's presence in early drafts of the EU Commission's 2012 GDPR.[45] Therefore, people may be feel increasingly confident to write to data controllers and request the removal of information, with the awareness that such a right not only exists, but is now commonplace. There is evidence that people are utilizing the RTBF in large numbers: between 2014 and 2020, nearly 4 million links were requested for deletion by Google.[46] Writing to a data controller, or filling in a relevant form to request a RTBF, is typically also far more straightforward than engaging a solicitor (who then instructs a barrister) and mounting a trial in defamation, and it is considerably less daunting to those not familiar with the legal system.

II. Hurdles to making a claim

One of the strongest arguments in favour of the RTBF as a method of obtaining redress for those defamed online (in comparison to defamation law) is the lack of legal hurdles

[45] See, for example, European Union Committee, 'EU Data Protection Law: A "Right to be forgotten"?' (HL 2nd report of session 2014–15) paper 40; Meg L Ambrose, 'It's about time: Privacy, information life cycles, and the right to be forgotten' (2013) 16(2) *Stanford Technology Law Review* 369; Jeffrey Rosen, 'The right to be forgotten' (2012) *Stanford Law Review Online* 88; Diane L Zimmerman, 'The "new" privacy and the "old": Is applying the tort law of privacy like putting high button shoes on the internet?' (2012) 17 *Communications Law and Policy* 107; Paul Schwartz, 'The EU–US privacy collision: A turn to institutions and procedures' (2013) 126 *Harvard Law Review* 1966; and W. Gregory Voss, 'One year and loads of data later, where are we? An update on the proposed European Union General Data Protection Regulation' (2013) 16(10) *Journal of Internet Law* 13.

[46] See (n 39).

necessary to be surmounted to assert the right. If a person withdraws consent to processing, objects to said personal data's processing or the processing is otherwise unlawful or unnecessary,[47] as discussed in earlier in this chapter, an individual can invoke their Article 17 rights. The definition of 'personal data' in the UK GDPR is similarly extremely broad:

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[48]

This catches all (potentially) defamatory statements made online that reference the given claimant. The very point of the RTBF is that it is one of a number of data subject rights introduced by the GDPR to rebalance the control over personal information online against unbridled free expression.[49] The central thesis behind the GDPR's adoption was that more needed to be done to protect personal data online,[50] and by very essence, reliance on the right was intended to be easy and the right strong. The only requirement to initially invoke the right is that the information in question must be personal data, which, as can be seen earlier in this chapter, is broadly defined. As shown through the analysis conducted in Chapter 3, a plethora of legal hurdles must

[47] According to UK GDPR, Article 17(1)(a), (b), (c) and (d).
[48] UK GDPR, Article 4(1).
[49] UK GDPR, Articles 12–23.
[50] Reding (n 5).

be met by a claimant for an action in defamation – there must be a defamatory statement, it must meet the serious harm threshold, there must be reference to the claimant and requisite communication (publication). Unlike s 1(1) of the Defamation Act 2013 there is no threshold of severity to invoke the RTBF as it is a broad data right and there is no time constraint operational as to *when* a data subject must invoke their right (such as the limitation period in s 8 Defamation Act 2013), relevant to the *repetition of statements online over a year later* scenario. To the contrary, the Strasbourg Court and the CJEU have both noted that the longer the passage of time between the information in question and the right being invoked, the stronger a claim for the information's removal in the event that a RTBF is contested.[51]

Another barrier that defamation law presents is the number of defences available to defendants on receipt of a defamation lawsuit. Aside from the new s 5 defence that shields operators of host websites,[52] there are numerous other defences operable to defend against a claim, such as the truth defence, honest opinion, publication on a matter of public interest and the (second) new defence introduced by the 2013 Act – protection for those writing in peer-reviewed journals.[53] When reading a judgment in English libel law, it is perhaps the only tort where judicial consideration of defences is often more lengthy than the claim itself. For example, in the High Court decision of *Banks v Cadwalladr* (concerning comments made in a TED talk and a tweet), Mrs Justice Steyn's consideration of a defence amounts to over 300 paragraphs.[54] To compound this, the 2013 reform put the defences of justification, fair comment

[51] As was the case in *Google Spain* and *Hurbain v Belgium* (App no 57292/16, 4 July 2023) [220]–[221].

[52] Defamation Act 2013. Discussed at length in Chapter 3.

[53] Section 6 Defamation Act 2013.

[54] *Banks v Cadwalladr* [2022] EWHC 1417 (QB) [100]–[415].

and *Reynolds* on a statutory footing.[55] The rapid pivot of the reform to prioritize expression has meant that aspects of the traditional defences have also been reinterpreted and their scope broadened. As discussed in Chapter 3, honest opinion in s 3 of the Act no longer has to relate to a matter of public interest, which was previously a requirement of the defence at common law.[56] What was previously known as the *Reynolds* defence now lives on in s 4 of the 2013 Act and has undergone the most significant changes from its common law predecessor. Section 4 is quite considerably broader in nature, as the standard of responsible journalism has (at least in statute) been abandoned as a benchmark to rely on the defence: instead, one must have reasonable belief that publication is in the public interest according to s 4(1)(b) and the publication itself must relate to a matter of public interest in s 4(1)(a).[57] This standard is now so wide that so-termed citizen journalists can rely on this defence, in certain circumstances.[58] By way of comparison with the RTBF, the main 'defence' for a data controller to refuse compliance with an erasure request under Article 17 is the 17(3)(a) exception outlined earlier, pertaining to freedom of expression. There is little said about this exemption in the UK (or EU) GDPR itself. If a RTBF request was refused and the matter litigated, to successfully argue that expression should trump an erasure right, the public interest would likely have to be *sufficiently* engaged under Article 17(3)(a). This accords with both Strasbourg and English case law on this matter, particularly in the field of misuse of private

[55] Now s 2 (truth), s 3 (honest opinion) and s 4 (publication on a matter of public interest) Defamation Act 2013.

[56] See, for example, *Telnikoff v Matusevitch* [1992] UKHL 2, [1992] 2 AC in 343. Also see Eric Descheemaeker, 'Mapping defamation defences' (2015) 78 *Modern Law Review* 641, 652ff.

[57] Defamation Act 2013.

[58] Such as in *Economou v De Freitas* [2018] EWCA Civ 2591, EMLR 7 and *Hay v Cresswell* [2023] EWHC 882 (KB), EMLR 17.

information – when Article 8 ECHR rights (privacy) and Article 10 (expression) rights must be weighed against each other, in cases such as *Von Hannover* (Nos 1, 2 and 3), *Axel Springer*, *PJS*, *Campbell* and *Ferdinand*.[59] Given that the purpose of the RTBF's drafting was to reinstate the informational autonomy of data subjects, any public interest claim that would negate a RTBF would have to be robustly argued. There are two other relevant 'defences' for the RTBF (for the purposes of this book): the *domestic purposes* exemption and the *journalistic* exemption. The 'domestic purposes' exemption exempts application of the GDPR to 'the processing of personal data by a natural person in the course of a '*purely personal or household activity*'.[60] This, of course, has the potential to include posts to social media. However, case law and academic commentary has shown that if the personal data in question is posted to a large group or audience (as is often the case on social media websites), then the domestic purposes exemption will not apply.[61] In the *defamation by social media* scenario, defamatory posts online will often be public or published to a section of

[59] *Von Hannover v Germany*, App no 59320/00 (ECHR, 24 September 2004); *Axel Springer AG v Germany* App no 39954/08 (ECHR, 7 February 2012) App nos 40660/08 and 60641/08 w/ *Von Hannover v Germany (No 2)* (7 February 2012); *Von Hannover v Germany (No 3)* App no 8772/10 (ECHR, 19 September 2013); *PJS (Appellant) v News Group Newspapers Ltd (Respondent)* [2016] UKSC 26; *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457; *Ferdinand v MGN* [2011] EWHC 2454 (QB). More will be said on this balancing exercise and how it should be conducted in RTBF cases later in this chapter.

[60] UK GDPR, Article 2(2)(a).

[61] David Erdos, "Beyond "having a domestic"? Regulatory interpretation of European data protection law and individual publication" (2017) 33(3) *Computer Law and Security Review* 275, 276; and Case C-101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* [2003] ECR I-12971 [47]; Fiona Brimblecombe and Gavin Phillipson, 'Regaining digital privacy? The new "right to be forgotten" and online expression' 4(1) *Canadian Journal of Comparative and Contemporary Law* 1, 29.

the public – this is how significant reputational and personal dignity harm is rendered. As such, this exemption should not prove a barrier to invoking a RTBF with respect to potentially defamatory posts on the internet.

There is also a journalism exemption instructed by the GDPR, present in the annexed Data Protection Act (DPA) 2018. In this Act, the journalistic exemption appears in Schedule 2, paragraph 26. It states that if activities are carried out for the 'purposes of journalism'[62] and

> with a view to the publication by a person of journalistic material [and] the controller reasonably believes the publication of the material would be in the public interest … the listed GDPR provisions do not apply to the extent that the controller reasonably believes that the application of those provisions would be incompatible.[63]

These provisions include Article 17. The exemption goes on to issue a caveat: 'in determining whether publication would be in the public interest the controller must take into account the special importance of the public interest in the freedom of expression and information'.[64] This means that a data controller must think it impossible to apply the relevant UK GDPR provision (in this case the RTBF) while acting in a journalistic way.[65] This exemption is reminiscent of Article

[62] DPA 2018, Schedule 2, para 26(1).

[63] Ibid para 26, section (2)(a), (b) and section (3).

[64] Ibid para 26, section (4).

[65] See UK Information Commissioner's Office, 'Data protection and journalism: A guide for the media' https://ico.org.uk/media2/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf accessed 14 March 2019; and Hugh Tomlinson, 'The "journalism exemption" in the Data Protection Act: Part I, the law' (*Inforrm*, 28 March 2019) https://inforrm.org/2017/03/28/the-journalism-exemption-in-the-data-protection-act-part-1-the-law-hugh-tomlinson-qc/ accessed 14 March 2019.

17(3)(a) in the sense that it will ultimately collapse into a 'personality interests versus freedom of expression' balancing exercise in the event that a RTBF's refusal is contested on these grounds. It is unclear at this point precisely how broadly the 'public interest' will be construed under Schedule 2, 26(2)(b). As has been demonstrated by misuse of private information case law, the English courts have been known to adopt inconsistent approaches to this concept.[66] Defendants can more persuasively argue that the exemption should apply when the subject matter of the information at issue is of 'great interest to the public'.[67] It is also unclear if citizen journalists will be covered by Schedule 2's journalism exemption. This author has observed elsewhere that the CJEU in *Google Spain* held that search engine Google could *not* rely on the journalism exemption present within the DPD '95,[68] and nor could it in *NT1 and NT2* in the English jurisdiction.[69] Indeed, to allow citizen journalists broad access to the journalistic exemption would carve away the genuine definition of what it is to be a journalist.[70] The 2018 Act suggests that citizen journalists were not intended to be covered by the exemption in most circumstances, as a data controller must adhere to a relevant privacy code.[71] As Mr Justice Warby has stated, not every transmission of ideas on the web is journalistic[72] – and to rely on the journalistic exemption, the publication in question must

66 See *Ferdinand* and *PJS* (n 59).

67 See, for example, counsel submissions of Bloomberg in *ZXC v Bloomberg* [2017] EWHC 328 (QB) [15].

68 Brimblecombe and Phillipson (n 61) 34–5.

69 See *NT1 and NT2* (n 44).

70 Brimblecombe and Phillipson (n 61) 35–6.

71 DPA 2018, Schedule 2, Part 5, para 26(5). On codes, see Peter Coe, 'A journalism Standards Code for modern journalism' (2023) 28(2) *Communications Law* 49.

72 *NT1 and NT2* (n 44) [98]. Also see Peter Coe, *Media Freedom in the Age of Citizen Journalism* (Edward Elgar 2021).

be 'properly characterised as journalism'.[73] As such, it appears that the journalistic defence in the DPA 2018 is now narrower than the s 4 'publication on matter of public interest' defence in the Defamation Act 2013, which relinquished its standard of responsible journalism on codification.[74] It is clear, then, that the broad array of defences operable in the English jurisdiction of defamation law are more numerous and extensive than those present in the UK GDPR.

III. Decision making

Another interesting point of comparison between the RTBF and English defamation law is the body which is responsible for deciding whether a claim is upheld. As explained, in the first instance, a data subject simply writes to a data controller to assert their RTBF and in that sense data controllers make the first – and possibly only – decision about whether information should be erased. This approach comes with advantages and disadvantages. The clear advantages of this process are ease, speed and time. As Google (for example) now receives many such requests, they have a dedicated team in place to assess whether the RTBF applies and whether any exemptions override such a request. Google is most likely to refuse a request not because an exemption applies, but because the request itself does not contain enough information.[75] Google employees involved in the initial assessment exercise also escalate number of requests to a specialist legal team to ensure the most informed decision is made.[76] Factors that may influence a decision to uphold a RTBF include whether a person is in the public eye, the nature of the information and

[73] Ibid (*NT1 and NT2*).

[74] Fiona Brimblecombe, 'Section 4 Defamation Act 2013: A tale of two approaches' (2024) 29(3) *Torts Law Journal* 245.

[75] See n 39.

[76] Ibid.

the public interest value of the information.[77] It was clear from the outset that the balancing factors of 'celebrity' and 'nature of the information' on the one hand and 'public interest' on the other would likely be applied to erasure requests by data-controller assessment teams.[78] This is because these are factors that English and Strasbourg courts use when conducting the 'ultimate balancing exercise' between privacy interests and competing freedom of expression concerns.[79] This balancing exercise is also the essence of the Article 17(3)(a) exemption to the RTBF. Other relevant factors to this balance may be: if the person concerned has '*waived*' their right to privacy (or perhaps a good reputation),[80] *circumstances* that the information was obtained in and if the information relates to a *private or public place*.[81] From the little information we know about what goes on in online conglomerates, it appears that at least some of these factors are being utilized to assess whether an erasure request under Article 17 is upheld. However, it is important to note that this range of guiding principles have not always been used logically by the Strasbourg and English courts and there is always the risk that data controllers – being less well versed in legal precedent – may interpret these factors in a way which unfairly negatively impacts a legitimate RTBF request. For example, the European Court of Human Rights (ECtHR) has made it clear that even if someone is a public figure, they

77 Ibid.

78 Fiona 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.

79 See, for example, Paul Wragg, 'Protecting private information of public interest: Campbell's great promise, unfulfilled' (2015) 7(2) *Journal of Media Law* 225 and Rebecca Moosavian, 'A just balance or just imbalance? The role of metaphor in misuse of private information' (2015) 7(2) *Journal of Media Law* 196.

80 Which will be returned to later in the discussion of *Hurbain*.

81 Brimblecombe and Phillipson (n 61).

still have a 'legitimate expectation of the protection of and respect for his or her private life' under Article 8 European Convention on Human Rights (ECHR).[82] Therefore, any decision automatically refusing a RTBF request on the basis that the person asserting it is well known is a misinterpretation of precedent.[83] There have been academic concerns voiced about the validity of the balancing criteria expounded by the English courts, particularly in relation to factors going to the weight of a competing expression interest.[84] Most notably, the 'role model argument' (which states that if a claimant is a role model that the information in question should lean towards publication) and the 'right to criticise' (which argues that information should be published if it prompts debate) are two of the more egregious examples of poorly reasoned 'balancing factors' employed by the English courts in this respect.[85] These missteps come as a stark warning that any balancing exercise articulated either by data controllers or the judiciary in assessing whether the RTBF is upheld must be trod carefully if similar mistakes are to be avoided. The RTBF presents an opportunity to articulate a new set of balancing factors more appropriate for the digital age; this course has begun to be chartered – with mixed success – via the 2023 case of *Hurbain* at the Grand Chamber of the ECtHR.[86] In the case, the Grand Chamber applied a modified version of previously articulated Article 8 and 10 factors in assessing whether a RTBF's enforcement was compatible with Article 10.[87] The new list of balancing factors given in *Hurbain* were: 1. *the nature of the information*, 2. *the time*

[82] *Lillo-Stenberg and Sæther v Norway* App no 13258/09 (ECHR, 16 January 2014) [97].

[83] See also *Couderc and Hachette Filipacchi Associes v France*, App no 40454/07 (ECHR, 12 June 2014) [84].

[84] Brimblecombe (n 78).

[85] Ibid.

[86] *Hurbain v Belgium* (n 51).

[87] Ibid [214]–[253].

elapsed, 3. *contemporary interest*, 4. *whether the person is well known and their conduct since the events*, 5. *negative repercussions for them*, 6. *degree of accessibility*, 7. *impact on freedom of expression*.[88] It is easy to see how each of these factors could be applied to a RTBF request with respect to personal information online that is false and defamatory. While certain factors elucidated in *Hurbain* should be welcomed, it is argued here that others are less helpful and should only be used by courts with caution (if at all). The factor of the *nature of the information* in question is clearly important and relevant if a RTBF is in dispute (and to the question of the applicability of an exemption such as Article 17(3)(a) UK GDPR). In *Hurbain*, perhaps predictably, the Strasbourg Court considered whether the information was 'sensitive' and falls within the scope of a person's private life or instead the public sphere[89] – this accords with earlier Strasbourg precedent in privacy cases, such as the famous cases of *Von Hannover*. It should be noted that the concept of the RTBF, as least as far as it arises out of the GDPR, does not, in principle, rely on information's sensitivity or 'private nature' – however, in situations which a RTBF is contested in a court (perhaps annexed to a 'defence' or exemption), it is clear that this factor may become relevant. *Hurbain* also raised the importance of the journalistic nature of the material[90] – which, of course, is also relevant to the journalistic defence in the UK GDPR/DPA 2018 and Article 17(3)(a)'s exemption. The Strasbourg Court in *Hurbain* also gave weight to the amount of *time that had elapsed* since the events and the article's publication online.[91] This was particularly relevant as the article in question related to G (a doctor) causing a fatal road traffic accident in 1994.[92] The article was placed in online archives

[88] Ibid.
[89] Ibid [214].
[90] Ibid [216].
[91] Ibid [220].
[92] Ibid. See opening matters.

in 2008 and G had been rehabilitated in 2006: the court held that G 'had a legitimate interest, after all that time, in seeking to be allowed to reintegrate into society without being permanently reminded of his past'.[93] While this balancing factor of elapsed time was of clear relevance to *Hurbain* given that the RTBF had been claimed by a rehabilitated, past offender, the passage of time may not always be – and should not always be – a pivotal factor in a RTBF claim. It is important to remember that the spirit of the RTBF is the idea of individual autonomy – that is, that someone can invoke the right because they no longer wish the information to be accessible on the web – to which the length of time is a factor that may *not* be relevant.[94] Indeed, if one was to find that a RTBF was only accessible to (for example) online posts detailing matters of the distant past in a general fashion, the right would be too narrowly constrained – and clearly would not align with the intentions of the EU drafters of Article 17. It is important to raise caveat here to say that in cases involving *past criminal behaviour* (such as in *Hurbain* itself), this factor may well be a legitimate consideration, due in part to the concept of rehabilitation of offenders. It is merely submitted here that this time factor ought not to be encouraged to grow and apply to all RTBF litigation *more generally*, to a range of different factual scenarios. The Grand Chamber in *Hurbain* also delivered precedent pertaining to the concept of the public interest in the context of RTBF claims; this is helpful as this matter has not been clarified by the UK GDPR, DPA 2018 nor subsequent English case law. *Hurbain* states: 'the public interest relates to matters which affect the public to such an extent that it may legitimately take an interest in them, which attract its attention or which concern it to a significant degree, *especially*

[93] Ibid [220]–[221].

[94] Ibid. As is the spirit behind the slew of 'rights of the data subject' present in the GDPR, Articles 12–23.

in that they affect the well-being of citizens or the life of the community'.[95] The court went on to elaborate that such an interest would arise if the matter was an important 'social issue',[96] and that public interest is not merely the same thing as the public's 'thirst'[97] for information about people's personal lives. The court then noted that the concept of the public interest would not always be 'decisive', as the concept's applicability can wane or change over time.[98] This is interesting, as it perhaps marks a point of departure from the Strasbourg conception of a RTBF and that arising out of Article 17 UK GDPR. It is argued here that the public interest *is* likely to be a determinative factor in future English RTBF litigation concerning the application of Article 17(3)(a)'s freedom-of-expression exemption. Indeed, it is likely already a latent decisive factor employed by in-house legal teams assessing whether a data subject's RTBF request is upheld. This is because the concept of the public interest enjoys a place of pivotal importance in English privacy jurisprudence with regard to misuse of private information case law. The comparison between RTBF claims and misuse of private information jurisprudence in the English jurisdiction cannot be ignored – one will doubtless have influence on the other.[99] It will be of great interest to lawyers in this area to see how the concept of the public interest is shaped in relation to contentious RTBF claims in the future, particularly in the English jurisdiction. Finally, in *Hurbain*, the court considered the *conduct* of the RTBF subject relevant to whether the right

[95] Ibid [223].
[96] Ibid.
[97] Ibid.
[98] Ibid [224].
[99] For discussion of one's influence over the other generally, see Fiona Brimblecombe and Helen Fenwick, 'Keeping control of personal information in the digital age: Efficacy and equivalence of tortious and GDPR/DPA relief?' (2022) 138 Law Quarterly Review 456–80.

ought to be upheld in accordance with the Convention. The ECtHR noted that 'there is nothing to suggest that G. made contact with the media in order to publicise his situation … on the contrary, all the steps taken by him demonstrate a desire to stay out of the media spotlight'.[100] This is the concept of 'waiver'; the idea that a claimant (often, in privacy law) can waive their privacy rights of the future by previous solicitation of publicity. The factor has been utilized at times by the English courts to block access to redress for invasions of privacy by the press. This factor is problematic for one key reason: that it ignores the agency of the given claimant in asserting their privacy interests on the later occasion, given that some information may be more private than others – and also the idea that a person can change their mind or their feelings about the degree to which they want their personal information to be a matter of public knowledge. This author has criticized this factor's employment in judicial reasoning elsewhere,[101] and it is disappointing to see its echoes in *Hurbain*, even faintly. As can be seen from the critique given here, there is more work still to do in improving and clarifying relevant factors to be used when deciding RTBF claims. This is unsurprising, as the right is, after all, young.

Turning back to the notion of decision makers themselves, unlike the RTBF, in defamation law the adjudicators of an action are solely the English judiciary (and not online 'controllers'). Although undoubtedly experts on the law, Chapter 3 has shown that there is much work the judiciary must do to effectively protect claimants against the rise of online defamation. The Defamation Act 2013 worked to impede the expansion of defamation law at a crucial time when more protection was needed to combat against increased infringements of reputation online. Set in this context of

[100] *Hurbain v Belgium* (n 51).
[101] See Brimblecombe and Phillipson (n 61) Part V, D.

judicial apathy, there is no advantage to claimants in a matter being adjudicated traditionally in court (in defamation law) when compared with assessment by a data controller on receipt of a RTBF request. That being said, there are, of course, legitimate concerns about the level of power and responsibility vested in data controllers, which are often private companies, when assessing a RTBF: as Ambrose observes, this 'places a huge, huge burden on them but also gives them a lot of power'.[102] However, with current judicial and legislative trends narrowing successful defamation suits, as demonstrated by Chapter 3, there is no more reason to fear adjudication by a private company than by the English judiciary in the case of online defamation.

IV. Ex post *remedies*

Both defamation law and the RTBF offer *ex post* remedies, in the sense that neither Article 17 nor libel law currently operates a mechanism to prohibit reputationally damaging falsities initially being uploaded to the internet. Rather, both seek to combat this issue after disclosure has occurred. As argued, in the event a potentially defamatory statement has been made online, the RTBF will often afford a timelier solution for the information's removal than litigation in defamation law. A long-standing common law rule forbids the issuing of interim injunctions in defamation in most

[102] Meg Leta Ambrose, Georgetown University. See James Doubek, 'Google has received 650,000 "right to be forgotten" requests since 2014' (*NPR*, 28 February 2018) www.npr.org/sections/thetwo-way/2018/02/28/589411543/google-received-650-000-right-to-be-forgotten-requests-since-2014 accessed 26 January 2025. 'EU Court tells Google that people have "the right to be forgotten"' (*NPR*, 13 May 2014) www.npr.org/2014/05/13/312197640/eu-court-tells-google-that-people-have-the-right-to-be-forgotten accessed 24 July 2025.

circumstances,[103] unlike defamation law's sister tort: misuse of private information. It has been argued elsewhere by this author that interim injunctions should be read-in to Article 17 by members of the judiciary in order that they apply to RTBF requests.[104] The tort of misuse of private information and data protection law have sufficiently converged in the English legal system for this to be done, due to the fact they are often considered in tandem in case law; the misuse tort having influence and effect on how the UK GDPR is interpreted in this sense.[105] This argument could (and should) be made by entrepreneurial counsel to best protect personality interests on the web. Further, if this argument *is* accepted in future, the RTBF will cease to operate as an *ex post* remedy – but will also have the force of providing an initial injunction much like the misuse tort, something that defamation law does not provide.

It also must be noted that under Article 17 a data subject can request erasure of their personal data from a secure database *outside of the public domain*. There is always the potential for a database that is initially private to later become public – so, in certain limited circumstances, the RTBF does not solely operate as an *ex post* remedy and can work in these cases to prevent later disclosures of personal (and potentially defamatory) information.

V. The 'right to be forgotten' and the data-dissemination *scenarios*

It is important to turn to the *data-dissemination* scenarios outlined at the beginning of this book and look at how a claimant in each particular scenario might fare differently when

[103] In most circumstances. See Gavin Phillipson, 'The "global pariah", the Defamation Bill and the Human Rights Act' (2012) 63(1) *Northern Ireland Legal Quarterly* 149, 155.

[104] Brimblecombe and Fenwick (n 99) 456.

[105] Ibid.

claiming a RTBF rather than taking action via defamation law. In the *defamation by social media* scenario, for a claimant to assert their rights under Article 17 they need only write to the data controller to demand the information's erasure. This could be a large company such as Facebook or X, or a smaller social media website. As outlined, the definition of data controller in Article 4 UK GDPR is so broad that a website operator or the defamatory information's poster could be classed as a controller; a data subject would be free to write to either.[106] As social media websites are providing a service to users in the UK, the UK GDPR will have extraterritorial effect (even if the websites are domiciled elsewhere).[107] As discussed, large social media websites will already have a strategy in place to assess RTBF requests, with a team likely considering certain factors that add to weight to the claim and any exemptions. Similarly, in the *third-party poster* scenario, a defamed individual would be free to assert their RTBF addressed to the host website as a controller, particularly in the event that the third-party poster themselves may be uncontactable. This would be the same if someone was defamed in a 'virtual world'. If a person was defamed by an *AI tool*, the website where this defamatory remark has been made available would likely fall under the Article 4(7) UK GDPR definition of controller, such that a RTBF claim could be made against them; or in the alternative, the AI tool's manufacturer could be deemed as a controller, as they could be seen as the 'body which, alone or jointly with others, determines the purposes and means of the processing of personal data'.[108] If the defamatory remark was repeated over a year later by the same publisher online, this would not bar any claim made under a RTBF: on the contrary, Article 17(2) takes active steps to prevent such a

[106] UK GDPR, Article 4(7).
[107] See UK GDPR Article 3(1) and 2(a).
[108] UK GDPR, Article 4(7).

repetition, by requiring that controllers who are subject to a RTBF request to 'take reasonable steps, including technical measures, to inform [other] controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data'.[109] This is strikingly different from the position of English defamation law with s 8.

VI. Future of the 'right to be forgotten' in UK and European law

This chapter has shown that, for a number of different reasons, the RTBF as a route to remedy for defamatory statements posted online has a number of distinct advantages over litigating in defamation law. However, it is important to also state that there is always more that can be done in order to protect personal reputation and dignity in the face of the rapid rise of defamatory remarks made on the web. There have been a number of RTBF-style cases heard at the Strasbourg Court since the CJEU's *Google Spain* decision, most notably *Hurbain*,[110] as already discussed in this chapter, but also the earlier cases of *M.L. and W.W. v Germany* and *Biancardi v Italy*.[111] *Biancardi* was decided in 2021 before the pivotal case of *Hurbain* and was a more modest early foray into establishing a pattern of judicial reasoning, applicable at the Strasbourg Court, to RTBF decisions. The applicant, who was the editor of an online newspaper, had, in 2008, published an article concerning a fight at a restaurant.[112] The applicant was asked by one of the people involved in the fight and the restaurant itself in 2010 to remove the article from the internet, which he did

[109] UK GDPR, Article 17(2).
[110] *Hurbain v Belgium* (n 51).
[111] *M.L. and W.W. v Germany* App nos 60798/10 and 65599/10 (28 June 2018). *Biancardi v Italy* App no 77*419/16* (25 November 2021).
[112] *Biancardi v Italy* (n 111) [5].

not do.[113] However, at a later hearing in 2011 the applicant admitted that he had de-indexed the article, resulting in it being harder to find.[114] The applicant editor was given a fine in the domestic Italian courts for breaching the claimant's 'reputation' as well as the relevant national law, the Personal Data Protection Code, and this decision was upheld by the domestic Supreme Court.[115] He claimed that his Article 10 rights had been infringed in so doing. The ECtHR, however, found no violation had taken place in *Biancardi*; it is a short judgment at 24 pages, and only 5 of those pages form a substantive assessment of the merits of the case. The court explained that the crux of the matter was the applicant's failure to de-list or de-index the article – and this is what the relevant issue was in the domestic courts.[116] In *Biancardi*, the Strasbourg Court used Article 8–10 – 'balancing factors' elucidated in the 2012 case of *Axel Springer* – as a starting point to assess whether there was a violation of Article 10.[117] This was undoubtedly a misstep, as the factors elucidated in *Axel Springer* more strongly relate to press intrusion into the lives of celebrities by the traditional media, as per the facts of the case (and many other Strasbourg cases that followed).[118] For this reason, these factors are largely outdated and of only limited help when considering Article 8–10 rights and the balance to be struck in RTBF-style claims. A RTBF arising from either *Google Spain* or Article 17 GDPR has a different context and aim to the Strasbourg jurisprudence arising out of the traditional, press intrusion cases of the 1980s, 1990s and 2000s, both in the ECtHR and the English courts. Interestingly, the ECtHR seemed aware that it was following

[113] Ibid [8].
[114] Ibid [10].
[115] Ibid [13] and [14].
[116] Ibid [59].
[117] Ibid [61].
[118] See n 59.

the incorrect approach for these very reasons in *Biancardi*;[119] ultimately, *Biancardi* has been superseded by the judgment of *Hurbain* in the Grand Chamber as earlier discussed, which was considerably more detailed in setting out new criteria for assessment in RTBF case law at Strasbourg.

Although the ECtHR's case law has been active, particularly with regard to RTBF requests relating to criminal pasts,[120] the same cannot be said of case law in the English jurisdiction. Aside from *NT1 and NT2* discussed previously,[121] in 2022 there was another English case concerning spent convictions, *ABC*.[122] In *ABC*, the claimant had pled guilty to nine counts of fraud in a Magistrates Court in 2015.[123] The defendant was a journalist and a court reporter, and the matter complained of was a factual, court report of the case on the journalist's blog.[124] The claimant ran a variety of actions against the blog post (including claiming it was misuse of private information and harassment),[125] but most notably argued that she had a 'right to be forgotten' under Article 17 after her convictions became spent in 2017.[126] The Court in *ABC* found it relevant that the claimant 'has not been rehabilitated by her convictions and sentence' as she had asserted her innocence on multiple occasions following her convictions.[127] The blog had been

[119] But it did not go as far as rectifying this to elucidate new factors of assessment. See *Biancardi v Italy* (n 111) [63].

[120] Mikel Anderez Belategi, 'The right to be forgotten concerning the criminal past: Developments in the case law of the European Court of Human Rights with particular reference to the anonymisation of digital press archives' (2024) 14(4) *Oñati Socio-Legal Series: The Influence of New Technologies on Law* 1639.

[121] See n 44.

[122] *ABC v Palmer* [2022] EWHC 3128 (KB).

[123] Ibid [2].

[124] Ibid [3].

[125] Ibid [5].

[126] Ibid.

[127] Ibid [49].

taken down permanently in May 2021.[128] However, before this, it was made public again by the defendant between June 2020 and May 2021, but the Court found this fell under the defendant's right to freedom of expression, as the claimant was making false claims about him 'and the events he had witnessed [in the Magistrates Court] at the time', and therefore the GDPR had not been breached.[129] Both *NT1* and *ABC* are low-level decisions, and hardly amount to a flood of caselaw on the RTBF. *ABC* follows *NT1* rather than adds to existing precedent.

There may be a number of reasons for the drought in English RTBF-style case law. Firstly, RTBF requests are often sent by private individuals and then examined and assessed privately by data controllers, who are themselves either private individuals or employees at a large company. On the outcome of such a request, the person who made it may either be satisfied or choose not to take the matter further, perhaps due to reasons supplied by the controller in the event that an erasure request is denied (for example, someone may feel that the public interest may be sufficiently engaged to warrant the request's refusal). This is a private loop and, as such, requires no court involvement – and generates no case law. Secondly, in the case of the UK, the ICO would normally be expected to 'intervene' if an appropriate matter is brought to their door – such as a failure to uphold what appears to be a legitimate erasure request – and partner with a claimant in bringing the matter in question before an English court on the basis of Article 17 UK GDPR. High-profile cases such as these have not happened since the UK GDPR's adoption. It is argued here that the ICO should play a more proactive role in bringing RTBF-style complaints to English courts, helping claimants to assert their erasure rights – particularly in light of the mounting

[128] Ibid [81].
[129] Ibid [84]–[85].

problem of online defamation. A more stringent approach in this vein would generate much needed English case law on the matter and give both claimants and potential defendants more information about the detail and precise scope of the right. This is particularly relevant as major reform of the ICO proposed by the then Conservative government in 2024 has since been abandoned, as the Data Protection and Digital Information (DPDI) Bill which included such reform has been 'washed up' and jettisoned in the wake of the 2024 general election, which shifted the UK's governance to a Labour Party majority.[130] More cases brought of this nature would not only potentially vindicate claimants in cases where false and potentially defamatory personal information is posted online, but would also give other individuals considering asserting their rights in this way an idea of what balancing framework the English courts intend to adopt when considering a disputed RTBF claim. More jurisprudence would also add much needed clarity and detail to the rather open-ended drafting of many aspects of Article 17 UK GDPR and how the courts may solve 'hard' cases.

Through involvement with the ICO, a number of test cases could be brought on the basis of a refused erasure request, where the information in question is personal data but also false and potentially defamatory. More precedent would be generated as to whether courts would treat an erasure request differently on the basis that the information was *false*. Strasbourg and English jurisprudence suggests that, in fact, an erasure request made under Article 17 that relates to false personal information about an individual would in fact have a stronger case for erasure than truthful information. This could be covered in the *nature of the information* factor as articulated by *Hurbain*,[131] and the lack of truth in the information contested

[130] See the DPDI Bill (No 2) https://bills.parliament.uk/bills/3430 accessed 27 January 2025.

[131] *Hurbain v Belgium* (n 51) [215]–[253].

for removal would likely not have requisite 'contemporary interest' as per *Hurbain*,[132] nor perhaps the public interest value pertaining to Article 17(3)(a) UK GDPR, as it may be difficult to argue that the public have a pressing need to know untrue information. Indeed, in *Google Spain* itself, the fact the continued access to the (truthful) information gave an inaccurate impression of the claimant was a powerful argument; the CJEU found that under Articles 6, 12 and 14 of the DPD '95 that data must be adequate, relevant, as well as accurate and up to date, and not 'irrelevant' or 'excessive'.[133] Although this case was decided under the previous EU data protection law framework, it is clear that the accuracy of personal data online is still a paramount concern of the GDPR. Article 16 UK GDPR contains 'the right to rectification', which requires that data subjects 'have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her'.[134] The relevance of Article 16 may also work to bolster a RTBF request regarding untrue defamatory content online, much like a claim in misuse of private information is supported by the presence of breach of confidence elements in an action.[135] In the event that a RTBF claim is refused, then a claimant could potentially invoke Article 16's rectification right to amend false and defamatory personal data on the web. This may go some way to dispel defamatory imputations conveyed by a given post. Complete erasure of such a statement, rather than mere rectification, in many cases, may, however, be the preferred remedy due to the binary nature of such statements.[136]

---

[132] Ibid.

[133] See Article 6, Directive 95/46/EC (n 6) and *Google Spain* (n 7) [92] and [94].

[134] UK GDPR, Article 16(1).

[135] As was the case in *HRH Prince of Wales v Associated Newspapers* [2006] EWCA Civ 1776 and *McKennit v Ash* [2006] EWCA CIV 1714.

[136] On the topic of 'complete erasure', it should be noted that the CJEU have made it clear that a RTBF order will, often, only be applicable to

The final issue that must be discussed here is the future of UK data protection law more broadly stated. As the UK left the EU after Brexit, the UK GDPR now has the status of domestic law, much like the DPA 2018, and is therefore vulnerable to amendments by successive governments and legislatures. Despite only being in force since 2018, the Conservative government incumbent during this period was at pains to alter the UK GDPR in order to remedy what many party members felt were unduly strict rules on both large and small businesses in terms of GDPR compliance. This was despite the fact that, by 2024, many businesses had already installed data-protection compliance officers and developed procedures in order to act in accordance with GDPR rules. In the wake of an earlier unsuccessful attempt to amend UK data protection law under Boris Johnson,[137] the second DPDI Bill proposed by the later iteration of the Conservative government was nearing its final stages when Rishi Sunak called a general election for 4 July 2024.[138] As a result of this, the Bill ran out of time to pass through the legislative houses and was never enacted. The washed-up DPDI (No 2) Bill proposed several changes to the UK GDPR and the DPA 2018, which could be seen as 'tinkering' around the edges of data protection law in order to reduce the overall protections offered. The idea behind the Bill was that it would reduce burdens for compliance on small businesses and make it easier to conduct aspects of scientific research. The Bill's primary changes were to reduce

---

the EU – although it acknowledged the possibility of a court ordering a worldwide de-referencing order in future under the GDPR. See C-507/17 *Google LLC v CNIL* ECLI:EU:C:2019:772 [72] and Cathryn Hopkins, 'Territorial scope in recent CJEU cases: *Google v CNIL* / *Glawischnig-Piesczek v Facebook*' (*Inforrm*, 9 November 2019) https://inforrm.org/2019/11/09/territorial-scope-in-recent-cjeu-cases-google-v-cnil-glawischnig-piesczek-v-facebook-cathryn-hopkins/ accessed 23 May 2025.

[137] DPDI Bill (No 1) https://bills.parliament.uk/bills/3322 accessed 27 January 2025.

[138] DPDI Bill (No 2) (n 130).

the burden on data controllers in order to relax rules around record keeping, alter the operation of data protection officers at companies, change GDPR impact assessments, broaden the scope of scientific research and, perhaps most concerningly, change the definition of 'personal data' in order to narrow it – and therefore narrow the amount of processing to which the UK GDPR would apply.[139] Ultimately, this Bill never came into force. Since the Labour Party's success in the 2024 UK general election, a new data protection Act has been very recently been passed: the Data (Use and Access) Act 2025, under Labour's initiative.[140] The Act is considerably less far-reaching and less punitive than the earlier DPDI (No 2) Bill and does not change the UK data protection law framework anywhere near as significantly (although one could argue that the proposed DPDI (No 2) changes were not particularly momentous anyway). Legal experts have observed that the changes in the Data (Use and Access) Act are only 'incremental' and do not represent a significant change to the law as it stands.[141] The changes in the 2025 Act (then a Bill) have also altered on its passage through the legislative process.[142] The Data (Use and Access) Act chiefly adopts a 'smart data' model,[143] and proposes some comparatively more

[139] Ibid.

[140] See https://bills.parliament.uk/bills/3825 accessed 25 May 2025.

[141] Nathalie Moreno and Ben Pumphrey, 'Empowering data use, access, and sharing across the UK's digital economy' (*Kennedys Law*, 30 October 2024) https://kennedyslaw.com/en/thought-leadership/article/2024/the-new-data-use-and-access-bill-empowering-data-use-access-and-sharing-across-the-uks-digital-economy/ accessed 27 January 2025.

[142] https://bills.parliament.uk/bills/3825/publications and see Nathalie Moreno, 'The UK's Data (Use and Access) Bill: Latest amendments and legal implications' (*Kennedys Law*, 6 March 2025) https://kennedyslaw.com/en/thought-leadership/article/2025/the-uks-data-use-and-access-bill-latest-amendments-and-legal-implications/ accessed 25 May 2025.

[143] See Explanatory Notes to the Data (Use and Access) Bill [HL] 9 [2] https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf accessed 25 May 2025.

modest changes to the UK's ICO (which will still remain independent),[144] while attempting to balance innovation with strong data protection ideals. The Act will create a new lawful ground of data processing under Article 6(ea) UK GDPR, 'processing is necessary for the purposes of a recognised legitimate interest'.[145] These interests are specified in Annex 1 to the Act.[146] Most controversially, the new Act also allows the government (Secretary of State) to update this list by regulation, contingent on parliament's approval.[147] This effectively gives the government the ability to expand this list at will (subject to parliamentary intervention), therefore rendering more types of data processing lawful in so doing. If this list were to rapidly expand in future, it may in practice work to reduce the number of scenarios in which a data subject can argue for a RTBF on the basis that data has been *unlawfully processed* under Article 17(1)(d). However, this is not a significant cause for concern, as a data subject could instead argue that it is *no longer necessary* for the data to be processed under Article 17(1)(a), or instead object to its processing on the grounds of Article 17(1)(c),

[144] Research briefing, Data (Use and Access) Bill https://lordslibrary.parliament.uk/research-briefings/lln-2024-0063/ and see 'Information Commissioner's response to the Data (Use and Access) (DUA) Bill' https://ico.org.uk/about-the-ico/the-data-use-and-access-dua-bill/information-commissioner-s-response-to-the-data-use-and-access-bill/ (both accessed 27 January 2025). Also see Explanatory Notes (n 134). Also see Department for Science, Innovation and Technology, 'Guidance Data (Use and Access) Act factsheet: ICO' (27 June 2025) accessible at: https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-ico

[145] Moreno and Pumphrey (n 132) and Data (Use and Access) Act 2025, clause 70(2)(b). Also see Schedule 4, Annex 1, 'Lawfulness of processing: Recognised legitimate interests', which lists the recognized legitimate interests. The Act is available at: https://www.legislation.gov.uk/ukpga/2025/18/enacted#schedule-4 (last accessed 23/7/25).

[146] Schedule 4, Annex 1, Data (Use and Access) Act 2025 (n 136).

[147] Data (Use and Access) Act 2025, clause 70(4)(6). Also see Explanatory Notes (n 134) 73, part 546.

or perhaps withdraw consent to the information's processing according to Article 17(1)(b) UK GDPR, any of which would render a RTBF functional. Furthermore, this may not be cause for concern regardless, as any governmental expansion to this list of recognized legitimate interests would be subject to parliamentary approval and under Annex 1 of the Act, this list is narrow. It appears, then, that the RTBF will not suffer from these changes to the law. This is perhaps not surprising, as the current Labour government will wish to maintain the UK's current adequacy rating from the EU in terms of data protection law, as this is necessary for it to conduct business with the EU. The EU's current adequacy decision for the UK is set to be reviewed in December 2025.[148] There have also been political rumours circulating for quite some time that certain members of the Labour Party wish the UK to eventually rejoin the EU,[149] or at the very least negotiate a substantial trade deal with the single market, resulting in complex treaties drawn up that may include compliance with the EU's data protection standards as a necessity. In any event, if at some point a comprehensive change to the UK's data protection framework is undertaken to the detriment of the RTBF, the Strasbourg Court has acknowledged that it recognizes the RTBF of individuals in some circumstances under Article 8.[150] The UK continues to accede to the ECHR and is bound by rulings of the ECtHR – English courts have an interpretive obligation to read English law in light of the Convention.[151]

[148] ICO, 'Adequacy' https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/adequacy/ accessed 23 July 2025.

[149] William Keegan, 'Keir Starmer ruled out rejoining the EU: Now he must think again' *The Guardian* (7 July 2024) www.theguardian.com/business/article/2024/jul/07/keir-starmer-ruled-out-rejoining-the-eu-now-he-must-think-again accessed 27 January 2025.

[150] *Hurbain v Belgium* (n 51) [199] 68.

[151] See ss 2, 3 and 6(1) of the Human Rights Act 1998.

As such, it appears that the RTBF is here to stay. While any changes to the RTBF are unwelcome from the perspective of the advocates of personality rights (and this book), Article 17 UK GDPR's vulnerability to legislative change is, of course, something it shares with English defamation law.

***

Conclusion for Chapter 4

Through a process of direct comparison of defamation law and Article 17 UK GDPR, this chapter has argued that the RTBF provides, in many cases, a more effective route to redress for those defamed on the internet. It is a more simplistic remedy in terms of the action needed to be taken on the part of those defamed and is also more accessible than a lengthy action in defamation law as it is easier to understand and considerably more affordable for data subjects. While defamation law is technically complex, the substantial media attention afforded to the RTBF is something that many people are now aware of, in the wake of *Google Spain*. The legal hurdles that must be overcome to assert a RTBF are far fewer than in defamation law. In every *data-dissemination* scenario that has been considered by this book, the RTBF provides a more straightforward route to an ultimate remedy than English defamation law. Despite this, the RTBF is not a perfect solution. This chapter has made it clear that more English case law on this topic is needed to accurately ascertain some of the details of Article 17 and how it must be balanced against freedom of expression in challenging cases. It is suggested here that, in future, online defamation claims ought to be run in tandem with RTBF actions in the event that an erasure request has been refused; in this way, legal observers can see how both regimes may impact one another when considered with regard to the same issue. Finally, it is stressed that any significant statutory change to the RTBF in Article

17 UK GDPR is most unwelcome from the perspective of upholding rigorous protection of reputation and therefore personal dignity, in the wake of more defamatory information on the internet circa 2025 than ever before.