Regaining digital privacy?

Regaining Digital Privacy? The New "Right to be Forgotten" and Online Expression

Fiona Brimblecombe* & Gavin Phillipson**

This article considers how the newly-formulated "Right to be Forgotten" in Article 17 of the EU's new General Data Protection Regulation *will apply to "online expression", that is, content placed online via social and other forms of media. It starts by seeking to refute the argument that the widespread sharing of personal information online means that digital privacy no longer matters, considering in particular the key role that privacy as informational control plays in self-actualisation and how the advent of a right to erase may alter judicial understandings of informational autonomy. It goes on to consider some of the key interpretive dilemmas posed by Article 17, in particular the questions of when individuals and online intermediaries may be fixed with obligations under the Regulation and who may claim the broad "journalism exemption"; in doing so it contests the notion that the privacy obligations of social media platforms like Facebook should invariably be treated differently from those of search engines like Google. It then goes on to argue that the right to privacy enshrined in Article 8 of the* European Convention on Human Rights, *as interpreted by the Strasbourg Court, is likely to be an important factor in the interpretation of the new right, and how it is balanced with freedom of expression. Using a variety of data dissemination scenarios it considers how Strasbourg's 'reasonable expectation of privacy' test, and the factors that underlie it, might apply to the resolution of different kinds of erasure claims under Article 17. In doing so it analyses the applicability of a number of relevant factors drawn from the Strasbourg case law, including the content of the personal data in question, its form, whether the data subject is a "public figure", implied "waiver" of privacy rights, how the data was collected and disseminated and whether it relates to something that occurred in a physically public location.*

---

* Tutor in Law and Doctoral Candidate, Durham Law School, Durham University.

** Professor of Law, Durham Law School, Durham University.

The authors would like to thank David Erdos, Kirsty Hughes and Tom Bennett for comments on all or part of an earlier draft and David Erdos for numerous helpful discussions: the usual disclaimer applies.

I. Introduction

No-one living in a European Union country could fail to have noticed that on 25th May 2018, a new data protection regime came into force across the EU — the *General Data Protection Regulation*.[1] Work on the final stages of this article was punctuated by the constant arrival of "*GDPR* emails" from various organisations, imploring the authors to "stay in touch" by consenting to the continuing use of their contact details. As the emails piled up in inboxes, *GDPR* jokes proliferated on Twitter.[2] But beyond the mundane requirements of ensuring some control for the storing of personal data like email addresses, the *GDPR* introduced something both far more controversial but also shrouded in considerable mystery: an explicit "right to be forgotten" ("RTBF").[3] As is well known, a limited right along these lines derives from a famous case decided by the Court of Justice of the European Union ("CJEU"): *Google Spain SL v Agencia Española de protección de Datos,* which interpreted the right to erasure under the previous *Data Protection Directive 1995* so as to give individuals rights in relation to search indexing.[4] This has given rise to (at the last count) 680,000 requests for delisting, which have led to over 1.8 million URLs being removed from search results, amid

1. EC, *Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1 [*GDPR*]. The *GDPR* replaced the previous Data Protection Directive 95/46 EC [*1995 Directive*].
2. Martin Belam, "Businesses Resort To Desperate Emailing as GDPR Deadline Looms" *The Guardian* (24 May 2018), online: The Guardian <https://www.theguardian.com/technology/2018/may/24/businesses-resort-to-desperate-emailing-as-gdpr-deadline-looms>
3. *GDPR, supra* note 1, art 17. This goes considerably further than the right to erasure in Article 12(b) of the *Directive*, *supra* note 1.
4. *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (13 May 2014), C-131/12, ECLI:EU:C:2014:317 (CJEU) [*Google Spain*]. The right to erasure appeared in the previous *1995 Directive*, *supra* note 1, art 12(b); the judgment also referenced the right to object in Article 14.

considerable controversy.[5] However this right was limited — at least in the original judgment — to requesting Google and other search engines to de-list certain search results: *Google Spain* did not itself cover the right to request the deletion of actual content.[6] Hence while that decision was controversial world-wide,[7] the *GDPR*, in introducing a more detailed,

5. Daphne Keller, "The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation" *Social Sciences Research Network* (22 March 2017), online: SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914684> at 25 [Keller, "Right Tools"]. The searches referred to are those made under an individual's name.
6. See Keller, "Right Tools", *supra* note 5 at 34–35 citing Article 29 Data Protection Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales C-131/12"*, (2014) 14/EN (WP 225) at 2, online: <http://www.dataprotection.ro/servlet/ViewDocument?id=1080> [Article 29 Google Spain Guidelines] (Keller has pointed out that "data protection regulators have said that Google de-listings do not significantly threaten [free speech] rights, precisely because information is still available on the webpage"). However, as David Erdos has noted, there have been several judgments at the domestic level applying *Google Spain* that *have* resulted in deletion of substantive content: for examples see David Erdos, "Delimiting the Ambit of Responsibility of Intermediary Publishers for Third Party Rights in European Data Protection: Towards a Synthetic Interpretation of the EU *acquis*" (2018) International Journal of Law and Information Technology 1–37 [Erdos, Intermediary Publishers].
7. See e.g. Eduardo Ustaran, "The Wider Effect of the 'Right to Be Forgotten' Case" (2014)14:8 Privacy & Data Protection 8; Paul Bernal, "The Right to Be Forgotten in the Post-Snowden Era" (2014) 5:1 Privacy in Germany (10 August 2014), online: PinG <www.pingdigital.de/ce/the-right-to-be-forgotten-in-the-post-snowden-era/detail.html>; Daniel Solove, "What Google Must Forget: The EU Ruling on the Right to be Forgotten", *LinkedIn* (13 May 2014), online: LinkedIn <https://www.linkedin.com/pulse/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten>.

comprehensive and explicit RTBF, will be more contentious still.[8] It should be of interest to Canadians, for two reasons. First, the *GDPR* has extra-territorial effect:[9] it will apply to entities based outside the EU that provide services to EU citizens involving the processing of their personal data. As is well known, *Google Spain* applied EU data protection law to Google, on the basis that it had a subsidiary base within the EU. But second, a Canadian version of RTBF is in the offing: the Office of the Privacy Commissioner of Canada recently concluded that such a right[10] already exists in Canadian law.[11] Canadian regulators and courts applying this right may well draw inspiration from European case law and regulatory practice arising under Article 17.

But what does the new provision actually mean, how will it work and how will it be reconciled with freedom of expression? Answers to these questions are far from easy, in part because scholars are only just starting to grapple with the new regime. As leading commentator Daphne Keller puts it, while "oceans of scholarly ink have been spilled discussing the

---

8. For reaction so far see e.g. Meg 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) 64:88 Stanford Law Review Online; Diane Zimmerman, "The 'New' Privacy and the 'Old': Is Applying the Tort Law of Privacy Like Putting High Button Shoes on the Internet?" (2012) 17:2 Communications Law and Policy 107; Paul Schwartz, "The EU-US Privacy Collision: A Turn to Institutions and Procedures" (2013) 126:7 Harvard Law Review 1966.
9. *GDPR*, *supra* note 1, recital 3, art 3(1) and 2(1)(a) (it applies to "the processing of personal data of data subjects who are in the [EU] by a controller or processor not established in the Union, where the processing activities are related to … the offering of … services … to such data subjects in the [EU]" at art 3(2)(a).
10. That is a right both to require search engines to 'de-index' certain results *and* to require individual websites to take data down.
11. See e.g. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5; and Office of the Privacy Commissioner of Canada, "Draft OPC Position on Online Reputation" (26 January 2018) online: OPC <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801>.

Google Spain case … the same cannot be said of the … *GDPR*".[12] But this is also because major questions generated by the new regime remain beset by uncertainty. As Keller puts it: "[e]ven Data Protection experts can't say for sure how the *GDPR* answers hugely consequential questions, like whether hosting platforms [such as Twitter, Facebook, YouTube and Tumblr] must carry out RTBF removals",[13] partly because of the sometimes "opaque" drafting of the *GDPR*.[14] There is also ambiguity around how far individuals using social media may themselves become fixed with obligations under the *GDPR*.[15]

These questions are important because the record of de-listing requests made under *Google Spain* gives us good reason to believe that social media companies will be a key target for Article 17 requests: George Brock found that "[t]he eight sites for which Google receives the most requests are either social media or profiling sites" and of these, requests to delink to Facebook posts have been the single largest category, with "some 130,000 Facebook links … removed from view" by May 2016.[16] Hence the question of whether individuals and social media platforms should be treated as data controllers will very quickly assume great practical importance. Both groups, if exposed to potential data protection obligations, will also want to know whether they can claim the benefit of the broad, "journalistic" exemption.[17] Ordinary people will also want to know if they can at least claim their own freedom of expression as a defence, even if they cannot claim to be acting for journalistic purposes. These major uncertainties have not comforted

12. Keller, "Right Tools", *supra* note 5 at 26.
13. *Ibid* at 30.
14. *Ibid* at 31.
15. See below, Part III.C.1.
16. George Brock, *The Right to be Forgotten: Privacy and the Media in the Digital Age* (London: IB Tauris, 2016) at 51.
17. There are four "special purposes" under which national law may grant exemptions from *GDPR* obligations under Article 85(2); the others being "academic", "literary" and "artistic" purposes. Either or both of the "academic" and "journalistic" exemptions may be relevant to academics blogging and using social media to promote and discuss their areas of research. See further below at 24, and Part III.C.3.

those expressing strong concern about the possible impact of all this on online freedom of expression, especially what some commentators have analysed as structural and procedural features that will push online intermediaries like Google and Facebook in the direction of acceding to RTBF requests even when unsound.[18] It is possible that national courts and legislatures, under pressure from media and the web giants, may seek to ameliorate the likely effect of the *GDPR* on their operations. Some national courts have at times been ready to cut down sharply the scope of key data protection definitions — such as "personal data" — in order to limit the impact of EU data protection rules on national law.[19]

There is clear guidance from the CJEU that EU data protection law must be interpreted and applied in a way that respects the "fundamental rights of the [EU] legal order"[20] which now include the basic rights to privacy, data protection and freedom of expression in the European Union Charter on Fundamental Rights.[21] Moreover, crucially, for the purposes of this article, the Court has said that guarantees in the Charter that are cognate to those in the European Convention on Human Rights ("ECHR") must be interpreted so as to give them "the same meaning and scope"[22] as the ECHR rights — in this case the more long-standing

18. See e.g. *infra* note 157.
19. For example, the UK Court of Appeal interpreted the notoriously broad concept of "personal data" narrowly by finding that whether an individual's data constitutes personal data depends inter alia on whether it is "information that affects his privacy, whether in his personal or family life, business or professional capacity" see *Durant v Financial Services Authority*, [2003] EWCA Civ 1746 at para 28.
20. *Lindqvist v Aklagarkammaren I Jonkoping*, C-101/01, [2003] ECR at I-12992 [*Lindqvist*].
21. EC, *Charter of Fundamental Rights of the European Union*, [2000] OJ, C 364/01 [EU Charter] (Articles 7, 8, and 10 protecting, respectively privacy, data protection and freedom of expression).
22. *Philip Morris Brands SARL v Secretary of State for Health*, C-547/14, [2016] ECLI:EU:C:2016:325 (CJEU); see also *Bernard Connolly v Commission of the European Communities*, C-274/99, [2001] ECR I-1638 at paras 37–42; see also Article 52(3) of the EU Charter, below at 40.

ECHR rights to privacy and freedom of expression.[23] Hence an important guide to the meaning of Article 17 is likely to be the jurisprudence of the European Court of Human Rights in Strasbourg ("the Strasbourg Court"). This is particularly so given that, as Keller observes, "[c]ases balancing rights to expression versus privacy … exist — but those rarely involve Data Protection, or set out rules for [online service providers], as opposed to ordinary publishers or speakers."[24] The one decision Keller cites here is the leading Strasbourg decision of *Von Hannover v Germany*[25] — which involved a traditional privacy claim against the print media. Hence a key enterprise of this paper: to try to figure out how the newly-formulated right to be forgotten will apply to online expression by drawing out relevant principles from the privacy case-law of the Strasbourg Court and applying them to this new situation. We should stress that our endeavour is limited to how the primary right should be construed, whom it will bind and who may claim exemptions from it by reference to the countervailing right of freedom of expression or the journalistic exemption. We do not go on to consider the substantive *content* of the freedom of expression side of the balance:[26] that would

23. *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 UNTS 221 arts 8–10 (entered into force 3 September 1953) [*ECHR*]. Article 8 provides: "(1) Everyone has the right to respect for his private and family life, his home and his correspondence". The second paragraph provides for restrictions only as they are provided for by law, in pursuit of a legitimate aim, such as the prevention of disorder or crime, or "protection of the rights and freedoms of others" and are necessary to protect these other rights or interests, which imports a proportionality test. Article 10 provides in para 1 that "Everyone has the right to freedom of expression"; the second paragraph provides a similar set of exceptions to para 2 of Article 8.
24. Keller, "Right Tools", *supra* note 5 at n 186.
25. No 59320/00, [2004] VI ECHR 41 [*Von Hannover*].
26. On balancing speech and privacy rights under the ECHR see, generally, e.g. Helen Fenwick & Gavin Phillipson, *Media Freedom Under the UK Human Rights Act* (Oxford: Oxford University Press, 2006) ch 1–2, 15; Eric Barendt, "Balancing Freedom of Expression and Privacy: The Jurisprudence of the Strasbourg Court" (2009) 1:1 Journal of Media Law 49.

require a separate paper.

This article is structured as follows. Part II will first sketch the challenges our contemporary online environment poses to traditional notions of privacy and explain how the RTBF offers the potential for greater privacy protection; in doing so it will answer some common objections to the notion of seeking to protect the privacy of users who themselves frequently disclose aspects of their own private life online. Part III will then set out the basic right under Article 17 and place it within the framework of the *GDPR*; it will consider some key interpretive questions that arise, including the potential legal responsibilities as "data controllers" of individuals and social media platforms under the *GDPR* and whether they may invoke the defence of freedom of expression and/or "journalistic purposes" when doing so. Part IV will introduce Strasbourg's "reasonable expectation of privacy" test and the multiple different ways it could be applied to the right to be forgotten, depending on the circumstances in which the right is invoked. Part V will then move on to consider the individual factors the Strasbourg Court employs when assessing whether a reasonable expectation of privacy exists and its strength — a crucial factor when it comes to balancing privacy claims against competing free expression interests. The following factors will be discussed: (a) the content of the data; (b) its form; (c) whether the data subject is a public figure; (d) implied "waiver" of privacy rights; (e) how the data was collected and disseminated; (f) whether the data relates to something that occurred in a physically public location.

II. Social Media and Self-Disclosure: The Abandonment of Privacy Online?

A. Why the Need for a Right to be Forgotten?

The right to erasure was formulated with the clear view of enhancing data privacy rights for EU citizens.[27] It is thus a considered response to technological advances that have resulted in "personal information being posted online at a staggering rate",[28] driven by the increasing prominence of social networking sites,[29] a digitised media,[30] cloud computing[31] and the widespread usage of websites in relation to professional life,[32] dating,[33] and sex.[34] A recent article noted that everyday 1.18 billion people will log into their Facebook accounts, often sharing both their own and other's personal data, 3,500 million tweets will be sent, 95 million photos and videos will be posted on Instagram and Youtube content creators will upload 72 hours of new video every minute.[35] A book published in 2014 recorded that Google processes, worldwide, over 3.5 billion searches a day. It adds, "the company had been in business more than a decade before it admitted that it had stored a record of every search ever

27. Viviane Reding, "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age" *European Commission Press Release Database* (22 January 2012), online: European Commission <http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm>.
28. Daniel J Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press, 2007) at 19.
29. 2.46 billion people worldwide now use social networking sites: see e.g. *Statista*, online: Statista <https://www.statista.com/topics/1164/social-networks/>.
30. See e.g. *BBC News*, online: BBC <www.bbc.co.uk/news>.
31. See e.g. *Apple's iCloud*, online: Apple <www.apple.com/uk/icloud/>.
32. See e.g. *LinkedIn*, online: LinkedIn <https://gb.linkedin.com/>.
33. See e.g. *Eharmony*, online: Eharmony <www.eharmony.co.uk/home/rh-seo/>; *Match*, online: Match <https://uk.match.com/>.
34. See e.g. *Tinder*, online: Tinder <https://www.gotinder.com/>.
35. Max Mills "Sharing Privately: the Effect Publication on Social Media Has on Expectations of Privacy" (2016) 9:1 Journal of Media Law 45.

requested".[36] What Solove calls "generation Google"[37] became familiar from an increasingly young age[38] with internet-enabled smartphones and tablets that can take, store and upload photographs in seconds, allowing for highly impulsive sharing. Meanwhile the popularity of blogging and vlogging, including by minors, continues to grow, with one study finding that many are more akin to "personal diaries" (37%) rather than being devoted to topics like politics (11%). Solove comments:

> As people chronicle the minutia of their daily lives from childhood onwards in blog entries, online conversations, photographs, and videos, they are forever altering their futures – and those of their friends, relatives, and others.[39]

Mayer-Schönberger's seminal work, *Delete*, drew attention to the risks of a "loss of forgetting" in the digital age, with the huge quantity of personal data now "remembered" online, due to the "perfect recall" of the internet, threatening to reduce the personal autonomy of individuals and their ability to "move on" in their lives.[40] As Solove puts it, people want the option of "starting over, of reinventing themselves" but may nowadays be hampered in doing so by their "digital baggage".[41] In this regard search engines play a crucial role, rendering information on incidents that happened years ago instantly retrievable world-wide. One author gives the example of a student posting on a blog that she spotted her teacher in a gay bar; when that kind of gossip circulated in hard copy

36. Brock, *supra* note 16 at 20.
37. Daniel Solove, "Speech, Privacy, and Reputation on the Internet" in Saul Levmore & Martha Nussbaum, eds, *The Offensive Internet: Speech, Privacy, and Reputation* (Cambridge, Mass: Harvard University Press, 2010) 17 [Solove, "Speech, Privacy"].
38. See e.g. Ofcom, "Children and Parents: Media Use and Attitudes Report" (October 2014), online: Ofcom <stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-use-attitudes-14/Childrens_2014_Report.pdf> (stating that almost 8 in 10 children aged 12–15 own a mobile phone and there has been an increase since 2013 in those children using such phones to go online).
39. Daniel Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press: 2007) at 24.
40. Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press: 2009).
41. Solove, "Speech, Privacy", *supra* note 37 at 18.

student gossip sheets, it would have been buried in obscurity within a few months. Nowadays, "a person thinking of hiring the teacher twenty years later" can find that information "with just a few keystrokes".[42]

B. Theoretical Dimensions

We have thus far suggested that this explosion of personal data online, and the harm it can do, shows why we need a right to delete. However we must at this point consider a commonly advanced objection: that, not only has the internet rendered privacy laws more difficult to enforce but that the behaviour of people online shows that people today — particularly, it is said, young people — proves that they value self-expression, or "transparency *over* informational privacy".[43] It is certainly a common trope to bemoan the prevalence of "young people who behave as if privacy doesn't exist"[44] or they "don't care" about it.[45] When the Pew Foundation canvassed the views of experts, one wrote "[w]e have seen the emergence of publicity as the default modality"[46] while the Foundation summed up their collective view as being that "privacy [is] no longer a 'condition' of American life".[47] In order to respond to this argument it is

42. Geoffrey R Stone, "Privacy, the First Amendment, and the Internet" in Saul Levmore & Martha Nussbaum, eds, *The Offensive Internet: Speech, Privacy, and Reputation* (Cambridge, Mass: Harvard University Press, 2010) 192.
43. *Ibid* at 193 (emphasis added).
44. Emily Nussbaum, "Say Everything" *New York* (12 February 2007), online: New York <nymag.com/news/features/27341/>.
45. See e.g. Irina Raicu, "Young adults take more security measures for their online privacy than their elders" *recode* (2 November 2016), online: recode <https://www.recode.net/2016/11/2/13390458/young-millennials-oversharing-security-digital-online-privacy>; see also Lee Rainie, "The state of privacy in post-Snowden America" *Pew Research Center* (21 September 2016), online: Pew Research Center <www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/>.
46. Lee Rainie & Janne Anderson "The Future of Privacy" *Pew Research Center* (8 December 2014) quoting Stowe Boyd, online: Pew Research Center <www.pewinternet.org/2014/12/18/future-of-privacy>.
47. *Ibid*.

necessary to recall some basics from the theoretical literature on privacy.[48] We make no attempt to add substantively to that already copious literature: our aim is simply to highlight the relevance of a key distinction that is in danger of being forgotten in this discussion. In summary our argument is that views like the above may tempt us to overlook a fairly fundamental distinction: between privacy as a state-of-being, and privacy as a *claim:* a moral claim, that can also be a legal one.

What is the essence of this distinction? The starting point is that privacy as a state-of-being is *descriptive*; privacy as a claim is *normative*. As a description of privacy, we consider that one of the most compelling comes from the scholarship of Ruth Gavison[49] and Nicole Moreham:[50] that privacy is a state of "desired in-access to others".[51] "Access" to a person can obviously occur on a number of different levels: through touch, through sight (a peeping Tom), through hearing (by someone eavesdropping on a private conversation), through intrusion into our physical space (someone coming uninvited into your garden or home), or through a person accessing personal information about us (by reading our emails or other online private content). The argument in short is that our privacy depends upon the extent to which others can see or access us. This is why — to give simple examples — we have locked doors for toilets, and why we do not, by and large, undress in public: locked doors and clothes alike put some barriers in the way of the visual access others

48. For a major recent work on privacy in a networked world see Julie E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven: Yale University Press, 2012).
49. Ruth Gavison, "Privacy and the Limits of the Law" (1980) 89:3 Yale Law Journal 421.
50. Nicole Moreham, "Privacy in the Common Law: A Doctrinal and Theoretical Analysis" (2005) 121:4 Law Quarterly Review 628. For an account along broadly similar lines, see also RB Parker "A Definition of Privacy" (1974) 27:2 Rutgers Law Review 275.
51. The "desired" element of course is to distinguish enjoying privacy from being marooned on a desert island, or in solitary confinement desperate for any human contact — it would be odd in such situations to describe someone as being in a state of perfect privacy: see e.g. Moreham, *ibid* at 636, *et seq.*

have to us.[52] We may also seek to bar access not to our writings but our *identities*, as where people blog anonymously online,[53] a classic example of the key online phenomena Mills calls "sharing privately". [54] A well-known key effect of the internet is that the unwanted access to us that one or two people might obtain in the physical world (through prying or eavesdropping) can be instantaneously granted to millions of others — when images or recordings of a person are posted online. The online world therefore poses the "insidious threat that information shared has the capacity to be disseminated further, throughout social networking sites and even reaching mass media".[55] The literature is full of examples: an extreme one concerns a girl who, back in 2000, made intimate videos for her boyfriend of her stripping and masturbating; they were placed online by persons unknown and became some of the first "viral videos", turning her into an accidental online porn star, with her own Wikipedia entry.[56]A more mundane example is the *Daily Mail* publishing Facebook photos of drunken "girls' nights out" to a mass audience under the headline: "The ladettes who glorify their shameful antics on Facebook".[57]

The above discussion shows how a key contemporary concern is that greater access to the *informational* dimension of our private sphere will

52. Kirsty Hughes analyses such behaviour as the placing of "privacy barriers" in the way of others; invasions of privacy occur when such barriers are breached: see Kirsty Hughes, "A Behavioural Understanding of Privacy and its Implications for Privacy Law" (2012) 75:5 The Modern Law Review 806.
53. For a decision that failed to recognise the vital privacy-based interest in anonymous blogging see *The Author of a Blog v Times Newspapers Ltd*, [2009] EWHC 1358 (QB).
54. Mills, *supra* note 35 at 46.
55. *Ibid.*
56. Nussbaum, *supra* note 44.
57. Andrew Levy, "The ladettes who glorify their shameful drunken antics on Facebook" *Mail Online* (5 November 2007), online: Mail Online <www.dailymail.co.uk/news/article-491668/The-ladettes-glorify-shamefuldrunken-antics-Facebook.html>. Multiple extreme examples of such persecutory and harassing speech are discussed by Danielle Citron in *Hate Crimes in Cyberspace* (Cambridge, Mass: Harvard University Press, 2016).

diminish our privacy as a state-of-being. In response to this concern, people put forward a *claim* to privacy. Many have argued that this is best captured as being a claim for *control* over our personal information:[58] that it is up to the individual how much of their private sphere — including information — they choose to share with others. Certainly, the notion of informational autonomy is the easiest to apply to the regulation of online privacy: both the EU and Strasbourg Courts have recognised it as a key value underlying both data protection and Article 8 ECHR. Recital 7 of the *GDPR* states that, "[n]atural persons should have control of their own personal data";[59] the Strasbourg Court recently observed that Article 8 ECHR, the right to privacy, "provides for the right to a form of 'informational self-determination'".[60] It is when that control is *taken from* individuals — revealing images of them are posted online, their phone is

58. Alan Westin, *Privacy and Freedom* (London: The Bodley Head Ltd, 1970) (Westin has argued that "privacy is the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others" at 7); see also Alan Westin, "The Origins of Modern Claims to Privacy" in Ferdinand Schoeman, ed, *Philosophical Dimensions of Privacy* (Cambridge: Cambridge University Press, 1984) 56; Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Palo Alto: Stanford University Press 2009); Paul Gewirtz, "Privacy and Speech" (2001) 2001:1 The Supreme Court Review 139; Charles Fried, "Privacy" (1968) 77:3 Yale Law Journal 475, esp 482–43; Solove, "Speech, Privacy", *supra* note 37 at 21 (Solove uses practical examples to show the keen desire for control over accessibility: over 700,000 people complained to Facebook when it introduced News Feed, alerting people's friends when their profile was changed or updated even though many of the complainants had publicly available profiles).
59. *GDPR*, *supra* note 1, recital 7.
60. *Satakunnan Markkinaporssi Oy and Satamedia Oy v Finland,* No 931/13 (27 January 2017) [*Satakunnan*].

hacked,[61] their email and telephone records accessed by government,[62] or photos taken of them coming out of a drug treatment facility[63] — that we can say their privacy has been "invaded".

From this one initial point emerges: while people can choose to give others greater or lesser "access" to their personal sphere, they cannot — as tabloid editors are prone to say as justification for publishing intrusive stories about publicity-seeking celebrities — "invade their own privacy". It is only when someone's control over their private sphere is *taken from* them that their privacy is *invaded*. That is, at least, the "old media" perspective. Applying this insight to *social* media is slightly more complex — but of far more universal application: it applies to all of us who post some kind of personal information online. It is true that our behaviour in doing this may show a very different attitude to privacy from that of our parents' or grandparents' generation;[64] this leads to the argument, noted above, that such behaviour shows that people nowadays care more about transparency and expression than privacy.

To address this argument, we must consider the complex relationship between the needs of self-expression and sociability and of privacy, used in a descriptive sense. We draw close to people by giving them access to us — to our thoughts, our vulnerabilities, homes, or personal space; in the case of sex and love, to the most intimate parts and aspects of ourselves. What we do appear to have seen in the last few decades

---

61. See e.g. UK, Leveson Inquiry, *An Inquiry into the Culture, Practices and Ethics of the Press* by The Right Honourable Lord Justice Leveson: Report, (London: Her Majesty's Stationery Office, 2012) (concerns about press practices such as blagging and hacking led to the Leveson Inquiry as well as numerous civil cases against newspapers, most of which were settled).
62. In the UK the revelation of the bulk collection of communications data by the state led eventually to the decision in *Secretary of State for the Home Department v Watson MP*, [2018] EWCA Civ 70 finding the then regulations unlawful: they have been replaced with permanent, sweeping statutory powers under the *Investigatory Powers Act* 2016.
63. As in the leading UK decision of *Campbell v MGN Ltd*, [2004] UKHL 22 [*Campbell*].
64. See Nussbaum, *supra* note 44, for a range of extreme examples of self-disclosure.

is a shift in the relative value people give to privacy as state-of-being, compared to the value they attach to self-expression online as a means of connecting with people. Some people undoubtedly use social media to do this in a rather undifferentiated way: for example, seeking approval for their physical appearance from an online mass audience, instead of a few close friends.[65]

However — and this is our key point — none of this means that people do not still value the *right* to privacy: they still want to decide *what* and *how much* they share — even if some use that choice to share far more with far more people than their parents would have dreamt of doing. A recent research project by the Pew Foundation found that "74% [of Americans] say it is 'very important' to them that they be in control of who can get information about them".[66] We see this in increasing concern and awareness about things like the "privacy settings" on Facebook,[67] how far people really give consent to the volume of information they are sharing with Google (which knows all the searches you've made) or Amazon or Kindle (which knows which of their books you have read); or Gmail, which has all the emails you've sent.[68] Different people will always draw this boundary differently and that in itself is no cause of concern: in the "offline" world we will all know some people who are quite reserved — sharing aspects of their private life with only a few

65. An extreme example is the phenomena of "ratings communities", like "nonuglies", where people post photos of themselves to be judged and rated by strangers. See Nussbaum, *ibid*, for these and other examples and e.g. <https://www.livejournal.com/blogs/en/nonuglies>.

66. Lee Rainie, "The State of Privacy in Post-Snowden America" *Pew Research Center* (21 September 2016), online: Pew Research Center <www.pewinternet.org/2014/12/18/future-of-privacy/>. While such control can be argued to have good *consequences* it can also be seen in deontological terms as an aspect of human dignity; for a classic account see Edward J Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39:6 New York University Law Review 962.

67. See e.g. Solove, "Speech, Privacy", *supra* note 37 at 21, discussed *supra* note 58.

68. For a recent major work on this subject see Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford: Oxford University Press, 2015).

trusted friends — and others, who will drunkenly share intimate details of their love-lives with near-strangers. Privacy boundaries vary greatly between different societies; even *within* given societies, they will vary greatly between individuals and be drawn and re-drawn repeatedly. All that we can generalise is that it is a pervasive feature of human relations that, as Solove puts it, most people "reveal information to certain groups while keeping it from others".[69]

A key point therefore is that, while the boundaries between self-expression and privacy will always vary between people and shift as society changes, none of that means that individuals should be deemed to have given up the core *right to privacy* — the claim that is, to exercise some control over access to their inner sphere, and particularly, their personal information. To argue that someone who chooses to share a great deal of their private information with others online, for that reason becomes fair game to have their private information taken from them without their consent, is a little like arguing that a woman who chooses to share her body intimately with many others by having numerous transitory sexual partners should lose her right to choose with whom she has sex.[70]

That then is the core response to the argument that the proliferation of intimate personal information placed voluntarily online provides a reason against allowing legal claims for invasion of privacy when such information is used *in*voluntarily. But there is a further point, also a well-known argument, but we think particularly apt in the case of social media. While the press and much scholarship, particularly from US First Amendment scholars, tends to portray privacy and self-expression as invariably in tension,[71] they also go hand-in-hand. Privacy, as Fried has argued, is essential to the intimate communication vital to fostering

---

69. Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004) at 42–4.
70. We do not of course suggest that the scale of violation in the two cases is comparable, merely the way in which, in both cases, past behaviour is used to justify dispensing with consent.
71. See e.g. Diane Zimmerman, "Requiem for a Heavyweight: a Farewell to Warren and Brandeis's Privacy Tort" (1983) 68:3 Cornell Law Review 291; Richards, *supra* note 68.

close relationships: most of us will only share information that might be deeply painful or simply embarrassing with a friend or partner *if* we are reasonably sure that they will keep it to themselves; hence an assurance of privacy can actually ensure greater self-expression between people and thus greater intimacy.[72] Online, this often translates into the need for anonymity, in which guise it facilitates individual self-exploration in the form of reading, watching and listening to a wide range of media often shared on social media, as well as blogging on intimate subjects. For example a deeply-conservative Evangelical Christian, seeking to explore his possible homosexuality is likely to do so online only if fairly sure that he can keep his explorations to himself. Exactly the same argument applies to the personal blogs that abound on the internet. This is what De Cew calls "expressive" privacy — "a realm for expressing one's self-identity or personhood".[73] This dimension of privacy then is crucial to individual self-development, exploration and self-actualisation: all values commonly argued to underlie free speech.[74]

Thus as Mayer-Schönberger has pointed out, the purpose of the right to delete is to combat the loss of control an individual faces when their information and history — in a very real sense their personal identity — becomes, in Bernal's words, "an indelible part of a mass of information usable and controllable by others".[75] However, the notion of a right to delete should also change the way the concept of informational autonomy is applied in privacy cases. Under the "old-media" paradigm, previous self-publicity could be treated as a "waiver"

---

72. See Charles Fried, "Privacy" (1968) 77:3 The Yale Law Journal 475; for a similar argument, see Jeffrey Reiman, "Privacy, Intimacy, and Personhood" (1976) 6:1 Philosophy & Public Affairs 26.
73. Judith W DeCew, "The Scope of Privacy in Law and Ethics" (1986) 5:2 Law and Philosophy 145, at 166, also see 167–170.
74. For classic accounts see Frederick Schauer, *Free Speech: A Philosophical Enquiry* (Cambridge: Cambridge University Press, 1982); Kent Greenawalt, "Free Speech Justifications" (1989) 89:1 Columbia Law Review 119; Eric Barendt, *Freedom of Speech*, 2d ed (Oxford: Oxford University Press, 2005) ch 1.
75. Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge: Cambridge University Press, 2014) at 206.

of privacy rights,[76] under which an individual's prior decision to speak to the press about an aspect of their private life could lead to courts finding they had lost their previous reasonable expectation of privacy. Such loss could apply to the whole of their personal life (under the extreme notion of a "blanket waiver") or just the same broad area (e.g. sex-life) that they had previously publicised.[77] This approach comes close to treating informational autonomy as a one-off event: the individual gets to choose *once* whether to share certain personal information with a large audience. Then precisely *because* they made that choice, they are deemed to have *lost* the right to exercise it later. That approach always contradicted the premise of the informational autonomy model but it was one that media organisations successfully persuaded at least some courts to adopt. But the right to delete inescapably insists on a different approach, under which the right to control over personal information is not a one-off, but something that one can exercise *continuously*; thus, information one had previously publicised could still be the subject of a deletion claim. The notion that control is "waived" by self-publicity is necessarily rejected as incompatible with any meaningful right to delete. Thus, RTBF requires a shift in our understanding of informational self-determination, from being (potentially) a one-off event, whereby control is exercised, but simultaneously lost for the future, to being instead a *continuing* entitlement.

In short, privacy in a socially-networked world is about degrees of control over information about ourselves and determining the degree and nature of social interaction with others. If we lose that control we become

76. See e.g. *infra*, text following note 256; for a critique of the concept of "waiver" see Gavin Phillipson, "Press Freedom, the Public Interest and Privacy" in Andrew Kenyon, ed, *Comparative Defamation and Privacy Law* (Cambridge: Cambridge University Press 2016) at 150. In the US context, celebrities may be seen to have waived their right to privacy; thus giving media bodies a claim of "implied consent" to privacy claims brought against them: see e.g. John P Elwood, "Outing, Privacy and the First Amendment" (1992) 102:3 Yale Law Journal 747.

77. Known as the "zonal approach": for examples, see e.g. *Douglas v Hello!*, [2003] 3 All ER 996 (CA) at para 226 (sex life) and *A v B*, [2005] EWHC 1651 (QB) (drug use).

"powerless objects available for capture", a mere "bundle of details, distortedly known, presumptuously categorised, instantly retrievable, and transferable to numerous unspecified parties at any time"'.[78] The right to delete is part of the attempt to re-empower us online; all of us. Because, unlike classic tort privacy actions, which are typically available only to the wealthy celebrities who can afford them, RTBF is a remedy that anybody can use — hundreds of thousands have already.[79]

III. The Right to be Forgotten: Key Interpretative Issues

A. The Focus of This Article

This article considers RTBF only in relation to what we might broadly term online expression: by this we include traditional media online, such as newspaper and news websites, but also social media, search engines, blogs and all the other now-familiar aspects of Web 2.0. We are not therefore concerned with relatively uncontroversial aspects of RTBF, such as requiring the deletion of ordinary commercially-valuable personal data like contact details from a company whose services we previously used, or of personal data held by employers or public bodies, like health services and law-enforcement agencies. Nor, in relation to social media platforms will we consider what Keller terms "back-end data", that is, data that online service providers (OSPs) themselves collect "by tracking their own users' online behaviour"[80] such as clicks, "likes", etc., in order to target advertisements at them. As straightforward commercial data we do not treat this as an aspect of online expression (though it undoubtedly raises privacy concerns). Hence, when we discuss RTBF we are concerned *only* with its use in respect of data placed online by another individual or media body, whether the data subject themselves or a third party. Finally,

78. Anne SY Cheung, "Rethinking Public Privacy in the Internet Era: A Study of Virtual Persecution by the Internet Crowd" (2009) 1:2 Journal of Media Law 191 at 210. See also Beate Rossler, *The Value of Privacy*, translated by RDV Glasgow (Cambridge: Polity Press, 2005) at 106.
79. See above, at 3.
80. Keller, "Right Tools", *supra* note 5 at 4.

we are not concerned with scenarios in which an individual uploads their own personal information (such as photographs) to a social networking site like Facebook *but* retains first-hand control over it: since they are at liberty simply to delete it from the site (or even close their account completely),[81] they would not need to invoke Article 17. However, if that data has subsequently been copied or shared such that it is now beyond the individual's control, that takes us into scenarios that we do consider.

B. Article 17 *GDPR*: The Basics

Article 17 gives the right to "data subjects" (an identifiable natural person to whom information online relates);[82] it lies *against* "data controllers" — those who "alone or jointly with others, determine the purposes and means of the processing of personal data";[83] this likely includes, for example, website hosts, authors of certain web-pages and search engines.[84] "Processing" is very broadly defined and includes "collection … storage … retrieval … use … disclosure by transmission, dissemination or otherwise making available"[85]; hence it plainly encompasses the publication of personal data online, in whatever form. As discussed at various points below, the *GDPR*, in common with the earlier *Directive*, affords particular protection to what was previously known as "sensitive personal data", now referred to as "special category data" (the former term will be used as the more intuitive match). This is defined in Article 9(1) as personal data revealing:

> racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or

81. See Sophie Curtis, "How to permanently delete your Facebook account" *The Telegraph* (19 August 2015), online: The Telegraph <www.telegraph.co.uk/technology/facebook/11812145/How-to-permanently-delete-your-Facebook-account.html>.
82. *GDPR, supra* note 1, art 4.
83. *Ibid,* art 4(4).
84. *Google Spain, supra* note 4 (the CJEU found that Google was a data controller; the definition in *GDPR*, Article 4 is virtually the same as that considered in *Google Spain*).
85. *GDPR*, *supra* note 1, art 4(2).

> … a natural person's sex life or sexual orientation.[86]

While Article 9(1) appears baldly to prohibit the processing of such data, there are broadly worded exceptions; these include the "explicit consent" of the data subject,[87] where the data subject has "manifestly made the data public"[88] and where:

> processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[89]

The *GDPR* is a Regulation and, as such, automatically applicable across all EU states without the need for domestic implementation; however, its provisions specifically allow for Member States to supplement it by domestic laws,[90] especially to provide exemptions to ensure proper protection for freedom of expression and information. Article 85(1) *GDPR* requires Member States "by law" to "reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information".[91] Article 85(2) more specifically states:

> For processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression, Member States shall provide for exemptions or derogations from [key provisions of the *GDPR*] if they are necessary to reconcile the right to the protection of personal data with the freedom of

86. *Ibid*, art 9(1).
87. *Ibid*, art 9(2)(a).
88. *Ibid*, art 9(2)(e) (we are grateful to David Erdos for pointing out that the exception actually refers to data "which *are* manifestly made public" — the possible significance of this odd use of the present tense is considered further below at note 103).
89. *GDPR*, *supra* note 1, art 9(2)(g).
90. For a useful summary of these provisions see Daphne Keller, "The GDPR and National Legislation: Relevant Articles for Private Platform Adjudication of 'Right to Be Forgotten' Requests" *Inforrm* (5 May 2017), online: Inforrm <https://inforrm.org/2017/05/05/the-gdpr-and-national-legislation-relevant-articles-for-private-platform-adjudication-of-right-to-be-forgotten-requests-daphne-keller/>.
91. *GDPR*, *supra* note 1, art 85(1).

expression and information.[92]

The UK has just passed such legislation,[93] the *Data Protection Act 2018*[94], which grants sweeping exemptions from the key requirements of the *GDPR* and the remedies it grants — including Article 17 — for processing, including of sensitive personal data, done in pursuit of "the special purposes", including journalism.[95] Many EU countries, however, had not passed any such legislation by the time this article went to press; hence the concrete effect of the *GDPR* will probably take many years to become apparent and considerable variation is likely to be found amongst the Member States. Since this article concerns the *GDPR* itself, rather than law in the UK, only brief mention will be made of the *2018 Act*, for illustrative purposes.

Article 17, as material, provides:

> (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:
>
> > (b) the data subject withdraws consent on which the processing is based … [96] and where there is no other legal ground for the processing;

92. *Ibid*, art 85(2).
93. While the UK has decided to withdraw from the EU and will currently do so on 29 March 2019, it is legislating so as to retain the vast majority of currently applicable EU law in the *European Union (Withdrawal) Act 2018* (UK), c 16. While the bill specifies certain EU instruments that will *not* be retained, the *GDPR* is not one of them.
94. *The Data Protection Act 2018* (UK), c 12 [*2018 Act*].
95. See below, at 34.
96. *GDPR, supra* note 1 (the provision refers both to consent under Article 6(1) to the processing of "ordinary personal data" and "explicit consent" under Article 9(1) to the processing of "sensitive personal data").

> (c) the data subject objects to the processing pursuant to Article 21(1)[97] and there are no overriding legitimate grounds for the processing,
>
> (d) the personal data have been unlawfully processed; …
>
> (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).[98] …
>
> (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 …

It also contains a requirement for controllers to inform third parties who are processing the same data that it has been requested for deletion under Article 17(2).[99] As will be seen, the right is broadly framed, and does not appear to require any threshold of seriousness to be met in order to invoke it.[100] Given the reference to withdrawing consent, Article 17 *may* apply to information initially uploaded by the data subject themselves as well as that uploaded by a third party. As Recital 65 makes clear:

---

97. The right to object referred to is objection to processing "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child" see *GDPR*, *ibid*, art 6(1)(f).
98. This means essentially that the information was collected from a child and they or their parents consented at the time (children may only consent from the age of 13 on). "Information society services" are defined as "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service" see *GDPR*, *ibid*, art 8(1). They include online shops, streaming services and social media, see *GDPR*, *ibid*, art 4(25).
99. *GDPR*, *ibid*, art 17(2) provides: "Where the controller has made the personal data public and is obliged … to erase [it], the controller, taking account of available technology and the cost of implementation, shall take reasonable steps … 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".
100. As opposed to, for example, a defamation claim brought in English law under the *Defamation Act 2013*, (UK) c 26 (see section 1).

> [T]he right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.[101]

The ability to use the right to delete in order to leave behind embarrassing childhood images or posts is one of the more widely-accepted aspects of RTBF. It should be noted that, in the case of material that was uploaded by the data subject as an adult, withdrawal of consent grounds a claim *only* where the previous consent of the data subject was the sole lawful basis for processing the data.[102] Thus for "ordinary data", the controller could rely instead on their "legitimate interests" (unless overridden by the privacy interests of the data subject) as a lawful basis for processing. If the data is "sensitive" within the meaning of Article 9, the controller could seek to rely on a deliberate decision by the data subject to make the data public[103] in the past, such as posting it to a public website as the basis. If this condition was found to be made out, then withdrawal of consent *per se* would not appear to ground a deletion request.

Finally, and very importantly, Article 17 makes clear that, even where paragraph (1) is satisfied, the right is only *prima facie* made out: it must then be balanced against freedom of expression of either or both of the data controller and (if the two are not the same) the original poster of the

---

101. *GDPR, supra* note 1, recital 65.
102. *Ibid*, art 17(1)(b).
103. *GDPR*, *ibid*, art 9(2)(e). As noted above, *supra* note 88, the wording of the *GDPR* refers to data "which *are* manifestly made public". In the UK context, the *2018 Act*, *supra* note 94, s 86(2) states that the processing of sensitive personal data "is only lawful" if "at least one condition" from both Schedule 9 *and* Schedule 10 is fulfilled. In many cases involving online expression the *only* likely condition that could be relied on in Schedule 10 is para 5: "The information contained in the personal data *has been made public* as a result of steps deliberately taken by the data subject" [emphasis added]. Evidently the effect of the UK legislation here might be different from the *GDPR* provision. How this situation would be resolved in other member states might turn on the particular terms of their own *GDPR* legislation.

data.[104] On the face of it, it appears therefore that freedom of expression could be invoked to refuse deletion as a particular remedy, even where the data being requested for deletion is being processed unlawfully. This might arise, for example, where the data requested for deletion is "sensitive" and there is no legal basis for processing it.[105]

C. Some Key Interpretive Dilemmas

As noted above, the *GDPR* leaves a number of extremely important issues unclear. Three in particular stand out: first, will private individuals uploading information about others online be classed as data controllers and hence subject to RTBF requests? Second, will social media platforms publishing such third-party content be controllers (often referred to as the "intermediary liability" issue)? And third, who will benefit from the broad exemption for "journalism"? As these issues are canvassed in detail elsewhere;[106] only a relatively brief account is offered here.

1. Can Individuals Using Social Media be Data Controllers?

We consider first the possible liability of individuals. Many might bridle at the notion that we "process the personal data" of others; however, most of us do it all the time. A very common scenario involves an individual

104. *GDPR*, *supra* note 1, art 17(3)(a).

105. We are indebted to David Erdos for pointing this out.

106. On the intermediary liability question see Keller, "Right Tools", *supra* note 5, and Erdos, "Intermediary Publishers", *supra* note 6; on the issue of individuals as possible data controllers see 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 [Erdos, "Domestic"]: Brendan V Alsenoy, "The Evolving Role of the Individual Under EU Data Protection Law" (2015) CiTiP Working Paper 23/2015, online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2641680>; on the scope of the journalist exemption see above Erdos, "Domestic" and David Erdos, "From the Scylla of Restriction to the Charybdis of License? Exploring the Present and Future Scope of the 'Special Purposes' Freedom of Expression Shield in European Data Protection" (2015) 52:1 Common Market Law Review 119.

posting a photograph of a friend or family member, often showing the two of them together. If the post included a comment such as "Annabel had a bad dose of flu but still looked great!" then the poster has processed *sensitive* personal data about another. So, in scenarios like these, will the poster be counted, at least for some purposes, as a "data controller"? The so-called "household" exemption in the *GDPR* is the starting point. This provides that the Regulation "does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity".[107] Recital 18 explains that this means processing "with no connection to a professional or commercial activity"[108] and that such processing "*could* include … social networking and online activity undertaken within the context of such activities".[109] Research by David Erdos on the attitude of national Data Protection Authorities ("DPAs") across the EU showed wide variation in their approach to this issue; however, a common theme was that a key distinction was to be drawn between publication to a small, controlled group — likely to fall within the "household exemption" — and publication to an indefinite group, which would not. As Erdos puts it:

> The vast majority [of]… DPAs hold that once personal information relating to somebody other than the publisher themselves is disseminated to an indefinite number, the personal exemption cannot apply.[110]

It appears that this is based on the decision of the CJEU in *Lindqvist*,[111] interpreting an almost identical exempting provision in the previous 1995 *Data Protection Directive*. In that case, the Court said that the exemption was confined:

> only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.[112]

---

107. *GDPR*, *supra* note 1, recital 18.
108. *Ibid*.
109. *Ibid* [emphasis added].
110. Erdos, "Domestic" *supra* note 106 at 276.
111. *Lindqvist*, *supra* note 20.
112. *Ibid* at para 47.

This approach has been echoed by the EU's Article 29 Working Party ("Working Party")[113], which in 2013 said: "[i]f a user takes an informed decision to extend access beyond self-selected 'friends', data controller responsibilities come into force".[114] Thus under our scenario of posting a photo of Annabel, the crucial factor would be the privacy settings the poster was using: provided the photo was posted only to a closed group of "friends", the Household exemption would likely apply, meaning the *GDPR* would not. However, if it were posted to a *public* forum — as in a Facebook post made available to all, or a tweet — then the individual *would* become a data controller in respect of that item.

Erdos notes further that some DPAs took a more "stringent approach" suggesting that, in general, use of others' personal data on social networking sites should require data subject consent.[115] Conversely, one of the most permissive DPAs was the UK's Authority, which said that the personal exemption would apply:

> whenever someone uses an online forum purely in a personal capacity for their own domestic or recreational purposes; [hence it] will not consider complaints made against individuals who have posted personal data whilst acting in a

113. *Directive*, *supra* note 1, art 29 established a Working Party on the Protection of Individuals with regard to the Processing of Personal Data ("the Working Party"). In the first UK case of a *Google Spain*-style delisting that reached the courts, Warby J in the High Court said: "All parties are agreed that [Guidance by the Working Party on *Google Spain*] will be of the greatest use to me in assessing the claims" see *NT1 and NT2 v Google*, [2018] EWHC 799 (QB) at para 39 [*NT1*].

114. Article 29 Data Protection Working Party, *Opinion 5/2009 on Online Social Networking*, (2009) 01189/09/EN (WP163) at 6. A subsequent report in 2013 suggested that such a factor should not be determinative but only be "an important consideration" amongst many see Article 29 Data Protection Working Party, *Statement of the Working Party on Current Discussions Regarding the Data Protection Reform Package*, (2013) Annex 2: Proposals for Amendments Regarding Exemption for Personal or Household Activities at 9; but by 2015 the Working Party had seemingly returned to advocating only a narrow limitation see Article 29 Data Protection Working Party, *Appendix: Core Topics in View of the Trilogue*, (2015) Annex to the letters at 3.

115. Erdos, "Domestic", *supra* note 106 at 286. This group had 11 DPAs including from Norway, Germany, France, and Belgium.

> personal capacity, no matter how unfair, derogatory or distressing the posts may be.[116]

Erdos's own view suggests a more qualitative analysis whereby:

> the interpretation of the personal exemption should be widened to encompass those forms of individual publication which do not pose a serious *prima facie* risk of infringing … the core privacy, reputation and related rights which data protection is dedicated to safeguard.[117]

He suggests three situations in which such a risk would be present: (a) "clearly pejorative posts" (e.g. a student critiquing a particular teacher by name); (b) "disclosure of private details re private life (especially if sensitive)" or (c) comments that are "so frequent and focused" that they amount to harassment.[118] We argue below that in making such a qualitative assessment, guidance from the Strasbourg Court could play a useful role.

In short then, it is not possible to be sure either about the correct interpretation of the *GDPR* in this respect, *or* the practice of national DPAs with primary responsibility for enforcing it. It is likely that the major variations in approach identified by Erdos will continue for several years, at least until authoritative and detailed guidance is obtained from the CJEU or the new European Data Protection Board.[119]

2. Intermediary Liability

What then of the social media platforms themselves? Keller points out how a request by another for Twitter to erase a tweet that Keller had written:

> affects at least four key sets of rights: my rights to free expression, [the data subject's] rights to Data Protection and privacy, other Internet users' rights to

116. UK, Information Commissioner's Office, *Social networking and online forums – when does the DPA apply?* (2014), at 15 online: ICO <https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf>.
117. Erdos, "Domestic", *supra* note 106 at 276, 292.
118. *Ibid* at 292.
119. Established under *GDPR*, *supra* note 1, art 68, and tasked with, *inter alia*, providing best practice guidance regarding deletion requests see *GDPR*, *supra* note 1, art 71(1)(d).

seek and access information, and Twitter's rights as a business.[120]

It is important to note, that in EU law, the liability of such "hosts" for third party content that is (for example) in breach of copyright, is governed by the E-Commerce Directive;[121] this, broadly, shields hosts from liability in respect of such content in the absence of knowledge of its unlawfulness. However, despite some suggestions to the contrary[122] it seems tolerably clear that this regime will not apply to data protection claims[123] and that the *GDPR* will. The starting point is *GDPR* Recital 18, which, having granted the exemption for "purely personal", or "household" processing, immediately goes on: "this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities".[124] The Working Party in a recent opinion argued that *both* the social networks and the original poster would be data controllers in relation to material posted by users.[125] Erdos thinks it is clear that social media platforms like Facebook[126] *will* be data controllers; this would be consistent with the E-Commerce Directive, he contends, as the primary obligations will be ex-post obligations to remove data once their attention is drawn to it (including the right to delete). This, he

120. Keller, "Right Tools", *supra* note 5 at 18–19.
121. EC, *Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, [2008] OJ, L-178 [E-Commerce Directive].
122. Especially by Keller, "Right Tools", *supra* note 5.
123. E-Commerce Directive, *supra* note 121, recital 14, seems decisive here: "The protection of individuals with regard to the processing of personal data is solely governed by [laws including the 1995 *Directive, supra* note 1], which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive".
124. *GDPR*, *supra* note 1, recital 18.
125. Article 29 Data Protection Working Party, *Opinion 1/2010 on the Concepts of "Controller" and "Processor"*, (2010) 00264/10/EN (WP 169) online: <www.pdpjournals.com/docs/88016.pdf>.
126. Found by the Court of Appeal in Northern Ireland to be a data controller under the 1995 *Directive*, *supra* note 1 see *CG v Facebook Ireland Ltd*, [2016] NICA 54.

argues, would not fall foul of the prohibition of obligations to engage in general monitoring in the Directive.[127]

Keller seeks to avoid the conclusion that, since we know from *Google Spain* that search engines are data controllers, platforms like Facebook must be too. She points out that the finding in *Google Spain* was justified by particular reasoning: that the search engine produces a "structured overview" of "vast aspects of [the data subject's] private life … which, without the search engine, could not have been interconnected or could have been only with great difficulty".[128] Keller then argues from this that social media platforms have a *lesser* impact on an individual's privacy, while deleting actual content (instead of merely de-listing it) would have a greater effect on freedom of expression; hence this sufficiently distinguishes social media platforms from search engines.[129] However, these arguments are probably best taken as arguing for a higher burden on those seeking to delete content, rather than merely de-list: she argues that "it should be *harder* to get content removed from a hosting platform, because the balance of rights and interests is different".[130] This is right in part: *in general*, removing content as opposed to simply delisting it when searched under an individual's name will be a greater interference with freedom of expression. Moreover (but also only in general) search engines can have a particularly serious impact on privacy, for the reasons she gives. The key point, however, is that this would not necessarily *always* be the case: as argued below, the extent to which a given piece of online content compromises a person's privacy depends upon a multi-factor assessment, in which perhaps the most important factor is the nature of the information itself.

Two pairs of examples will illustrate the point. Celebrity A is seeking to have Google de-link to some mildly embarrassing gossip-journalism reports about her excessive drinking one evening several years ago. Celebrity B in contrast wants Facebook to remove a post by an estranged friend revealing details of B's past struggles with a serious eating disorder.

127. Erdos, "Intermediary Publishers", *supra* note 6.
128. *Google Spain*, *supra* note 4 at para 80.
129. Keller, "Right Tools", *supra* note 5 at 36.
130. *Ibid* at 43 [emphasis in original].

Here it seems clear that Celebrity B has a far stronger and more serious privacy claim, not least because her case deals with one of the classes of sensitive data.[131] That then demonstrates that claims against hosts *can* raise much more weighty privacy interests than those against search engines.

The second pair of examples considers the freedom of expression side of the balance. Politician C is seeking, shortly before an election, to have Google immediately remove from search returns (pending investigation) links to stories detailing truthful allegations of misconduct during a previous election.[132] Celebrity D is seeking to have topless photographs hacked from her iCloud account removed from a Tumblr site. In this case, although D is seeking to have actual content removed and C merely to have it de-listed, it is clear beyond argument that Google would have a far stronger claim under the freedom of expression derogation than Tumblr: political expression is invariably treated by Strasbourg as the "highest value" speech.[133]

Keller's broad-brush comparison of search engines with social media platforms, therefore, only takes us so far: while the former may *in general* pose a greater threat to privacy but have a weaker free speech claim, it is not hard to generate examples where both propositions are decisively reversed. The conclusion, therefore, seems clear: in each case, a court or regulator would have to treat the status of the data controller (search

131. Namely information relating to health see *GDPR*, *supra* note 1, art 9(1).

132. An example along these lines is actually used by Keller to show the potentially draconian effect of a right to restrict processing under Article 18 (i.e. pulling the item offline), pending investigation as to whether e.g. the data is inaccurate: Keller, "Right Tools", *supra* note 5 at 40.

133. See e.g. *Von Hannover*, *supra* note 25 ("[t]he Court considers that a fundamental distinction needs to be made between reporting facts . . . capable of contributing to a debate in a democratic society, relating to politicians in the exercise of their functions, for example, and reporting details of the private life of an individual who … does not exercise official functions. While in the former case the press exercises its vital role of 'watchdog' in a democracy by contributing to 'impart[ing] information and ideas on matters of public interest . . . it does not do so in the latter case" at para 63).

engine or host) as but one factor amongst many in weighing the strength of the RTBF claim.

3. Reliance on the Journalism Exemption or Freedom of Expression

The final issue concerns the ability of bodies like Facebook, Twitter and private individuals to claim either the "special purposes" journalism exemption or their own freedom of expression as a defence to RBTF claims. As noted above,[134] the *GDPR* provides in Article 85 for Member States to legislate to provide specific exemptions for freedom of expression and the special purposes. The UK's legislation for this purpose, the *Data Protection Act 2018*, provides a sweeping exemption: the requirements of lawful processing and the other data protection principles, together with all the key rights of the data subject (including Article 17), do not apply where:

> (2) (a) the processing is being carried out with a view to the publication by a person of journalistic, academic, artistic or literary material;
>
> (b) the controller reasonably believes that the publication of the material would be in the public interest;
>
> (3) The listed *GDPR* provisions do not apply to the extent that the controller reasonably believes that the application of those provisions would be incompatible with the special purposes;
>
> (4) 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.[135]

This is a very broad exemption,[136] though much will depend on its

134. See above, at 23–24.

135. *2018 Act*, *supra* note 94, schedule 2, paras 26(2)–(4).

136. It is in substance the same (with the addition of "academic purposes") as the exemption provided in the previous *Data Protection Act 1998* (UK), c 29, which implemented the previous Directive, *1995 Directive*, *supra* note 1.

interpretation.[137] The first question is who will fall within it. In *Google Spain*, the CJEU said that "the processing carried out by the operator of a search engine"[138] did not appear to fall within the journalism exemption; Google was not able to rely on it. The English High Court, in the first *Google Spain*-style case heard in the UK,[139] followed this, finding that Google acts:

> for a commercial purpose which, however valuable it may be, is not undertaken for any of the special purposes, or "with a view to" the publication by others of journalistic material. Such processing is undertaken for Google's own purposes which are of a separate and distinct nature.[140]

What then of operators like Facebook and Twitter? Notably in *Google Spain*, the CJEU, in the same paragraph as that cited above, said that "the processing by the publisher of a web page consisting in the publication of information relating to an individual may … be carried out 'solely for journalistic purposes' and thus fall within the journalism exemption".[141] In a more recent decision the CJEU said that activities:

> may be classified as 'journalistic activities' if their object is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They are not limited to media undertakings and may be undertaken for profit–making purposes.[142]

The importance of intermediaries was recognised by the Advocate General in *Google Spain,* who said that they "act as bridge builders between content providers and internet users … " thus playing a role that "has been considered as crucial for the information society".[143] Also

---

137. Courts are likely to follow the interpretation given to the very similar provision in the 1998 Act: see e.g. *Campbell v MGN*, [2002] EMLR 30 (CA (Eng)) at para 85, confirming that actual publication of newspapers (online and in hard copy) as well as processing *with a view to publication* falls within the exemption.
138. *Google Spain*, *supra* note 4 at para 85.
139. *NT1*, *supra* note 113.
140. *Ibid* at para 100.
141. *Google Spain*, *supra* note 4, at para 85.
142. *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, C-73/07, [2008] ECR I-09831 at para 61.
143. *Google Spain*, *supra* note 4 at para 36.

of relevance here is Recital 153 of the *GDPR*, which provides:

> In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, *broadly*.[144]

This is in line with the definition of "journalist" given by the Council of Ministers of the Council of Europe, quoted with approval in a recent Strasbourg judgment as being "any natural or legal person who [was] regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication".[145]

All of the above would appear to support the notion that at least *some* content appearing on Facebook, Twitter and the like, could be considered journalism, even where not published by professional journalists. But however broadly and flexibly the notion is interpreted it would seem highly unlikely that it could cover *all* kinds of content: As the High Court in the English *Google*[146] case put it:

> [T]he concept is not so elastic that it can be stretched to embrace every activity that has to do with conveying information or opinions. To label all such activity as "journalism" would be to elide the concept of journalism with that of communication.[147]

Erdos notes that many national DPAs hold that the special purposes derogation "only protects forms of expression undertaken by individuals which are patently akin to that of professional journalism".[148] Even the extensive definition of the Council of Ministers just quoted would confine it to persons *regularly* engaged in "the dissemination of information to the public".[149] This could, for example, include someone who regularly uses Twitter or Facebook to post information about and comment on issues of the day; it would *not* cover someone simply posting pictures of, e.g., a relative's baby. Erdos comments that:

> In referring to special *purposes* rather than special *actors,* [the definition in the

144. *GDPR*, *supra* note 1, recital 153 [emphasis added].
145. *Satakunnan*, *supra* note 60 at para 118.
146. *NT1*, *supra* note 113.
147. *Ibid* at para 98.
148. Erdos, "Domestic", *supra* note 106 at 276.
149. *Satakunnan*, *supra* note 60 at para 118.

> *GDPR*] is not restricted to professional journalists, artists and academic or non–academic writers but rather is in principle open to everyone (a reality given emphasis by the CJEU in *Satamedia*) including private individuals.[150]

And he argues that:

> [T]he *GDPR*'s apparent removal of the [previous] requirement that processing be conceptualised as "solely" for the special expressive purposes as well its general emphasis on construing this clause "broadly" [Recital 153] provides an opportunity to decisively reject … prioritisation of expression by actors with a particular professional status.[151]

He, therefore, concludes that the journalism exemption *should* cover "individuals disseminating a message to the collective public"[152] but that it will probably *not* cover those engaging merely with "self expression" and the "linked general freedom to converse".[153]

If this is right, then courts and regulators will, over time, have to engage in the extremely difficult task of classifying certain content on Twitter and Facebook as posted for journalistic purposes (e.g. comments on politics and current affairs), and some as not (e.g. family pictures). If the *content* is classified as falling within the "journalistic purposes" exemption, there would seem no good reason to hold that the individual poster *can* claim the journalism exemption but that the host (Facebook, Twitter) could not. Even if a court were minded to make this distinction it would make no difference in practice: if only the individual poster was classified as falling within the journalism exemption, a RTBF claim made against Facebook, for example, could be resisted on the basis that the disputed content fell within the purposes of journalism, seen from the perspective of the original poster.

Finally, even where content is *not* considered journalism, a host (or individual user) could still resist an Article 17 request on the basis that "the processing was necessary for exercising the right of freedom of expression"[154] of the original poster. The CJEU has said consistently, as far

150. *Ibid* at 289.
151. *Ibid* at 290.
152. *Ibid*.
153. *Ibid*.
154. *GDPR*, *supra* note 1, art 17(3)(a).

back as the *Lindqvist* case, that both data protection authorities and courts have a duty in certain cases outside of the special purposes exemption to interpret data protection rules with regard for freedom of expression.[155] How far eventual interpretation of the *GDPR* will privilege journalistic purposes over the freedom of expression of ordinary members of the public remains at present a matter of speculation. Much may depend on the particular legislation introduced by national Parliaments,[156] as well as the policies and guidance of national DPAs. What also remains to be seen is how far intermediaries like Facebook and Twitter will go in seeking to defend the freedom of expression of its individual users, given that the original posters of material will not, seemingly be involved at all in decisions on whether to remove the content pursuant to deletion requests. This is something that Keller argues is a major structural problem with

155. *Lindqvist*, *supra* note 20 at para 87.

156. The sweeping exemption granted by the UK's *Data Protection Act 2018*, *supra* note 94, only applies to "special purposes" material, but broader exemptions to protect freedom of expression and information may subsequently be introduced by UK Regulation made under section 16. Section 16(1)(c) gives the Secretary of State power to make regulations for the purposes of the power in Article 85(2) to provide for exemptions or derogations from certain parts of the *GDPR* where necessary to reconcile the protection of personal data with the freedom of expression and information. These will likely be similar to the terms of the previous *Data Protection (Processing of Sensitive Personal Data) Order 2000* (UK), 2000 no 417, which the *2018 Act* revoked (per Schedule 19).

RTBF under European data protection law.[157]

IV. A Possible Role for Article 8 ECHR?

Article 17 is a new and broadly-framed provision and offers little guidance as to its proper interpretation, in particular how the tension it creates with freedom of expression, should be resolved. The Working Party's guidance on *Google Spain* said that, "in determining the balance" between data protection rights and freedom of expression, "the case-law of the European Court on Human Rights is especially relevant".[158] Hence the remainder of this paper will consider how far the Strasbourg's Article 8 privacy jurisprudence may guide interpretation of Article 17, an analysis not yet attempted in the literature. It will do so by elucidating principles from that jurisprudence, and considering whether they are either: (a) applicable to the interpretation of the right to be forgotten; (b) applicable but with modification; or (c) inapplicable.

---

157. Daphne Keller, "The 'Right to Be Forgotten' and National Laws Under the GDPR" *Inforrm* (4 May 2017), online: Inforrm <https://inforrm.org/2017/05/04/the-right-to-be-forgotten-and-national-laws-under-the-gdpr-daphne-keller> (Keller discusses in detail a number of serious issues concerning procedural fairness relating to the handling of RTBF requests under Article 17: she points out that the original speaker who provided the content (e.g. the author of a Tweet) will not be represented during the decision of a host (or search engine) as to whether to remove (or delist) the content, which, she argues, "puts a very heavy thumb on the scales against the [speaker]" at para 15. She also points out that, while data subjects can appeal a refusal to delete to the DPA, and ultimately to the courts, there are "no public correction mechanism for cases where Google actually should de-list *less* [emphasis in original]" (*ibid*, para 18). Finally, in "Right Tools", *supra* note 5, Keller highlights that in most cases, online service providers are not even allowed to tell the accused user that her content has been de-listed or erased. This, she argues, "places the fate of online expression in the hands of accusers and technology companies – neither of whom has sufficient incentive to stand up for the speaker's rights" at para 48).
158. Article 29 Google Spain Guidelines, *supra* note 6 at 14.

A. The General Relevance of Strasbourg Case Law

It is clear beyond argument that Strasbourg jurisprudence will be relevant to the interpretation of the *GDPR*. Article 52(3) of the EU Charter states that when Charter and ECHR rights overlap the ECHR's definition (in effect, Strasbourg's interpretation) of the right should be taken to be the same as that of the corresponding provision within the Charter.[159] In other words Charter rights must be interpreted consistently with ECHR rights that correspond to them and are thus "complementary" to the ECHR rights.[160] Since the right to privacy in Article 8 ECHR corresponds with Article 7 of the EU Charter,[161] Strasbourg jurisprudence is directly relevant to the CJEU and European courts' formulation of Article 17. This is enhanced by the long-standing inter-court comity between the CJEU and Strasbourg. Both courts regularly cite each other's judgments,[162] in many cases the CJEU taking Strasbourg's more experienced lead when adjudicating upon fundamental rights.[163] Over the course of the last decade a strong working relationship between the two courts has been fostered.[164]Further, the "*Bosphorus* presumption", whereby Strasbourg operates a rebuttable presumption that EU law offers

159. EU Charter, *supra* note 21, art 52(3); see Wolfgang 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 at 64–67.
160. Tommaso Pavone, "The Past and Future Relationship of the European Court of Justice and the European Court of Human Rights: A Functional Analysis" *Social Science Research Network* (28 May 2012) at 13, online: SSRN <https://ssrn.com/abstract=2042867>.
161. EU Charter, *supra* note 21.
162. Noreen 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 at 1815.
163. Pavone, *supra* note 160 at 1.
164. O'Meara, *supra* note 162 at 1816. See also Sylvia de Vries, "EU and ECHR: Conflict or Harmony?" (2013) 9:1 Utrecht Law Review 78 at 79 (it has been said that lines are becoming "increasingly blurred" between rights protection afforded between the ECtHR and the CJEU).

rights protection at least equivalent to that of the ECHR, shows the privileged nature of EU law at Strasbourg. Overall, the strong structural relationship between the two courts[165] means that Strasbourg case law is likely to have a significant influence on the interpretation of the EU's new data protection framework.

B. How Strasbourg's Article 8 Jurisprudence Might Apply

Strasbourg has developed the test of whether a claimant had a "reasonable expectation of privacy" ("REP") in order to decide Article 8 claims in a plethora of cases, including *Halford v UK*,[166] *PG & JH v UK*,[167] *Peck v UK*,[168] *Perry v UK*[169] and more recently *Von Hannover v Germany* (*nos 1, 2 & 3*)[170] and *Lillo-Stenberg and Sæther v Norway*.[171] In deciding whether such an expectation arises, Strasbourg uses the factors discussed in Part V below. If a REP is *not* established, the claim fails; if it is, the court proceeds to balance the Article 8 claim against the right to freedom of expression under Article 10; in doing so it will often return to the same

165. Which will be strengthened further once the planned accession of the EU to the ECHR goes ahead, as required by the EC, *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*, [2007] OJ, C-306/01, art 6(2). The process is currently stalled but see e.g. Christina Eckes, "EU Accession to the ECHR: Between Autonomy and Adaption" (2013) 76:2 Modern Law Review 254; Tobias Lock, "The Future of the European Union's Accession to the European Convention on Human Rights after Opinion 2/13: Is it Still Possible and is it Still Desirable?" (2015) 11:2 European Constitutional Law Review 239.
166. *Halford v United Kingdom*, No 20605/92, [1997] 24 EHRR 523.
167. *PG and JH v United Kingdom*, No 44787/98, [2001] IX ECHR 195 [*PG*].
168. *Peck v United Kingdom*, No 44647/98, [2003] I ECHR 123 [*Peck*].
169. *Perry v United Kingdom*, No 63737/00, [2003] IX ECHR 141 [*Perry*].
170. *Von Hannover*, *supra* note 25; *Von Hannover v Germany (no 2)*, No 40660/08 [2012] I ECHR 399 [*Von Hannover no 2*]; *Von Hannover v Germany (no 3)*, No 8772/10, [2013] V ECHR 264 [*Von Hannover no 3*].
171. *Lillo-Stenberg and Sæther v Norway*, No 13258/09, [2014] ECHR 59 [*Lillo-Stenberg*].

factors in order to consider the *weight* of the privacy claim.[172] There are several different possibilities as to how courts and regulators in Europe might use elements of the REP test to guide their interpretation of Article 17. Different national courts may, at least for some time, produce different interpretations of this relationship, which will remain until authoritative guidance is provided by the CJEU or the new EU Data Protection Board, which will take time. Moreover, given that the *GDPR* specifically allows national legislatures to flesh out aspects of the new regime via national law, there is room for divergent national approaches to flourish permanently, as indeed happened under the previous EU data protection scheme.[173] There is also the intriguing possibility of a clash between the *GDPR* and the European Convention on Human Rights: a claim could be brought to the Strasbourg court that a particular ruling under Article 17 by a national court violates the right to freedom of expression under Article 10.[174]

There are a number of possible approaches that courts and Regulators might take to the relevance of Strasbourg's REP test to Article 17. These include:

1. Determining that the deletion right only applies where the data

172. See H. Tomás Gómez-Arostegui, "Defining 'Private Life' Under Article 8 of the European Convention on Human Rights by Referring to Reasonable Expectations" (2005) 35:2 California Western International Law Journal 153, online: CWILJ <https://scholarlycommons.law.cwsl.edu/cgi/viewcontent.cgi?referer=https://www.google.ca/&httpsredir=1&article=1164&context=cwilj>.

173. David Erdos made the first systematic study of national laws implementing Directive 95/46 in terms of the protection they provided for media freedom: see David Erdos, "European Union Data Protection Law and Media Expression: Fundamentally Off Balance" (2016) 65:1 International and Comparative Law Quarterly 139 (he found "a total lack of even minimal harmonisation" (abstract) and, in different member states "outcomes ranging from subjecting the media to entirely inappropriate peremptory rules to completely eliminating the individual's substantive data protection rights when they come into conflict with media expression" at 180).

174. *Satakunnan*, *supra* note 60, concerned such an unsuccessful claim (although not of course in relation to the *GDPR*).

subject has a reasonable expectation of privacy. This would seem an implausibly restrictive interpretation of Article 17, but one that media bodies, including social media companies, may seek to argue before national courts and regulators.

2. Treating the REP test as wholly irrelevant to the right to be forgotten; given the Working Party's clear view of the importance of the Strasbourg jurisprudence[175] this seems unlikely.
3. Using the REP factors *only* in order to reconcile an erasure claim under Article 17 with the freedom of expression exception.[176]
4. Using the test or factors from it to assist in determining whether RTBF would apply only in doubtful or borderline situations, where the deletion request was particularly contentious in some way. In particular, consideration of factors derived from the REP test could help resolve:
    - the scope of the household exemption;[177]
    - in relation to "sensitive" data, whether the individual had deliberately made it public;[178]
    - whether and when hosts should be fixed with liability as data controllers;[179]
    - where the deletion request is made on the basis of the data subject's objection to processing being carried out "for the purposes of legitimate interests pursued by the data controller or a third party", determining which interests can be outweighed by "the interests or fundamental rights and freedoms of the data subject".[180] Factors from the REP test could help determine how strongly those interests are

175. Above, at 39.
176. *GDPR*, *supra* note 1, art 17(3)(a).
177. Discussed above, Part III.C.1.
178. *GDPR*, *supra* note 1, art 9(2)(e) (such a finding could ground an alternative basis for processing other than consent — which may be withdrawn under Article 9).
179. Recalling that in *Google Spain*, *supra* note 4, the CJEU decided that Google should be treated as a data controller partly because of the serious impact that its activities could have on the data subject's privacy.
180. *GDPR*, *supra* note 1, art 6(1)(f).

engaged; and
- the overall balance of a RTBF request with freedom of expression and/or the purposes of journalism.

At this point it will be helpful to give examples of different ways in which personal data may be disseminated online; these may affect the balance between expression and privacy rights and hence how the principles employed by the Strasbourg Court in adjudicating Article 8 claims may apply to the right to erasure.

1. Data Dissemination Scenarios

i. Information concerning a data subject ("A") is uploaded by a third party ("B") without A's consent (the "third party scenario")

Personal data placed online in this manner directly parallels traditional Article 8 claims considered in the Strasbourg case law. Nearly all its privacy jurisprudence concerns non-consensual publication of personal information by a third party, often the press, as in key cases like *Von Hannover*[181] and a more recent decision in which a celebrity couple complained of covert photographs of them published by a Norwegian magazine.[182] In such scenarios, Strasbourg principles pertaining to the weight of the Article 8 claim could be directly "read across" to Article 17 cases. Strasbourg has made clear that the processing of personal data by an external actor that creates a permanent record of an event is a significant consideration in determining whether a REP exists.[183] Indeed Strasbourg has appeared willing to find a breach of Article 8 in relation to personal data merely *stored* by a third party against a subject's wishes.[184] Such storage will often be a significantly less serious breach of privacy than the *dissemination* of personal data online, as would be the case with a claim under Article 17 of the *GDPR*. If European courts take Strasbourg's lead

181. *Von Hannover*, *supra* note 25.
182. *Lillo-Stenberg*, *supra* note 171.
183. *PG*, *supra* note 167.
184. *Amann v Switzerland*, No 27798/95, [2000] II ECHR 245 at para 70.

in this regard this would tend to give Article 17 a wide ambit.[185]

ii. A data subject ("A") made personal data available online; it is reposted without consent to third party sites and A wishes to delete it (the "data leak" scenario)

A crucial factor here will be whether the initial posting was (a) to a restricted forum (e.g. a controlled group of Facebook "friends"); or (b) to the world at large (e.g. on Twitter or to "the public" on Facebook).[186] The Strasbourg case law can be readily used to support an expectation of privacy in scenario (a), *provided* that the data subject could not have reasonably foreseen that the information would be viewed by such a large audience.[187] There are obvious parallels here with *Peck v UK, PG and JH* and *Perry*. In *Peck,* stills of a CCTV recording distributed by the local council of the aftermath of Peck's suicide attempt on a public street (he had attempted to cut his wrists) were broadcast on national television.[188] Strasbourg held that while Peck would have realised that any passers-by in the street at the time could have seen him, he could not reasonably have anticipated that his actions would end up being viewable by a mass audience.[189] Similarly, in both *PG and JH* and *Perry,* Strasbourg found

185. However, the situation would be more difficult were B to publish personal data about A *alongside* information about themselves, e.g. where B uploads a photograph onto a social networking site that shows A and B together. A deletion request would raise a direct conflict between B's autonomy (manifested in their expressive act of posting the photo) and A's autonomy (manifested in their desire to exercise informational control over it); see Geoffrey Gomery, "Whose Autonomy Matters? Reconciling the Competing Claims of Privacy and Freedom of Expression" (2007) 27:3 Legal Studies 404.

186. As already noted, in the former case, at least the poster of the data might well not even be treated as a data controller: above, at 28.

187. In the case of *Peck*, *supra* note 168, the ECtHR stated that Mr Peck, who had attempted to commit suicide on a public street, had a partial expectation of privacy as he could not have reasonably foreseen that the stills of the CCTV footage of the event would be broadcast on television and distributed to other police constabularies.

188. *Peck*, *ibid* at paras 10–15.

189. *Ibid* at para 62; Gómez-Arostegui, *supra* note 172 at 17.

the existence of an REP due to the fact the claimants' data had been processed in more extensive a manner than they could have reasonably foreseen.[190]

However, the Strasbourg REP test does not naturally apply where the data subject had initially uploaded the data to a publically accessible online domain: in such circumstances, Strasbourg would presumably reason that the claimant should have foreseen that in uploading data to a public platform he or she was exposing it to an unknown and hence unlimited amount of users. As such, the claimant would appear to have voluntarily surrendered control over who accesses the data.[191] This reveals a potential tension between the REP test and Article 17. The former focuses upon the degree of publicity that a claimant could have *reasonably foreseen*;[192] Article 17 emphasises the importance of a data subject's ability to rescind their consent to previous publication of private data.[193] As discussed above, this upholds the ability of a subject to regain data privacy lost online (even through their own initial act of publication), rather than focusing only on their expectations at the time of the initial disclosure: in this way Article 17 treats informational self-determination as a *continuing* process.

Despite this difference, can some common ground be found here? In *Pretty v United Kingdom*[194] the Court found that the "notion of personal autonomy is an important principle underlying the interpretation of

190. *PG*, *supra* note 167; *Perry*, *supra* note 169.
191. In all of the following cases the press made personal information known without consent: *Lillo-Stenberg*, *supra* note 171; *Von Hannover*, *supra* note 25; *Von Hannover (no 2)*, *supra* note 170; *Von Hannover (no 3*), *supra* note 170.
192. *Peck*, *supra* note 168; *PG*, *supra* note 167; *Perry*, *supra* note 169.
193. *GDPR*, *supra* note 1, art 17(1)(b).
194. *Pretty v United Kingdom*, No 2346/02, [2002] III ECHR 155.

its guarantees".[195] As discussed above, the right to delete is designed to enhance autonomy in its informational form, by affording individuals greater control over dissemination of their personal data.[196] Given that the application of a conventional REP test would here rob the right to delete of much of its effectiveness, it arguably needs some re-working so as to recognise informational autonomy as a continuing process.[197] Rather than European courts using Strasbourg's REP test to limit the scope of Article 17 right to delete, it might instead be for Strasbourg to reconsider the test in light of Article 17 and the changing nature of privacy in the digital age. The "reasonable expectation" of a user might in appropriate circumstances be said to encompass the ability to rescind a former publication of private data. It should be recalled that if this were accepted, this would only ground a *prima facie* claim for deletion:[198] it would then have to be balanced against freedom of expression under Article 17(3)(a).

195. *Ibid* at para 61; see also Begüm Bulak and Alain Zysset, "'Personal Autonomy' and 'Democratic Society' at the European Court of Human Rights: Friends or Foes?" (2013) 2:1 UCL Journal of Law and Jurisprudence 230. Althaf Marsoof, "Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression" (2011) 19:2 International Journal of Law and Information 110.
196. Reding, *supra* note 27.
197. Above, at 19–20.
198. Which itself would only apply where withdrawal of consent *per se* grounded an Article 7 claim: see above, at 25–26.

V. Factors Going to the Weight of the Article 8 Claim and Their Possible Application to RTBF

A. The Nature of the Information

Strasbourg has previously found that bodily integrity,[199] sexuality,[200] family grief,[201] personal identity[202] and personal information[203] are all aspects of private life under Article 8. In general it has stressed that the more intimate the personal data disclosed, the stronger the claim to privacy will be.[204] An individual's sexual or romantic life is viewed as particularly sensitive and thus an important aspect of their private life.[205] For example, in *Avram v Moldova*, women were secretly filmed by the police frolicking in a sauna with male police officers in a state of partial undress and the footage later passed to local television stations and broadcast. Strasbourg found a breach of Article 8, stressing that an individual's sexual and romantic life should be free from unwanted observation by others.[206]

One area of uncertainty here is the approach taken to "intimate" information. What is considered intimate can vary, depending upon

199. *X and Y v The Netherlands*, No 8978/80, [1985] 8 EHRR 235; see also Lorenc Danaj and Aleks Prifti, "Respect for Privacy from the Strasbourg Perspective" (2012) 2012:5 Academicus: International Scientific Journal 108.
200. *ADT v United Kingdom*, No 35765/97, [2000] IX ECHR 295.
201. *Pannullo and Forte v France*, No 37794/97, [2001] X ECHR 279.
202. *Van Kück v Germany*, No 35968/97, [2003] VII ECHR 1.
203. *Smirnova v Russia*, No 46133/99, [2003] IX ECHR 241.
204. *Von Hannover (no 2)*, *supra* note 170; *Von Hannover (no 3)*, *supra* note 170.
205. See e.g. *Dudgeon v United Kingdom*, No 7525/76, [1981] 4 EHRR 149; and Gómez-Arostegui, *supra* note 172 at 6.
206. *Avram v Moldova*, No 41588/05 (5 July 2011) [*Avram*]; Dirk Voorhoof, "European Court of Human Rights: Avram and other v Moldova" (2012) 1:1 Iris: Legal Observations of the European Audiovisual Observatory 1.

factors such as culture, religion, gender, age and personality type.[207] It is also fact-sensitive: while Strasbourg generally views data concerning an individual's romantic life as peculiarly intimate, in *Lillo-Stenberg v Norway* it held that a wedding was not necessarily a private occasion.[208] As noted above, while Article 17 covers all personal data, the *GDPR* specifies certain categories as particularly sensitive (above, at 22–23). These should, however, be applied with a degree of flexibility, especially when assessing unusual or complex claims. At the national level this may depend upon what specific provision Member States make to allow freedom of expression claims to outweigh the prohibition on processing personal data.[209] Article 17 itself does not distinguish between sensitive and ordinary data, in providing that deletion requests may be refused where necessary "for exercising the right of freedom of expression",[210] but even when engaging in this kind of "pure" balancing act, courts are likely to find that, as the Working Party put it:

> *As a general rule*, sensitive data … has a greater impact on the data subject's private life than 'ordinary' personal data. A good example would be information about a person's health, sexuality or religious beliefs. DPAs are *more likely to intervene* when de-listing requests are refused in respect of search results that reveal such information to the public.[211]

Following this approach, domestic courts may seek to find ways of avoiding automatic consequences that may flow from the classification of data as "sensitive". As Lady Hale said in the leading privacy decision of *Campbell v MGN Ltd*,[212] while medical information relating to health is generally considered obviously private, "[t]he privacy interest in the fact that a public figure has a cold or a broken leg is unlikely to be strong enough to justify restricting the press's freedom to report it. What harm

207. Chris Hunt, "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2011) 37:1 Queen's Law Journal 167 at 197–200.
208. *Lillo-Stenberg*, *supra* note 170 at para 37.
209. See the example of provisions in the UK's *Data Protection Act 2018, supra* note 156.
210. *GDPR*, *supra* note 1, art 17(3)(a).
211. Article 29 Google Spain Guidelines, *supra* note 6 at 17 [emphasis added].
212. *Campbell*, *supra* note 63.

could it possibly do"?[213] We suggest that courts taking this more flexible, fact-sensitive approach should employ a mixed objective-subjective test, relying upon a mixture of cultural and contextual factors. These could include an examination of what information may normally be considered intimate for someone of the same age or religion, as well as an examination of a subject's personal sensitivities: for example, a person who had had gender reassignment surgery would likely be particularly sensitive about a photograph circulating that showed them as their previous gender.[214]

B. The Form of the Information: Images or Text?

When assessing the strength of Article 8 claims, Strasbourg may take into account the form in which the personal data is disclosed — such as photographs, sound recordings or written text.[215] Thus "privacy may be thought of as being domain specific".[216] Strasbourg has treated privacy rights relating to photographs as particularly significant: as Gomery observes, "it has become plain that the courts treat *images* of a person in a public space differently than they would a *description* of the person in the same place because a photograph may make a data subject clearly 'identifiable'".[217] As Marsoof comments in relation to the English decision in *Douglas v Hello!*:[218]

---

213. *Ibid* at 157.
214. See Hunt, *supra* note 207 at 197–99 arguing that both individual sensitivities and cultural or community norms need to be considered. On privacy as particularly engaging certain types of information bearing on an individual's reputation and therefore their dignity, see generally Ruth Gavison, "Privacy and the Limits of the Law" (1980) 89:3 Yale Law Journal 421 at 457; Robert Post, "Three Concepts of Privacy" (2000) 89:6 Georgetown Law Journal 2087; Robert Gerstein, "Intimacy and Privacy" in Ferdinand Schoeman, ed, *Philosophical Dimensions of Privacy* (Cambridge: Cambridge University Press, 1984) 266 at 270; and David Hughes, "Two Concepts of Privacy" (2015) 31:4 Computer Law & Security Review 527 at 534.
215. See Gomery, *supra* note 185 at 427.
216. Marsoof, *supra* note 195 at 129.
217. Gomery, *supra* note 185 at 427 [emphasis added].
218. [2006] QB 125 (UK) citing *Douglas v Hello!*, *supra* note 77 at para 106.

> the unauthorised publication of photographs has been condemned more forcefully than other forms of privacy leaks. In *Douglas v Hello!* it was observed that "[a] photograph can certainly capture every detail of a momentary event in a way which words cannot, but a photograph can do more than that. A personal photograph can portray, not necessarily accurately, the personality and the mood of the subject of the photograph."[219]

Similarly, in *Von Hannover v Germany (no 2)*,[220] Strasbourg said:

> [A] person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development.[221]

Article 17 does not refer to particular forms of personal data but it appears likely that many individuals will wish to use it to delete online photographs of themselves. Stories abound of online photographs having a subsequent detrimental impact on a person's private life or their career.[222] However other forms of personal data accessible online, including text, also have the potential to be significantly detrimental to a data subject's privacy or reputation, especially if they describe intimate details of, for example, their sex life. Hence courts and regulators should undertake a flexible approach on a case-by-case basis when deciding upon deletion requests. It may often be the case that the *content* of the data and the repercussions of its open accessibility on the data subject are more important than its form.

---

219. Marsoof, *supra* note 195 at 129.
220. *Von Hannover (no 2)*, *supra* note 170.
221. *Ibid* at para 96.
222. Daniel Bean, "11 Brutal Reminders That You Can and Will Get Fired for What You Post on Facebook" *Yahoo* (6 May 2014), online: Yahoo <https://www.yahoo.com/tech/11-brutal-reminders-that-you-can-and-will-get-fired-for-84931050659.html>. See e.g. "Teacher sacked for posting picture of herself holding glass of wine and mug of beer on Facebook" *The Daily Mail Online* (7 February 2011), online: The Daily Mail Online <*www.dailymail.co.uk/news/article-1354515/Teacher-sacked-posting-picture-holding-glass-wine-mug-beer-Facebook.html*> (schoolteacher Ashley Payne's employment was terminated due to photographs of her on Facebook, showing her drinking alcohol on holiday).

C. Is the Data Subject a Public Figure?

1. The Importance of the "Public Figure" Criterion.

One of the most important factors used by courts and regulators in assessing privacy claims is whether the claimant is a "public figure". In *Google Spain* the CJEU said that the legitimate interest of the public in having information available on social networks "may vary, *in particular, according to the role played by the data subject in public life*".[223] In its commentary on the decision, the Working Party said: "there may be information about public figures that is genuinely private and that should not normally appear in search results, for example information about their health or family members".[224] But it went on:

> [A]s a rule of thumb, if applicants are public figures, and the information in question does not constitute genuinely private information, there will be a stronger argument against de-listing search results relating to them.[225]

The English High Court, when applying *Google Spain* domestically, found this criterion, of "playing a role in public life" to be "broader" than the notion of being a public figure like a politician or sportsperson.[226] But the notion that the Working Party meant to postulate the widest possible approach to the concept of public figure seems doubtful. In particular, their explanation that, "[a] good rule of thumb is to try to decide where the public having access to the particular information … would protect them against improper public or professional conduct",[227]suggests that the fact that a given celebrity was well known to the public would be less important than whether knowing the information in question could protect the public against improper conduct on their part. Given that members of the public are generally not affected by the way in which celebrities behave in their private lives this may suggest a more restricted approach. This is supported further by

223. *Google Spain*, *supra* note 4 at para 81 [emphasis added].
224. Article 29 Google Spain Guidelines, *supra* note 6 at 14.
225. *Ibid* at 14.
226. *NT1*, *supra* note 113 at para 137.
227. Article 29 Google Spain Guidelines, *supra* note 6 at 13.

the Working Party's guidance that:

> [t]here is a basic distinction between a person's private life and their public or professional *persona*. The availability of information in a search result becomes more acceptable the less it reveals about a person's private life.[228]

In sum, the view of the Working Party would seem to point away from the notion that a celebrity, for example, has a reduced expectation of privacy in relation to information concerning core areas of their private life, such as their sex-life, family matters or health, simply by virtue of their fame.

In strong contrast, it appears that Google, when deciding RTBF requests to date, treats "public figure" as meaning simply "someone recognised at national or international level", something it decides simply by "a search of relevant URLs or names".[229] The problem with this is that fame can bear no relationship to importance. An extreme and notorious example is the overweight 16-year-old boy who became known as "Little Fatty": a picture taken of him in the street by chance went viral in Asia with "hit" rates in the tens of millions and eventual coverage in Reuters and the Independent.[230] Clearly this boy would (at least at the time) have fitted Google's definition of a "public figure", since he would be recognised at national *and* international level. But if this is the case then the notion of "public figure" risks becoming completely un-tethered from any links it once had with the notion of a *legitimate* public interest in the persons' doings, as with a politician or public official. It also suggests that one basis for making someone a legitimate target for public attention is simply that in the past they have attracted public attention. Under this approach the media — and indeed ordinary internet users — can reduce a person's expectation of privacy simply by constantly intruding into their privacy. In such circumstances, the very person who needs privacy most — because they are constantly suffering from intrusion — is granted less of it, because of the very attention they are seeking to escape. It may be that this issue will not arise in the large majority of RTBF requests — a

228. *Ibid* [emphasis in original].
229. Brock, *supra* note 16 at 51.
230. Cheung, *supra* note 78.

recent study found that fewer than 5% of delisting requests under *Google Spain* concerned "criminal, politicians or high-profile public figures" [231] — but it is important nonetheless.

2. Strasbourg's Approach to "Public Figures"

The position of the Strasbourg Court in relation to the right to privacy of public figures and celebrities is unclear. The Court has certainly been prepared to find that celebrities and public figures still have rights to privacy: Princess Caroline of Monaco won her first case at Strasbourg despite the finding by the German Constitutional Court that she was a "public figure par excellence"[232] — a finding that led the German courts to hold that she had to tolerate being constantly followed and photographed by paparazzo as she went about her daily life. Strasbourg found that the partial denial by German law of a remedy for such constant intrusive publicity breached Article 8.[233] In *Lillo-Stenberg v Norway,* Strasbourg reiterated that:

> in certain circumstances, even where a person is known to the general public, he or she may rely on a "legitimate expectation" of protection of and respect for his or her private life.[234]

However, Strasbourg does appear to regard a person's public figure status as *reducing* their expectation of privacy. Thus, in *Von Hannover (no 2)* the Grand Chamber said that, "[Princess Caroline] and her partner, who are undeniably very well known, [cannot be viewed as] ordinary private individuals. They must, on the contrary, be regarded as public figures",[235] and hence afforded a somewhat reduced expectation of privacy. It is notable that the reason the Court gave for this finding was not that Princess Caroline is a member of a royal family, or that she performs official functions (she does not) but simply because of her celebrity

231. Brock, *supra* note 16 at 51, citing Google, "Transparency Report: Search Removals Under European Privacy Law" *Google* (2018), online: Google <https://www.google.com/transparencyreport/removals/europeprivacy/>.
232. *Von Hannover*, *supra* note 25 at paras 19–21.
233. *Ibid*.
234. *Lillo-Stenberg*, *supra* note 171 at para 97.
235. *Von Hannover (no 2)*, *supra* note 170 at para 120.

status. Similarly, in *Axel Springer*,[236] the claimant "X" was well known to the public because he played one of the main characters in a popular TV series. The Grand Chamber judgment remarked:

> [T]hat role was, moreover, that of a police superintendent, whose mission was law enforcement and crime prevention. That fact was such as to increase the public's interest in being informed of X's arrest for a criminal offence. Having regard to those factors and to the terms employed by the domestic courts in assessing the degree to which X was known to the public, *the Court considers that he was sufficiently well known to qualify as a public figure.* That consideration thus reinforces the public's interest in being informed of X's arrest and of the criminal proceedings against him.[237]

Furthermore, despite Strasbourg's comments (above) in *Lillo-Stenberg v Norway*, it ultimately found that the couple in question did *not* have a right to privacy in respect of covert photographs taken of their wedding — partly *because* they were celebrities.[238] Such cases appear to show Strasbourg finding public figure status not because of the significance of the claimant's role in public life, but simply on the basis that they are well known to the public. While in the recent Grand Chamber decision in *Couderc and Hachette Filipacchi Associés v. France*[239] the Court appeared in places to row back on this, commenting that "the right of public figures to keep their private life secret is, in principle, wider where they do not hold any official functions",[240] other parts of the judgment deny any such a distinction. Thus the Court immediately added that the principle that politicians "lay themselves open to close scrutiny of their every word and deed by both journalists and the public at large … applies not only to politicians, but to *every person* who is part of the public sphere, whether through their actions or their position".[241] The Court confirmed this approach in a passage that starts by asserting that "exercising a public function or of aspiring to political office" exposes one to greater public

236. *Axel Springer AG v Germany*, No 39954/08, [2012] ECHR 227 [*Axel Springer*].
237. *Ibid* at para 99 [emphasis added].
238. *Lillo-Stenberg*, *supra* note 171.
239. *Couderc and Hachette Filipacchi Associés v France*, No 40454/07, [2015] ECHR 992.
240. *Ibid* at para 119.
241. *Ibid* at para 121 [emphasis added].

scrutiny, but then adds immediately that "certain private actions by public figures cannot be regarded as such, given their potential impact in view of the role played by those persons on the political *or social scene*"[242] — apparently equating the roles of celebrities with politicians and public officials. Strasbourg's notion of "public figure" thus now extends well beyond politicians and others exercising real public power, to encompass those who are simply famous, for whatever reason. In particular, in *Von Hannover (no 2)* and *Axel Springer*, Strasbourg appeared to use "public figure" to mean simply a person in whose doings the public are interested. Used in this way, the public figure doctrine means that the right to privacy is sharply reduced by reference simply to public curiosity; the supposedly sacrosanct distinction between the public interest and what interests the public thus comes close to being (indirectly) collapsed.

3. Conceptual Problems with the "Public Figure" Doctrine

There is, however, a deeper problem with placing reliance on "public figure" status as a reason for reducing a person's *prima facie* expectation of privacy:[243] the concept is inherently analytically imprecise and hence not conducive of clear judicial reasoning. It acts as a relatively crude and generalised proxy for three more precise arguments that by their nature should be fact-sensitive.[244] The first is that aspects of the lives of some well-known people may become so widely publicised that they can no longer meaningfully be considered private. Quite evidently, this is no more than an unhelpful generalization. It clearly will not always be the case and cannot be decided in advance of examining the particular situation before the court. Nevertheless, a softened version of this argument — that being well known to the public per se diminishes one's reasonable

242. *Ibid* at para 120 [emphasis added].
243. The following two paragraphs draw briefly on Phillipson, *supra* note 76.
244. The three arguments correspond to those advanced by Dean Prosser in his classic exposition of the US privacy torts, see William L Prosser, "Privacy" (1960) 48:3 California Law Review 383, discussed and applied in the leading New Zealand decision, *Hoskings v Runting*, [2005] 1 NZLR 1 at para 120.

expectation of privacy — captures exactly Strasbourg's current approach. The second argument is that public figures may reasonably be considered to have consented to publicity about their private life, or "waived" their right to privacy. Such a contention makes two mistakes: first, it *assumes* that all public figures seek publicity voluntarily — which is by no means the case — and second, it draws no distinction between seeking publicity for one's *private* life, and seeking publicity in relation to one's vocation, surely an elementary distinction.

The third argument is that there is a degree of legitimate public interest in aspects of the private lives of public figures, as, for example, in the case of philandering politicians. This, however, is not a reason for reducing the scope of the protection given to public figures, but rather a description of a *countervailing* consideration, to be weighed in the balance against their right to protection for privacy. Even put in those terms it is flawed, because it again amounts to an unhelpful generalization: whether there is a legitimate public interest in the life of the public figure will depend upon the nature of the information in question, their role in public life and whether the information contributes significantly to an important public debate.

Thus far more analytical clarity can be obtained by asking each of the above questions separately and in a highly fact-sensitive way. The first question then turns into a distinct enquiry as to whether the information in question is already in the public domain; in that regard, the Grand Chamber of the Strasbourg Court has recently remarked: "[t]he fact that information is already in the public domain will not necessarily remove the protection of Article 8 of the Convention".[245] The second question is whether the public figure has waived their right to privacy by, for example, deliberately making an aspect of it public — this is considered as a separate factor in the next section. The third question falls outside the scope of this article as it concerns, not the expectation of privacy of the data subject, but the *countervailing* freedom of expression of the publisher of the data. Thus, the better approach would take note of public figure status *only* as a way of deciding whether to move on

245. *Satakunnan*, *supra* note 60 at para 134.

to considering any of the above three distinct issues. This would be a considerably more structured and sophisticated methodology — and one that avoids lumping together in one category politicians and pop stars, central bankers and footballers.

In this area then, it is suggested that reference to Strasbourg's "public figure" jurisprudence when considering RTBF is more likely to confuse than assist. The ability to keep certain aspects of one's life private is an important facet of personal autonomy and human dignity to which all individuals are *prima facie* entitled;[246] the approach suggested above upholds that principle while allowing for sensible exceptions based upon specific consequences that may *flow from* public figure status.

D. Prior Conduct of the Person Concerned as Waiving Their Right to Privacy

The Working Party's guidance on *Google Spain* suggests considering whether the content had been "voluntarily made public" by the data subject or whether at least they might reasonably have foreseen that it "would be made public".[247] Strasbourg has looked more broadly at the "prior conduct" of an individual in terms of either shunning or soliciting publicity when evaluating the strength of Article 8 claims.[248] In terms of the former there is some evidence of Strasbourg treating an individual's previous attempts to *shield* themselves from intrusion as strengthening their Article 8 claim. In *Von Hannover v Germany (no 3)*,[249] the Court acknowledged Princess Caroline's efforts to keep her private life out of the press as a relevant factor (although on the facts sufficiently considered

246. See e.g. *Campbell*, *supra* note 63, upholding in part the privacy claim of the supermodel Naomi Campbell; Gavin Phillipson, "Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act" (2003) 66:5 Modern Law Review 726; Gewirtz, *supra* note 58 at 181–82.
247. Article 29 Google Spain Guidelines, *supra* note 6 at 19.
248. *Lillo-Stenberg*, *supra* note 171; *Von Hannover (no 2)*, *supra* note 170; *Von Hannover*, *supra* note 25.
249. *Von Hannover (no 3)*, *supra* note 170.

by the German courts).[250] Similarly, in the first *Von Hannover* case, an important factor was that Princess Caroline had made considerable efforts to shield herself from the public eye.[251] In the case of an ordinary person, the element of constant media interest would of course be absent; however the basic factor of the individual's evidenced desire for a degree of privacy could be read across to an Article 17 claim in our "data leak" scenario: where the initial upload was to a restricted website (for example, viewable only to a small group of "friends" on Facebook), this "prior conduct" could be argued to evince a desire for a degree of privacy in respect of the data, which should lend weight to a deletion request.

The other side of the coin is situations in which an individual has appeared previously to *court* publicity for their private life, a situation which many courts find counts *against* an expectation of privacy.[252] In *Axel Springer* the Strasbourg court found that:

> [t]he conduct of the person concerned prior to publication of the report or the fact that the photo and the related information have already appeared in an earlier publication are also factors to be taken into consideration … However, the mere fact of having cooperated with the press on previous occasions cannot serve as an argument for depriving the party concerned of all protection against publication of the report or photo at issue.[253]

The Court's statement that previous conduct of an individual amounting to solicitation of the press would not deprive a data subject of *all* privacy rights implies that such conduct would act only to *partially* reduce an expectation of privacy. As one of us has previously noted, this statement "is of little comfort to privacy advocates" since all it does is rule out the

---

250. *Ibid* at para 55.

251. *Von Hannover*, *supra* note 25 at paras 68, 74 (the Court noted that, of the complained-of photos, one showed Caroline dining in a secluded place (a corner of a restaurant) and another her relaxing within a private members' club).

252. *Theakston v MGN Limited*, [2002] EWHC 137 (QB) (Ouseley J said that since Theakston, a TV presenter, "has courted publicity … and not complained at it when, hitherto, it has been very largely favourable to him … he cannot complain if publicity given to his sexual activities is less favourable in this case" at para 68).

253. *Axel Springer*, *supra* note 236 at para 92 [emphasis added].

extreme (and implausible) "blanket" version of waiver, in which any prior disclosures to the press negate all protection for private life.[254] Moreover, Strasbourg went on to find that as the claimant, a television actor, had previously given interviews and in doing so revealed certain details about his personal life, his reasonable expectation of privacy (and in turn the strength of a claim he could bring under Article 8) had been reduced:

> In the Court's view, he had therefore actively sought the limelight, so that, having regard to the degree to which he was known to the public, his "legitimate expectation" that his private life would be effectively protected was henceforth reduced.[255]

Notably the judgement did not explain why the claimant's previous choice to reveal certain select details about his personal life led to his reasonable expectation of privacy being reduced with respect to other personal data which he had not voluntarily disclosed.[256]

Under this approach it would appear that a data subject who had initially uploaded personal information to an openly accessible platform online and subsequently wished to remove it (perhaps after it was been posted to third party sites) might be treated as having partially waived their right to privacy. The case would also depend on whether the sole ground that the defendant had to justify processing was consent. Where this is the case, a deletion request can be based simply on revocation of consent.[257] How this will be considered where the initial consent was to what we might term "fully public" processing — that is, publication "to the world" on a public website, remains unclear. The circumstances of the original uploading could be considered in the overall balance with freedom of expression. In such circumstances, courts and regulators could consider, for example, whether the information had been put online when the data subject was significantly younger[258] or at a different

254. Phillipson, *supra* note 76 at 151.
255. *Axel Springer*, *supra* note 236 at para 101 [emphasis added].
256. Phillipson, *supra* note 76 at 150–51.
257. *GDPR*, *supra* note 1, art 17(1)(b); see above, at 25–26.
258. The *GDPR* expressly contemplates the special importance of being able to delete information placed online when the data subject was a child: see *GDPR*, *supra* note 1, recital 38, above at 25–26.

stage of their life in terms of personal life or career. It could be asked whether the data subject now has particularly pressing reasons for wanting to delete the information, as where a graduate was seeking to remove pictures of themselves behaving raucously at university parties because they were now seeking professional employment.[259] At worst, the Strasbourg "waiver" approach could be read across even to a data subject seeking the deletion of personal information published by a third party; if so, the claimant could have their privacy claim deemed weaker by virtue of *previously* having voluntarily disclosed different personal information online.

However this notion that a voluntary disclosure of private information prevents an individual from being able to complain about an involuntary disclosure is *wholly incompatible* with the core value of the individual's right to control over the release of personal information.[260] All of us exercise this right to selective disclosure in our social lives: we may tell one friend an intimate secret and not another; at times be open, at others more reticent. But someone who is shown a friend's personal letter on one occasion does not assume that they have thereby acquired the right to read, uninvited, all other such letters. In other words, to suggest that public figures should be treated as barred from complaining about publicity that is unwanted and intrusive *now*, because they had *previously* sought it, would deny them the very *control* over personal information that is inherent in the notion of personal autonomy: previous disclosures should be treated not as an *abandonment* of the right to privacy, but an *exercise* of it.[261] As suggested above, the advent of a substantive RTBF is a chance to re-conceptualise the notion of control over personal information as a continuing rather than a one-off event. Here it is to be

259. See e.g. Alan Henry, "How You're Unknowingly Embarrassing Yourself Online (and How to Stop)" *LifeHacker* (5 October 2013), online: Lifehacker <lifehacker.com/how-youre-embarrassing-yourself-online-without-knowing-495859415>; Solove, "Speech, Privacy", *supra* note 37 at 17.

260. Phillipson, *supra* note 76 at 150 (we draw briefly on this work in the paragraph that follows).

261. See e.g. Nissenbaum, *supra* note 58; Reiman, *supra* note 72.

hoped that the RTBF will influence Strasbourg, rather than the other way around.

E. Circumstances in Which the Information Was Obtained

In *Lillo-Stenberg v Norway*, the Court emphasised the importance of considering the way in which intrusive photographs were captured, commenting, "the situation would have been different if the photographs had been of events taking place in a closed area, where the subjects had reason to believe that they were unobserved".[262] Thus a claimant's lack of knowledge that photographs may be taken appears to be a factor going to the weight of an Article 8 claim.[263] In the first *Von Hannover* case, the Court observed that one particular, rather undignified, image of the Princess falling over at a private beach club was "taken secretly at a distance of several hundred metres, probably from a neighbouring house, whereas journalists' and photographers' access to the club was strictly regulated".[264] The Court also considered the *frequency* with which photographs were being taken and published, noting that "photos appearing in the tabloid press are often taken in a climate of *continual harassment* which induces in the person concerned a very strong sense of intrusion into their private life or even of persecution".[265]

This factor is easily read across to our "third party scenario", since it is in essence much the same as the large number of cases Strasbourg has considered in which the personal data is initially gathered by a third party (the press) and then disseminated to a mass audience. The fact that the individual had made no disclosure of the data at all would surely add strength to their Article 17 claim. In the "data leak" scenario, where the initial upload was given only restricted access e.g. to Facebook "friends", and the leak to public platforms occurred without notice or consent, it would be easier to draw parallels with the notion of surreptitious

262. *Lillo-Stenberg*, *supra* note 171 at para 39.
263. *Von Hannover*, *supra* note 25 at para 68.
264. *Ibid* at para 68.
265. *Ibid* at para 59 [emphasis added].

gathering, thus strengthening the privacy side of the scales. Here an analogy could be drawn with cases like *Peck* and *Von Hannover*: just as individuals appearing in public places accept that they will be subject to casual observations by passers-by, but do not accept the risk of this being converted, by press coverage into essentially mass-observation, so those uploading pictures to be seen only by "friends" would not anticipate the far greater coverage that would result if the information leaks to publically-available sites.

As noted above, this argument becomes harder where the initial upload was to a publically accessible website: it could then be argued that the data subject should have foreseen subsequent greater publicity, though this might depend on the scale and intrusiveness of that publicity. If the further dissemination was of such a scale or nature as to amount to harassment, parallels could be drawn to the circumstances surrounding photographs captured of Princess Caroline in *Von Hannover v Germany*.[266] Finally there is the scenario in which personal information had been uploaded to an openly accessible website but on an anonymous basis, only for the data subject to be later identified against their wishes. Courts and regulators should take a context-sensitive approach here, recognising the key *expressive* value in being able to "share privately".[267]

F. Does the Personal Data Relate to a Public or Private Location?

Several Strasbourg cases focus upon the physical location in which personal data was obtained in deciding whether it warrants protection under Article 8.[268] A claim to privacy in respect of a photograph taken in a public street is less likely to attract Article 8 protection than if the subject of the picture was in a private dwelling.[269] *Lillo-Stenberg v*

266. *Von Hannover*, *supra* note 25.
267. See *The Author of a Blog v Times Newspapers Ltd*, [2009] EWHC 1358 (QB) for a case that failed to recognize the importance of this value; the notion of "sharing privately" comes from Mills, *supra* note 35.
268. *Von Hannover*, *supra* note 25; *Von Hannover (no 2)*, *supra* note 170; *Peck*, *supra* note 168.
269. See e.g. *Lillo-Stenberg*, *supra* note 171.

Norway concerned photos of a wedding of a celebrity couple who had married outdoors on a publically accessible islet.[270] Strasbourg upheld that Icelandic court's judgment that Article 10 should prevail over the couple's Article 8 claim to bar publication of the photos, partly because it was an outdoor wedding taking place in a public place and holiday destination.[271]

However other cases show a more nuanced approach. In *Pfeifer v Austria*[272] Strasbourg said that Article 8 encompasses "a person's physical and psychological integrity".[273] When attempting to define the scope of the right to privacy in *Niemietz v Germany*,[274] the Court said that "it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude there entirely the outside world",[275] seemingly advocating a flexible reading of what a private zone could encompass.[276] However, the key case here is the seminal *Von Hannover v Germany*[277] in which the Court stressed "there is … a zone of interaction … with others, even in a public context, which may fall within the scope of 'private life'".[278] The German courts had held that photographs taken in a physically public location of someone they considered a public figure *par excellence* must be tolerated; the only exceptions were images showing Princess Caroline with her children or in a "secluded place", such as a quiet corner of a restaurant. Strasbourg disagreed, finding that this "secluded place" test was unacceptably narrow; the images depicting Princess Caroline in a public place deserved protection under Article 8 as they gave viewers an

---

270. *Ibid* at paras 5–8.
271. *Ibid* at paras 39–44.
272. *Pfeifer v Austria*, No 24733/04, [2011] ECHR 328.
273. *Ibid*; Bulak & Zysset, *supra* note 195 at 234.
274. *Niemietz v Germany*, No 13710/88, [1992] 16 EHRR 97.
275. *Ibid* at para 29.
276. This approach potentially conflicts with the majority's viewpoint in *Campbell*, *supra* note 63, that some information is "obviously private", see Moreham, *supra* note 50 at 646.
277. *Von Hannover*, *supra* note 25.
278. *Ibid* at para 50; *Avram*, *supra* note 206 at para 37; Gomery, *supra* note 185 at 409.

insight into her personality and "psychological integrity".[279]

The above jurisprudence has obvious relevance to RTBF claims and, if followed, should result in courts and regulators resisting crude notions that an event taking place in a public or semi-public environment cannot for that reason be considered worthy of privacy protection.[280]

VI. Conclusion

At the time of writing, Article 17 is only a few days old and its proper interpretation and likely impact remain matters of profound uncertainty. This article has attempted, using Strasbourg's privacy case law as its primary guide, to offer some preliminary answers to the most pressing questions surrounding the application of the newly-formulated right to online expression. The answers it has proposed are necessarily tentative: much of the analysis has involved applying case-law developed in response to very different scenarios from the online deletion right in the *GDPR*. But we hope that our analysis has at least shown that the RTBF has profound implications for how we think about online privacy. It may be that in the end Article 17 influences Strasbourg's case-law as much as the other way around. What *is* certain is that far more work — by regulators, courts and scholars — is needed to fully work out what Article 17 will mean and how it will impact the world of online expression. Most importantly, we do not yet know how significant a contribution it will make to its overall

279. Bryce Clayton Newell, "Public Places, Private Lives: Balancing Privacy and Freedom of Expression in the United Kingdom" (Proceedings of the 77th ASIS&T Annual Meeting, vol 51, at 1–10, 2014) at 6, online: Social Science Research Network <https://ssrn.com/abstract=247909>; Roger Toulson, "Freedom of Expression and Privacy" (2007) 41:2 The Law Teacher 139 at 140.

280. Prosser, *supra* note 244 (noting that "[t]he decisions indicate that anything visible in a public place may be recorded and given circulation by means of a photograph, to the same extent as by a written description, since this amounts to nothing more than giving publicity to what is already public and what any one present would be free to see" at 394). For a forensic critique see E. Paton-Simpson, "Private Circles and Public Squares: Invasion of Privacy by the Publication of 'Private Facts'" (1998) 61:3 Modern Law Review 318, especially 321–326.

goal: the enhancement of our informational autonomy online and with it, the greater freedom to make life choices that might be inhibited by the fear of behaviour being recorded in permanent form online recedes.[281] As Mayer-Schönberger puts it:

> Since the beginning of time, for us humans, forgetting has been the norm and remembering the exception. Because of digital technology and global networks, however, this balance has shifted. Today … forgetting has become the exception, and remembering the default.[282]

We are about to find out how far the right to be forgotten can start to shift this balance back.

281. Westin, *supra* note 58 at 56; Francis Chlapowski, "The Constitutional Protection of Informational Privacy" (1991) 71:1 Boston University Law Review 133; Gerstein, *supra* note 214; Tom Gerety, "Redefining Privacy" (1977) 12:2 Harvard Civil Rights – Civil Liberties Law Review 233 at 281; Ruth Gavison, "Too Early for a Requiem? Warren and Brandeis Were Right on Privacy vs. Free Speech" (1992) 43:3 South Carolina Law Review 437.

282. Mayer-Schönberger, *supra* note 40 at 2.