British Institute of International and Comparative Law

THE RIGHT TO BE FORGOTTEN IN DATA PROTECTION LAW AND TWO WESTERN CULTURES OF PRIVACY

UTA KOHL*

Abstract Data protection law has emerged as an important bulwark against online privacy intrusions, and yet its status within privacy law remains awkward. Its starting point of protecting 'personal' rather than 'private' information puts it at odds with privacy more generally. Indeed, in its very design, data protection law caters for the protection of public personal information, or personal information which has attained a degree of publicness through disclosure. Building on James Whitman's comparative privacy study, this article argues that data protection law is not the odd bedfellow of privacy law properly so called but may be understood as a manifestation of the Continental European culture of privacy. Its distinctiveness does not lie in its apparent technicality but in its robust openness to privacy in public—an idea that is alien to the Anglo-American culture of privacy. Whilst these two cultures of privacy have long 'met' in different jurisdictions, this article locates their enduring influence and antagonism within three contemporary privacy regimes. By taking the right to be forgotten, as an archetypal privacy-in-public right, in the testing context of spent criminal convictions, the article gauges the comparative openness to such claims, first, of the Court of Justice of the European Union as the authoritative voice on General Data Protection Regulation normativity; secondly, of the US judiciary as committed to the First and Fourth Amendment; and, thirdly, of the European Court of Human Rights on Article 8 of the European Convention on Human Rights and its fused Anglo-American and Continental European privacy jurisprudence. It is the latter jurisprudence in particular that highlights the tensions arising from trying to marry the two privacy traditions, or merge data protection and 'privacy' law. Yet, these tensions also offer insights and opportunities.

Keywords: human rights, comparative law, privacy, right to be forgotten, European Convention of Human Rights, data protection law, General Data Protection Regulation (GDPR), Fourth Amendment.

* Professor of Law, University of Southampton, Southampton, United Kingdom, U.Kohl@soton.ac.uk. The author would like to thank Andrew Charlesworth and Peter Quirk for helpful comments and suggestions on an earlier draft. This article was written as part of a Leverhulme funded research project on 'Modern Technologies, Privacy Law and the Dead' and is dedicated to the author's friend and colleague, the late Professor Christopher Harding, Aberystwyth University.

[*ICLQ* vol 72, July 2023 pp 737–769] doi:10.1017/S0020589323000258

I. INTRODUCTION

Despite the increasing prominence of data protection law, its status within or outside of privacy law remains contested. Most problematically, data protection law protects 'personal' rather than 'private' information, and so is, from the outset, directed at public personal information, or personal information which has become public to some extent. The argument made in this article is that data protection law is not an awkward off-shoot of privacy law properly so called, but rather a manifestation of the Continental European culture of privacy and reflects its robust openness to privacy-in-public. The discussion takes as its starting point James Whitman's comparative privacy study[1] which situates the heart of American privacy culture in the literal 'inner space' of the home (building on its English common law roots) and the heart of Continental European privacy culture in a metaphorical 'inner space' in public.[2] The latter culture recognises privacy-in-public but the former does not. Although these two cultures share much common ground and have long been intermingled in different jurisdictions, this article shows their enduring difference in three contemporary privacy regimes. Using the right to be forgotten as an example of data protection law and its orientation towards privacy-in-public, it assesses the comparative openness to such claims, first, of the Court of Justice of the European Union (CJEU) as the authoritative voice on data protection law normativity; secondly, of the US judiciary and its commitment to the First and Fourth Amendment, and, thirdly, of the European Court of Human Rights (ECtHR) under Article 8 of the European Convention on Human Rights (ECHR) and its fusion of Anglo-American and Continental European privacy jurisprudence. The Strasbourg jurisprudence in particular highlights the tensions arising from trying to marry these two privacy traditions, or of merging data protection and 'privacy' law. At the same time, these tensions also offer—as encounters with 'foreign' normativity—insights and opportunities.

[1] JQ Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113(6) YaleLJ 1151; for an engagement with Whitman's cultural approach, as opposed to a functional approach to comparative methodology, see Special Issue of AmJCompL (2017) Vol 65; see especially J Gordley, 'Comparison, Law, and Culture: A Response to Pierre Legrand' (2017) 65 AmJCompL 133; P Zumbansen, 'Les Jeux Sont Faits: Comparative Law—As It Really Was Meant to Be?' (2017) 65 AmJCompL 237. See also RC Post, 'Three Concepts of Privacy' (2001) 89 GeoLJ 2087; EJ Eberle, *Dignity and Liberty: Constitutional Visions in Germany and the United States* (Praeger 2001); GE Carmi, 'Dignity Versus Liberty: The Two Western Cultures of Free Speech' (2008) 26 BostonUIntlLJ 277; B Markesinis et al, 'Concerns and Ideas about the Developing English Law of Privacy (and How Knowledge of Foreign Law Might be of Help)' (2004) 52(1) AmJCompL 133.

[2] For reflection on space and privacy, see I Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding* (Brooks/Cole 1975); M Hildebrandt, 'Privacy and Identity' in E Claes, A Duff and S Gurwirth (eds), *Privacy and the Criminal Law* (Intersentia Publishers 2006) 43, 46, where the author comments: 'the concept of space is important for privacy, though not in a naturalistic sense. Space is a crucial source of perceptual information that allows a person to move around and fit into her environment, to interact with it or even to reshape it.' See also J Feinberg, 'Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution' (1983) 58 NotreDameLRev 445.

The wider context for the discussion lies in twenty-first-century socio-technological developments which have enormous potential for intrusion into privacy and which may be categorised into forms of overt and covert information practices. *Overt* information or data practices refer to digital disseminations and disclosures, such as revelations on social media or search results, that can have significant consequences for individuals.[3] As early as 1998 Lasica reflected on the repercussions of personal information being accessible online across time and space: 'Our past now follows us as never before. For centuries, refugees sailed the Atlantic to start new lives; Easterners pulled up stakes and moved west. Today, reinvention and second chances come less easily: You may leave town, but your electronic shadow stays behind.'[4] For Rosen, the web's memory is 'threatening, at an existential level, our ability to control our identities' and is profoundly at odds with the individualism that emerged in the Renaissance and with it the 'new conception of malleable and fluid identity' as expressed 'in the American ideal of the self-made man'.[5]

Since then the argument in favour of a right of information bankruptcy,[6] or giving individuals a second chance, has been answered in the European Union (EU) by the right to be forgotten, first, in the judgment of the CJEU in *Google Spain*[7] and then, explicitly in the right to erasure, or the right to be forgotten, in the General Data Protection Regulation (GDPR).[8] This right allows individuals to 'edit' their online profiles when the internet has not forgotten that which ought to have been forgotten. Like a spent conviction, data is to be considered 'spent' if it is 'inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed'.[9] In the US, however, this right has not been legally recognised, as from a US perspective it is not for the State to facilitate such reinvention (as discussed below).

These approaches are reversed when it comes to *covert* information practices, or the ubiquitous and surreptitious collection, aggregation and analysis of personal data, including governmental surveillance. Here it is the EU that is

[3] H Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2009) 11, where the author maps privacy against information technologies by distinguishing between the technological capacities of (1) tracking and monitoring, (2) aggregation and analysis, and (3) dissemination and publication.

[4] JD Lasica, 'The Net Never Forgets' (*Salon*, 26 November 1998) <https://www.salon.com/1998/11/25/feature_253/>.

[5] J Rosen, 'The Web Means the End of Forgetting' *The New York Times* (New York, 21 July 2010); J Rosen, 'The Purposes of Privacy: A Response' (2001) 89 GeoLJ 2117.

[6] VM Schönberger, *Delete: the Virtues of Forgetting in the Digital Age* (Princeton University Press 2009) 99–100.

[7] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* EU:C:2014:317 (*Google Spain*).

[8] 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 L119/1, art 17.

[9] *Google Spain* (n 7) para 93.

https://doi.org/10.1017/S0020589323000258 Published online by Cambridge University Press

moving towards creating governmental backdoors into encrypted data,[10] as shown by its relatively permissive stance towards bulk surveillance. In *Big Brother Watch v UK*[11] which concerned the legality of the US National Security Agency (NSA) and UK Government Communications Headquarters' (GCHQ) surveillance programmes as revealed by Edward Snowden, the ECtHR held that bulk interception is not per se illegal—thus dispensing with the requirement of 'reasonable suspicion' for targeted interception—as long as it is justified by the need to protect against security threats and is accompanied by end-to-end safeguards against abuses of power.[12] It took a dissenting judge to make the point that the shift 'from targeting a suspect who can be identified to treating everyone as a potential suspect, whose data must be stored, analysed and profiled … is more akin to a police state than to a democratic society'.[13]

Similarly, in *La Quadrature du Net and Other*[14] and *Privacy International*[15] the CJEU held that although 'general and indiscriminate'—or bulk—retention or transmission of personal data is unlawful under the EU Charter of Fundamental Rights,[16] bulk data retention may be justified to prevent 'activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities'.[17] These cases appear to close the door to indiscriminate State surveillance, yet in fact they leave it slightly ajar.

Meanwhile, the US responded to the Snowden revelations with the rather more pro-active and decisive step of the US Freedom Act 2015[18] that ended the governmental bulk surveillance programme of domestic telecommunications metadata and implicitly attests to quite how profoundly State surveillance jars with the American ideal of individual liberty.[19]

[10] European Council, 'Council Resolution on Encryption – Security through Encryption and Security Despite Encryption' (24 November 2020) 13084/1/20.

[11] *Big Brother Watch and Others v United Kingdom* App No 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021); in contrast to earlier authority that insisted on targeted surveillance based on 'reasonable suspicion', eg *Weber and Saravia v Germany* App No 54934/00 (ECtHR, 29 June 2006); *Liberty and Others v United Kingdom* App No 58243/00 (ECtHR, 1 July 2008); *Kennedy v United Kingdom* App No 26839/05 (ECtHR, 18 May 2010).

[12] *Big Brother Watch* ibid, paras 348–350 (majority judgment).

[13] *Big Brother Watch* ibid, para 22 (partly dissenting judgment by Pinto de Albuquerque).

[14] Joined Cases C-511/18 and C-512/18 *La Quadrature du Net and Other v France* EU:C:2020:791.

[15] Case C-623/17 *Privacy International v United Kingdom* EU:C:2020:790.

[16] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 7 (privacy), art 8 (data protection), art 11 (freedom of expression).

[17] *La Quadrature du Net and Other* (n 14) paras 134–139, especially para 135; contrast to Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson and Others* EU:C:2016:970.

[18] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act [2015]; see also *United States v Moalin*, No 13-505732 (9th Cir 2020).

[19] D Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 SDLRev 745, 768 (discussing the structural shifts and power imbalances that occur as a result of surveillance).

The distinction between overt and covert information practices and resultant privacy threats, and the differences in the EU and US responses to them, roughly map onto the two Western cultures of privacy as set out in Whitman's comparative study. Yet, in so far as the EU and US responses affirm the continued presence of these cultures, they also contain the seeds for questioning their standing as insular responses to privacy threats that are transnational in nature and the validity of their underlying assumptions. As demonstrated in the discussion in the second half of the article on the right to be forgotten, the traditional legal cultures of privacy have, for quite some time, been challenged, reconfigured and even been displaced in response to changing informational demands, as well as economic or political changes.

II. TWO PRIVACY CULTURES AND THE 'INNER SPACE'

There is a rich and complex jurisprudence on the concept of privacy, grappling both with the great variety of privacy interests and claims (for example, reproductive decisions, sexual orientation, surveillance, pollution, gun ownership, data protection, corporal punishment, search and seizure, to mention just a few[20]) and stark differences in cultural sensitivities about what is or is not 'private' and thus what ought to be protected.[21] This article builds on Whitman's framing of privacy around two dominant cultures which have emerged from divergent preoccupations in Western legal thought and which are located within 'much larger and much older differences in social and political traditions': one centres around *liberty* and the other around *dignity*.[22] The value of liberty is key to understanding the American privacy culture, whilst dignity underlies the Continental European one. These two values help explain the comparative differences as well as congruencies and overlaps between the two privacy traditions.[23] Even in their differences, both traditions seek to establish a literal or metaphorical inner space for self-authorship or self-sovereignty.

A. The Anglo-American Literal 'Inner Space'

Whilst Whitman speaks of an American culture of privacy as being preoccupied with the home as the site of protection, the inviolability of the home as a place of

[20] Council of Europe, 'Guide on Article 8 of the European Convention on Human Rights' (31 August 2022) <https://www.echr.coe.int/documents/guide_art_8_eng.pdf>.

[21] F Schoeman, 'Privacy: Philosophical Dimensions' (1984) 21(3) AmPhilQ 199.

[22] Whitman (n 1) 1160; see also Post (n 1) and Eberle (n 1), whose comparative analysis based on dignity and liberty preceded Whitman.

[23] For an empirical overview of the histories of privacy recognition of EU Member States, see D Erdos, 'Comparing Constitutional Privacy and Data Protection Rights within the EU' (2022) 47 ELR 482.

https://doi.org/10.1017/S0020589323000258 Published online by Cambridge University Press

security and liberty has a far longer common law history in England—a sentiment which would have chimed with early American settlers. So, the discussion here refers to the Anglo-American culture of privacy which goes as far back as *Semayne's Case* (1604)[24] which dealt with the power of the Sheriff to enter a house at the suit of a common person,[25] and in which Edward Coke captured the idea of the inviolate home:

> That the house of every one is to him (a) as his castle and fortress as well for his defence against injury and violence, as for his repose … [E]very one may assemble his friends and neighbours (d) to defend his house against violence: but he cannot assemble them to go with him to the market, (e) or elsewhere for his safeguard against violence: and the reason of all this is, because *domus sua cuique est tutissimum refugium* [everyone's house is his safest refuge].[26]

'My home is my castle' encapsulates the traditional common law understanding of privacy, even if not under that label.[27] In the home one has a right to be free from outside interferences, clearly articulated in terms of privacy in the US case of *Katz v US*: 'a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited'.[28]

The home may be understood as an extension of the body, its armour or protective shell, which has constituted another core sphere of inviolability.[29] These intermeshed spheres of inviolability or non-interference have long been recognised and protected through civil causes of actions, such as trespass to land and trespass to the person, which are actionable per se, as the interference is itself the injury. In addition, traditional common law has also long protected secrets through breach of confidence actions, and these can be

[24] *Semayne's Case* (1604) 5 Co Rep 91a, 77 ER 194.

[25] See *Wilson v Arkansas* 514 U.S. 927, 932 (1995): 'This "knock and announce" principle appears to predate even Semayne's Case … [which] itself indicates that the doctrine may be traced to a statute in 1295, and that at that time the statute was "but an affirmance of the common law."'

[26] *Semayne's Case* (n 24) 195.

[27] *Semayne's Case* has been linked to Article 8 of the ECHR in, eg, *Bempoa, R (on the application of) v London Borough of Southwark* [2002] EWHC 153, para 13. See Erdos (n 23) where the author shows that the protection of the home is also long standing in many Continental European jurisdictions.

[28] *Katz v United States* 389 U.S. 347, 361 (1967).

[29] W Blackstone, *Commentaries on the Laws of England: A Facsimile of the First Edition of 1765–1769* (University of Chicago Press 1979) vol 5, amendment IV, document 8: 'For every man's house is looked upon by the law to be his castle of defence and asylum, wherein he should suffer no violence'; *R v Meade and Belt* (1823) 1 Lew CC 184: 'the making of an attack upon the dwelling, and especially at night, the law requires as equivalent to an assault on a man's person; for a man's house is his castle, and therefore, in the eye of the law, it is equivalent to an assault …' For paradigmatic US cases on the body as a private sphere, see *Griswold v Connecticut* 381 U.S. 479 (1965) (recognises an implicit right to privacy in the US constitution, and includes the use of contraception) and *Roe v Wade* 410 U.S. 113 (1973) (the right to abortion) now overruled by *Dobbs v Jackson Women's Health Organization* No. 19-1392, 597 U.S. (2022).

personal or trade secrets. Where such claims concern personal information, they again generally concern a person's home or body.[30]

The idea of a person's seclusion from society within their home also lies at the heart of various theories seeking to explain privacy, such as those centred on the 'intimate sphere'[31] or the right to be left alone.[32] By extension, claims to privacy in public places, such as having one's photograph taken by a stranger in a public street, are not easily accommodated within this common law view of privacy.[33] Feinberg observed: 'My personal space, however, diminishes to the vanishing point when I enter the public world. I cannot complain that my rights are violated by the hurly burly, noise, and confusion of the busy public streets; I can always retrace my steps if the tumultuous crowds are too much for me.'[34] Such a retreat is, of course, to the home.

Whilst pursuant to *Semayne's Case* 'the liberty or privilege of a house doth not hold against the King',[35] William Pitt, the Earl of Chatham, famously reasserted the maxim in 1763, albeit in rather different terms:

> The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter—the rain may enter—but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement.[36]

It is this idea that the main threat to privacy comes from the State whose powers are presumptively restricted to the public realm, that is the realm outside the home, that has resonated most strongly in America. Although privacy as such is not explicitly recognised in the American Bill of Rights, it has emerged from an array of constitutional guarantees, all of which are directed against State exercises of power. The most important of these is the freedom from unlawful search and seizure, found in the Fourth Amendment: 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated …'.

Whitman argued that 'in forbidding the government to seize the documents of a merchant in a customs case, the Supreme Court [in *Boyd v US*[37]] … issued an

[30] G Phillipson, 'Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act' (2003) 66(5) ModLRev 726, 733.

[31] R Wacks, 'The Poverty of Privacy' (1980) 96 LQR 73; JC Innes, *Privacy, Intimacy, and Isolation* (OUP 1992).

[32] SD Warren and LD Brandeis, 'The Right to Privacy' (1890) 4 HarvLRev193.

[33] This traditional position changed in a number of common law jurisdictions, including England and Wales in *Campbell v MGN Ltd* [2004] UKHL 22; and Canada in *Les Editions Vice Versa Inc v Aubry* [1998] 5 BHRC 437.

[34] Feinberg (n 2) 454; see also: 'Where one has one's domicile, however, and where one owns land, there one has space that is entirely one's own, where uninvited intruders (with certain necessary and well understood exceptions) may not enter.'

[35] *Semayne's Case* (n 24) 197.

[36] In H Brougham, *Historical Sketches of Statesmen who Flourished in the Time of George III* (First Series, G. Cox 1845) vol 1, quoted, for example, in *Southam v Smout* [1964] 1 QB 308, 320. This extension of the prohibition to the King has, of course, been subject to exceptions, as provided by law, eg search warrants.

[37] *Boyd v United States* 116 U.S. 616 (1886).

aggressive declaration of the "sanctity" of an American home'[38] and thus that 'the standard history of modern American privacy rights should really begin, not with Warren and Brandeis's distant and dim echo of Continental ideas, but with *Boyd v United States*, four years earlier'.[39] The anti-State focus of American privacy is deeply inscribed with the settler mentality of self-reliance, self-rule and distrust of government. In this citizens-versus-government conception of privacy, governments cannot be trusted to not interfere unduly with individuals and thus their power must be curtailed. Privacy as liberty thus consists of liberty *from* government to emphasise the liberty *to* govern oneself, or self-sovereignty, with the home as the archetypal place where a person is their own master.

B. The Continental European Metaphorical 'Inner Space'

In the Continental European culture of privacy, privacy does not attach to the home as the sacred space but is—as part and parcel of wider personality protection—preoccupied with one's public image as the foundation for self-authorship.[40] This view of privacy is at least as concerned with one's treatment within society as it is with one's entitlement to withdraw from society. It is not about seclusion per se but rather about controlling one's image in the public realm. Recognising the social context of individual flourishing, this conception of privacy sets boundaries to an individual's treatment in the public domain where such treatment fulfils 'no reasonable social purpose and serves only to provoke a scandal and personal humiliation …'.[41] Here privacy is functionally delimited through the *personal* nature of the information.[42]

Continental privacy is thus understood in terms of informational self-determination,[43] and protects a metaphorical 'inner space' against unwanted exposure. This conception of privacy guards against the threat of public

[38] Whitman (n 1) 1212.

[39] ibid 1212–3.

[40] ibid 1161, 1189–95; see also J Kohler, *Das Eigenbild im Recht* (J Guttentag 1903); Warren and Brandeis (n 32).

[41] Kohler ibid 10 (translation by author).

[42] Typically, see Article 2(1) of the German Basic Law on the right to free development of one's personality, which includes as part of the right to personal dignity (art 1(1)) the right to control the use of one's image or words, eg in a news story. W Kahl, *Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz* (Mohr Siebeck 2000) 8. See also *Tonband/Recording* (German Constitutional Court, 31 January 1973) 2 BvR 454/71, BVerfGE 34, 238.

[43] Recognised in the *Census Case* (German Constitutional Court, 15 December 1983) BVerfGE 65 in the context of creating protection against the 'transparent citizen' and providing a theoretical foundation for data protection law; see G Hornung and C Schnabel, 'Data Protection in Germany I: the Population Census Decision and the Right to Informational Self-Determination' (2009) 25(1) CLSRev 84. For common law privacy theorists who define privacy as informational self-determination, control or autonomy, see AF Westin, *Privacy and Freedom* (Atheneum 1967); C Fried, 'Privacy' (1968) 77 YaleLJ 475, 482; Phillipson (n 30) 732 P Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP 2014). More generally, on different theories: Schoeman (n 21); Nissenbaum (n 3) 69ff; H Fenwick and G Phillipson, *Media Freedom under the Human Rights Act* (OUP 2006) 662ff.

in-dignities. In other words, dignity in public is the core value that underlies the Continental European culture of privacy. Its historical background lies in the strict hierarchical nature of European societies, where public humiliation was used as a tool of disempowerment. In *The Politics of Humiliation: A Modern History*,[44] the historian Ute Frevert shows how a gradual shift from humiliation to dignity occurred in Europe from the early nineteenth century:

> [A]s lower-class people increasingly objected to disrespectful treatment … [they] used the language of honour and concepts of personal and social self-worth—previously monopolised by the nobility and upper-middle classes—to demand that they not be verbally and physically insulted by employers and overseers. This social change was enabled and supported by a new type of honour that followed the invention of 'citizens' (rather than subjects) in democratising societies. Citizens who carried political rights and duties were also seen as possessing civic honour. Traditionally, social honour had been stratified according to status and rank, but now civic honour pertained to each and every citizen, and this helped to raise their self-esteem and self-consciousness.[45]

Against this social background, hate speech and anti-discrimination law can also be understood as legal regimes that intervene in practices of public humiliation.[46] Equally, the right to privacy—based on the Roman delict of *injuria*, concerned with a person's 'fame, reputation and honour'[47] and directed against insult—is inscribed with the idea of levelling up, or democratisation of dignity, by giving everyone some control over their public image. In Whitman's words:

> Germany and France have been the theater of a *levelling up*, of an extension of historically high-status norms throughout the population. As the French sociologist Philippe d'Iribame has elegantly put it, the promise of modern Continental society is the promise that, where there were once masters and slaves, now 'you shall all be masters!'[48]

While privacy as liberty supports the home as the space for one's own mastery, in Continental Europe being master of one's life demanded, first and foremost, equal respect and dignity in the public realm—or in Lord Hoffman's words: 'Meddling with such matters [personal information] is metaphorically an invasion of my territory, a violation of the castle of my *personhood*.'[49] This contextualises why, for example, human dignity is the overarching value of the German Constitution (Art 1(1)) followed by 'the right to free

[44] U Frevert, *The Politics of Humiliation: A Modern History* (OUP 2020).

[45] U Frevert, 'The History of Humiliation Points to the Future of Human Dignity' (*Psyche*, 20 January 2021) <https://psyche.co/ideas/the-history-of-humiliation-points-to-the-future-of-human-dignity>.

[46] Whitman (n 1) 1164–5.

[47] NR Whitty, 'Overview of Rights of Personality in Scots Law' in NR Whitty and R Zimmermann (eds), *Rights of Personality in Scots Law: A Comparative Perspective* (Edinburgh University Press 2009).

[48] Whitman (n 1) 1166 (emphasis in original).

[49] Lord Hoffman, 'Mind Your Own Business' (Goodman Lecture, 22 May 1996, unpublished) cited in Fenwick and Phillipson (n 43) 663 (emphasis added).

https://doi.org/10.1017/S0020589323000258 Published online by Cambridge University Press

development of one's personality' (Art 2(1)) from which privacy rights are derived. Given the preoccupation with one's dignified standing in public, the media is often the target against whom privacy is asserted.[50] However, the underlying threat which this conception addresses lies in social hierarchies and their formal and informal maintenance through public humiliation.[51] In its design, privacy as dignity challenges the elite's prerogative to honour and dignity.

Reflecting on the essential differences between the two approaches, Robert Post argued that:

> [the] concept of privacy as freedom is an almost exact inversion of the concept of privacy as dignity. Privacy as freedom presupposes difference, rather than mutuality. It contemplates a space in which social norms are suspended, rather than enforced. It imagines persons as autonomous and self-defining, rather than as socially embedded and tied together through common socialization into shared norms.[52]

Post's analysis is persuasive in so far as privacy as dignity is focused on mutuality or sameness through an entitlement to equal respect in the social realm, but it is misleading in suggesting that this view does not imagine persons as autonomous and self-defining and 'seeks to eliminate differences by bringing all persons within the bounds of a single normalized community'.[53] The theoretical starting point for privacy as dignity is the Kantian idea of human personhood whose inalienable hallmark is free will,[54] that is the 'unpredictably individual, creatures whom no science of mechanics or biology could ever capture in their full richness'.[55] So privacy as dignity flows from personal autonomy as a higher-order concept.[56]

Privacy as dignity also recognises that personal autonomy as a lower-order concept may, as a matter of one's lived experience, be infringed, circumscribed or taken away in its entirety within social hierarchies that deny equal respect to all participants. Slaves or others in lesser forms of servitude have very limited autonomy. This aspect was undoubtedly less pressing to American settlers whose common immigration background acted as a powerful equaliser, even if the myth of equality could only stand with the significant blind spots of Native Americans and African slaves.[57]

[50] Whitman (n 1) 1161. [51] Frevert (n 45). [52] Post (n 1) 2095. [53] ibid 2095.

[54] Whitman (n 1) 1182; see also Whitty (n 47) 159f, arguing that there is a distinction between 'the traditional idea of dignity, its core being honour, respectability and status from the enlightenment idea of human dignity conceived of as personal autonomy …' (internal marks omitted). See I Kant, *Groundwork of the Metaphysics of Morals* (1785, M Gregor and J Timmermann trans and eds, CUP 1998, revised 2012) 57: 'thus a free will and a will under moral laws are one and the same'. [55] Whitman (n 1) 1181 (emphasis omitted).

[56] Whitty (n 47) 161, referring to the different levels at which 'dignity' can be defined.

[57] The value of dignity has exceptionally surfaced in the American jurisprudence in the practice of 'perp walks', see eg *Lauro v Charles* 219 F.3d 202 (2d Cir. 2000) where it was held that public

As a matter of substance, the Continental European idea of privacy set out to recognise everyone's basic entitlement to dignity in order to equalise life opportunities and public participation.[58] As a matter of process, privacy as dignity gives individuals the autonomy to decide what is and what is not an affront to their dignity in a dynamic, evolving way. Individuals can control the flow of their personal information and are free to withdraw their consent to the dissemination of such information, even where they initially consented, including through contract.[59] Personal autonomy cannot be abandoned or relinquished. Thus, Continental European privacy is also deeply concerned with self-authorship or, in Post's words, with the expression of the 'spontaneous, independent, and uniquely individual aspect of the self',[60] but asserts that this is only possible where there is equality of dignity in the public realm.

One can contrast and align the two conceptions of privacy on multiple levels. Both are broadly concerned with self-authorship but localise its flourishing in different realms, against the peculiar social and political traditions and background conditions in which they emerged and to which they responded. The Anglo-American version carves out the body, the home, and implicitly the family, as the space for self-sovereignty; meanwhile Continental European privacy fixes its attention on the public realm as the arena for personal self-determination under conditions of respect and dignity.[61]

The conceptions make a natural fit with the jurisprudential tradition of each jurisdiction: privacy as liberty focused on a physical space is rooted in the empiricism, materialism and pragmatism of Anglo-American jurisprudence, whilst privacy as dignity and its preoccupation with a person's public image based on inalienable personhood reflects the idealism and rationalism of European thought. Furthermore, privacy as dignity understands the 'public' against which protection is sought as the social realm, in contrast to privacy as liberty where 'public' refers above all to governmental activities.

Still, even in their divergences, these two conceptions are united in their overall objective of protecting self-authorship and self-sovereignty,[62] which shines strongly through the Continental European privacy culture. Meanwhile

arrests (or '"a ritual degradation that publicly signals [the arrestee's] change in status from an ordinary citizen."' (204)) staged only for the press violated the accused's Fourth Amendment rights.

[58] See, for example, accounts that ground the right to informational self-determination 'in the interest of the public, to guarantee a free and democratic communication order'. Hornung and Schnabel (n 43) 86; or accounts of privacy and freedom of expression being mutually supportive, eg Fenwick and Phillipson (n 43) 686.

[59] Whitman (n 1) 1176.

[60] Post (n 1) 2095.

[61] There is a complementarity in that the American emphasis on seclusion and being hidden stresses the autobiographical dimension of personal identity, whilst the Continental European emphasis on personal oversight of one's standing in public is concerned with the biographical or social dimension of identity. See literature on the related topic of identity, or the right to identity, eg Hildebrandt (n 2); S Gutwirth, 'Beyond Identity?' (2008) 1 IDIS 123; P De Hert, *A Right to Identity to Face the Internet of Things* (Council of Europe Publishing 2007).

[62] Whitman (n 1) 1163.

in the Anglo-American privacy tradition, being the master in one's home is synonymous with self-determination,[63] and implicitly with self-authorship, although never put in such 'vague and grandiose' ways as in Continental European jurisprudence.[64] The 'inner space' of the person protected by German-style privacy law is the literal 'inner space' of the American and English home.

III. CONTEMPORARY PRIVACY REGIMES AND THE RIGHT TO BE FORGOTTEN

Whilst Anglo-American privacy limits protection to the private sphere and personal confidential information, in Continental European culture privacy is neither confined to intimate or personal confidential information nor necessarily limited to an a priori private sphere.[65] This is quintessentially the approach adopted in data protection law, which is 'a privacy law all but in name',[66] and which does not deny protection merely because the information is public. Indeed, data protection law is based on the assumption that there has been a disclosure of personal information and gives individuals a degree of control to oversee and manage that disclosure: 'there would be no need for data protection if there was a general prohibition of information disclosure'.[67]

Consistently, Fuster and Gutwirth have argued that the shift from privacy to data protection is one from 'secrecy' to 'control'.[68] Data protection law delivers informational self-determination[69] against an understanding that much personal information is necessarily in the public domain, or has been disclosed to public and private institutions, but protection should not be foregone simply because of that disclosure. Notably, the Council of Europe developed data protection law in the early 1980s in response to the increasing collection of personal data by a wide array of private bodies, against the perceived narrowness of Article 8 of the ECHR[70]—which, as discussed below, draws heavily on the Anglo-

[63] Feinberg (n 2) 483ff, commenting on the judicial interpretation of the US Bill of Rights in *Griswold v Connecticut* (n 29) speaking of 'zones of privacy' which denote zones of individual discretion.

[64] Whitman (n 1) 1182.

[65] Note, however, that the balancing of the conflicting rights is, in German jurisprudence, structured along a privacy-ascending, speech-descending order of five spheres: the public, social, private, confidential and intimate spheres which reflect a private–public spectrum, rather than a simple binary: Markesinis et al (n 1) 188ff.

[66] E Barendt, '"A Reasonable Expectation of Privacy": a Coherent or Redundant Concept?' in AT Kenyon (ed), *Comparative Defamation and Privacy Law* (CUP 2016) 96, 111.

[67] Case C-369/98 *The Queen v Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher* EU:C:2000:79 (Opinion of AG Alber) para 41.

[68] GG Fuster and S Gutwirth, 'Opening up Personal Data Protection: A Conceptual Controversy' (2013) 29 CLSRev 531.

[69] *Census Case* (n 43); see further D Korff and M Georges, 'The Origins and Meaning of Data Protection' (SSRN, 13 January 2020).

[70] P De Hert and S Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action' in S Gutwirth et al (eds), *Reinventing Data Protection?* (Springer 2009) 3, 5f, commenting on the Council of Europe's adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No 108) (28 January 1981)

American culture of privacy. Thus, although data protection law is framed in seemingly technical concepts and language (eg 'data' instead of 'information'; 'data subject' or 'data controller'; purpose limitation, or data minimisation) and presents as a form of data management, it is clearly an expanded version of privacy.

With its focus on 'personal' rather than 'private' information, data protection law largely bypasses controversies based on the private–public binary,[71] and showcases its capacity to recognise layers or degrees of publicness of personal information. Rights attach to information because it is personal, ie related to a person, not because it is 'private' in the sense of being both personal and confidential.[72] Even personal data that is necessarily in the public domain, such as one's name or image, is prima facie protected.[73] Whilst heightened protection is given to 'sensitive personal data',[74] again such information is often not intimate or confidential at all:

> … 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 data concerning a natural person's sex life or sexual orientation shall be prohibited.[75]

Personal information concerning ethnic origin, political opinions or religious beliefs is generally public, and classifying it as 'sensitive' resonates with the Continental European focus on the levelling up of dignity. That some of the sensitive data grounds are also prominent categories in anti-discrimination law does not so much show that data protection law protects privacy and equality, but rather the strong egalitarian overtones of privacy in public as reflected in data protection law.[76] Privacy gives individuals the power to shield themselves from public indignities which generally affect minorities

in response to the perceived limitations of Article 8 (the definition of 'private life' and the vertical nature of the protection) in the early 1970s.

[71] The GDPR also to private and public actors consistent with the Continental European culture of privacy; it requires a balancing of the 'privacy' interests and the public interests in, for example, public health, national security and law enforcement.

[72] Contrast to English law, eg *Douglas & Ors v Hello! Ltd & Ors* [2007] UKHL 21, para 83 (relying on *Coco v A. N. Clark (Engineers) Ltd* [1969] RPC 41): 'for the adjective "confidential" one can substitute the word "private". What is the nature of "private information?" It seems to us that it must include information that is personal to the person who possesses it and that he does not intend shall be imparted to the general public.' This is consistent with the traditional approach under Article 8 (discussed below) and was also endorsed by the CJEU, eg in *Joined Cases* C-465/00, C-138/01 and C-139/01 EU:C:2003:294, paras 74–75. See also Markesinis et al (n 1) 162ff.

[73] Note that some types of sensitive personal data under the GDPR would be confidential data, eg 'data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited'.

[74] GDPR (n 8) art 9, formerly Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Data Protection Directive) art 8.

[75] GDPR (n 8) art 9(1).

[76] Cf De Hert and Gutwirth (n 70) 6, 10.

https://doi.org/10.1017/S0020589323000258 Published online by Cambridge University Press

more significantly. The exposure of one's name, image or words in public creates the potential for humiliation and so is to be controlled by its 'owner'; and just because personal information has legitimately entered the public realm for one purpose does not mean that it can be freely used by others, and forever.[77]

A. The CJEU on the Right to be Forgotten within the GDPR

An archetypal data protection right that perfectly captures its privacy-in-public orientation is the right to be forgotten. Reflective of the Continental European culture of privacy, it allows individuals, in certain circumstances, to withdraw personal data which is already in the public domain, and thereby to manage their public image in the broad sense. The right to be forgotten also expresses the *Zeitgeist* of that tradition by responding to a socio-technical environment that amplifies the public visibility of personal information, and thus its harm potential. The CJEU first 'found' the right in *Google Spain*[78] based on the right to object to the processing of personal data in conjunction with the right to rectification, erasure or blocking of such data under the Data Protection Directive.[79] Now it is a fully fledged right in Article 17 of the GDPR.

In *Google Spain* the information about Mr González's bankruptcy and repossession proceedings a decade earlier, which could be found through a Google search, had already been in the public domain through the Spanish newspaper's publicly accessible archive. Yet, the visibility of that archive was significantly heightened and prolonged through the search engine: 'it is undisputed that that activity of search engines plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name …'.[80] The Court thus recognised degrees of publicness of personal information. The legitimacy of the publication in the newspaper and its online archive did not prevent a claim in respect of the enlarged subsequent audience generated by the search engine.[81]

Since the judgment Google has received more than 1.1 million delisting requests.[82] Most relate to private individuals seeking to shield themselves from continued unwanted public exposure based on 'innocent' information concerning, for example, family or work matters,[83] that entered the public

[77] The 'purpose limitation principle'—see GDPR (n 8) art 5(1)(b); as 'purpose limitation' is a central concept in data protection law, it appears with high frequency in the Regulation.

[78] *Google Spain* (n 7).

[79] Data Protection Directive (n 74) arts 14, 12(b).

[80] *Google Spain* (n 7) para 36.

[81] ibid, paras 85–87.

[82] Google, *Google's Transparency Report* <https://transparencyreport.google.com/eu-privacy/overview?hl=en_GB>; for a brief account of the factors taken into account by Google, see *NT1 & NT2 v Google LLC (The Information Commissioner intervening)* [2018] EWHC 799 (QB) para 131.

[83] S Tippmann and J Powles, 'Google Accidentally Reveals Data on "Right to be Forgotten" Requests' *The Guardian* (London, 14 July 2015): 'These include a woman whose name appeared in prominent news articles after her husband died, another seeking removal of her address, and an individual who contracted HIV a decade ago.'

domain and remained there. In these 'ordinary' claims the right to be forgotten does its core work. A small number of requests, however, involve public figures or perpetrators of 'historic' crimes who want to have their public record cleansed, and it is here that unwanted public exposure encounters the potentially strong competing public interest in having access to the information, as protected by the right to freedom of expression. These rare cases crystalise the tensions underlying the right to be forgotten, and how these tensions are resolved differently by the two conceptions of privacy.

They highlight that self-authorship generally is a social affair, in which the public self is an important counterpart to the private self. Individuals define themselves against others, and reflexively respond to other's perceptions of themselves.[84] Yet one's ability or entitlement to insist on how one is viewed by others is necessarily limited given that others also have, individually and collectively, a legitimate interest in information about members of their community, particularly public figures or those who have become publicly known due to their wrongdoing. There is room for reasonable disagreement on when the demands of self-authorship should trump the public interest in knowing about the behaviour of critical members of the community, and whether this should go beyond the protection from damaging false information, as provided for by defamation law.

These rare cases also make clear that personal responsibility entails taking responsibility for one's past actions and decisions: 'It would be evading responsibility for what one is doing to permit one to say that the later self is not the same self as the earlier self…'.[85] So whilst personal autonomy, which underlies, and is protected by, privacy, assumes fluid personhood capable of change and reinvention, personal autonomy equally entails personal responsibility, which includes taking responsibility for one's past. As a result, wiping the slate clean cannot but be exceptional.

Again, there is room for reasonable disagreement on when the State should intervene to give an individual a second chance. Common law jurisdictions recognise 'forgetting' concepts, such as bankruptcy or the idea of spent criminal convictions,[86] according to which certain past actions are treated as

[84] The social aspect of privacy has been acknowledged, eg in *Botta v Italy* App No 21439/93 (ECtHR, 24 February 1998) para 32, referring to 'the development, without outside interference, of the personality of each individual in his relations with other human beings'.

[85] JC Buitelaar, 'Post-Mortem Privacy and Information Self-Determination' (2017) 19 Ethics Inf Technol 129, 137; see also Feinberg (n 2) 478; D Parfit, 'Later selves and moral principles' in A Montefiore (ed), *Philosophy and Personal Relations: A French Study* (Routledge & Kegan Paul 1973) 137ff.

[86] See, for example, the UK Rehabilitation of Offenders Act 1974. Note, in the UK the effect of rehabilitation in terms of the right to be forgotten is limited, partly, by virtue of the fact that not all offences fall within the remit of the Act and, partly, by virtue of the judicial authority to the effect that a conviction being spent does not necessarily coincide with a privacy entitlement, but is merely a factor which goes towards it: *Gaughran v Chief Constable for the Police Service of Northern Ireland* [2015] UKSC 29; see also *dicta* in *R (T) v Chief Constable of Greater Manchester Police* [2014] UKSC 35, para 18: 'the point at which a conviction … recedes into the past and becomes part of a

having been sufficiently paid for and the community now has an interest in reintegrating the 'wrongdoer'. Yet the GDPR's right to be forgotten takes 'rehabilitation' a step further by prima facie extending it to unwanted public exposure.[87]

An authoritative interpretation of the right to be forgotten through the CJEU—well versed in the idea of privacy-in-public even in testing contexts—can be found in *GC and Others v CNIL and Google*[88] (*GC and Ors*). Here the CJEU was asked whether and how search engines could handle 'sensitive personal data' given the heightened compliance requirements under data protection law.[89] The case concerned four separate de-referencing requests:

- a satirical photomontage on YouTube of a former local political figure which revealed the existence of an intimate personal relationship with another political figure;
- historic news articles concerning the suicide of a member of the Church of Scientology and the data subject's previous role as a public relations' officer in that church;
- dated news stories concerning a judicial investigation into the funding of a political party, with no follow-up news article to indicate that the proceedings against the data subject had since been closed; and
- a data subject's criminal conviction for sexually assaulting children under the age of 15 years.[90]

For the comparative purposes of this article, the CJEU's interpretation of the right to be forgotten illustrates the nature and strength of the Continental European privacy tradition in challenging circumstances in a number of respects. First, the Court reiterated its previous holding in *Google Spain* that an individual's right to be forgotten overrides 'as a general rule' the public's interest in accessing information as an aspect of freedom of expression,[91] even if in the specific case:

person's private life will usually be the point at which it becomes spent under the 1974 Act. It is a neat and logical suggestion which this court should adopt.'

[87] For similar earlier domestic provisions, see *Segerstedt-Wiberg and Others v Sweden* App No 62332/00 (ECtHR, 6 June 2006) and *Österreichischer Rundfunk v Austria* App No 35841/02 (ECtHR, 7 December 2006).

[88] Case C-136/17 *GC, AF, BH, and ED v Commission Nationale de l'Informatique et des Libertes (CNIL), Premier ministre, and Google LLC* EU:C:2019:773 (*GC and Ors*). But see O Lynskey, 'Deconstructing Data Protection: The "Added Value" of a Right to Data Protection in the EU Legal Order' (2014) 63 ICLQ 567 (where the author documents instances where the CJEU has conflated data protection and privacy).

[89] GDPR (n 8) art 9, which prohibits processing unless one of the exceptions, such as express consent, is satisfied.

[90] *GC and Ors* (n 88) paras 25–28.

[91] ibid, paras 53, 66; *Google Spain* (n 7) paras 81, 97. See also S Kulk and F Borgesius, 'Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe' in E Selinger, J Polonetsky and O Tene (eds), *The Cambridge Handbook of Consumer Privacy* (CUP 2018) 301, noting its inconsistency with the approach of equal status taken by the ECtHR.

> [the balance may] depend on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.[92]

As the right to be forgotten is designed to operate in the public realm and act as a restraint on public communications, it routinely clashes with the demands of freedom of expression. Thus, if it would not 'as a general rule' override freedom of expression, it would not, as a rule, discharge its function. The CJEU was, however, not insensitive to the public's interest in being able to access the relevant information, as underscored by the right's focused remedy of shielding individuals only from the results of searches of their names, and by otherwise leaving the personal information in the public domain, and also as explicitly secured by the right's public interest exception.[93]

Secondly, in the controversies in *GC and Ors*, the personal matters in question had, with one exception, already and legitimately been in the public domain. By the same token, Google's privacy duties arose because as a search provider it was directly responsible for bringing the information to a new public. Its liability was thus not secondary, or depending on the wrongdoing by the original publisher, but wholly based on its role as an additional disseminator:

> the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites … [and] plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to … internet users who otherwise would not have found the web page …[94]

Consistently, the Court never inquired whether the sensitive information was in 'private', that is, personal *and* confidential.

Thirdly, and related, the public role played by the data subject in the past or present was relevant to the issue of whether the public may have a continued interest in the information,[95] but having engaged in activities that brought public attention did not by itself negate the data subject's entitlement to exercise the right to be forgotten. Activities that attract public attention (and are thus 'manifestly made public by the data subject'[96]) may often legitimise the initial use and disclosure of the personal information, but subsequently the right to be forgotten

[92] *GC and Ors* (n 88) para 66; see also para 67, noting the strengthened privacy interests in the case of sensitive personal data.

[93] *Google Spain* (n 7) para 81; now GDPR (n 8) art 17(3)(a).

[94] *GC and Ors* (n 88) para 36; *Google Spain* ibid, paras 35–37.

[95] *GC and Ors* ibid, para 66.

[96] Data Protection Directive (n 74) art 8(2)(e) and GDPR (n 8) art 9(2)(e); *GC and Ors* ibid, para 63. Information Commissioner's Office, 'Special Category Data: What are the Conditions for Processing?' (e) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-are-the-conditions-for-processing/#conditions5>: '[this] clearly assumes a deliberate act by the individual. It's not enough that it's already in the public domain – it must be the person concerned who took the steps that made it public.'

https://doi.org/10.1017/S0020589323000258 Published online by Cambridge University Press

returns to the data subject a degree of oversight over that information.[97] The CJEU recognised the sensitivity of privacy to time and context, including vis-à-vis criminal investigations and convictions, but framed that sensitivity in terms of the public's changing interest in the information.[98] It did not, however, try to argue that personal information which is in the public domain may re-acquire, after some time, a private or confidential quality, and may therefore be, once more, worthy of protection.[99] As will be seen in the discussion of Article 8 of the ECHR, the above points assume significance when information privacy is predicated on the 'private' status of the information in question.

B. US Courts on the Right to be Forgotten

From a US perspective, the right to be forgotten is an anomaly because it protects non-private information against intrusions by private actors. Neither fits within the US conception of privacy. At the constitutional level, the 'negative' right to be left alone is first and foremost enshrined in the Fourth Amendment that guards against search and seizure without a warrant, and as such is exclusively focused on governmental intrusions of the home with some limited extensions beyond the home (as shown below). Horizontal protection, which would construct 'the right to be left alone' not as 'a claim for noninterference by the state … [but] *for* state interference in the form of legal protection against other individuals'[100] is virtually unknown in US constitutional law.

Meanwhile, intrusions by private actors, such as media companies, are covered by a selection of privacy tort actions, but these do not recognise invasions through disclosures of personal information which is already in the public domain. With a strong bias in favour of freedom of speech, US privacy protection necessarily assumes a sharp distinction between private and public information; it is not willing to recognise the possibility of degrees of publicness of personal information which could trigger legitimate privacy demands and thus restrictions on wider damaging publications.[101] In

[97] *GC and Ors* ibid, para 69: a search engine can refuse a de-referencing request if the 'processing is covered by the exception in Article 8(2)(e) of the directive, provided that the processing satisfies all the other conditions of lawfulness laid down by the directive, and the data subject has not exercised the right under Article 14(a) of the directive to object to that processing on compelling legitimate grounds relating to his particular situation.'

[98] ibid, para 77.

[99] 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 Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12' (26 November 2014) 14/EN WP225, 13: 'A good rule of thumb is to try to decide where the public having access to the particular information – made available through a search on the data subject's name – would protect them against improper public or professional conduct.'

[100] R Gavison, 'Privacy and the Limits of Law' (1980) 89(3) YaleLJ 421, 438 (emphasis in original). See also S Gardbaum, 'The "Horizontal Effect" of Constitutional Rights' (2003) 102 MichLRev 387.

[101] DJ Solove and NM Richards, 'Privacy's Other Path: Recovering the Law of Confidentiality' (2007) 96 GeoLJ 123.

https://doi.org/10.1017/S0020589323000258 Published online by Cambridge University Press

William Prosser's typology of US tort privacy actions the public–private dichotomy is the touchstone of liability for three out of his four categories: '1. Intrusion … into his private affairs. 2. Public disclosure of embarrassing private facts … 3. Publicity which places the plaintiff in a false light in the public eye …';[102] the fourth category of 'appropriation … of the plaintiff's name or likeness' creates a type of intellectual property rather than a privacy claim.

When addressing the second category of 'public disclosures of private facts'— a concern which prompted Warren and Brandeis 70 years earlier to declare a general right to privacy to protect one's personality[103]—Prosser concluded that its ambit was tightly circumscribed.[104] It certainly required a public disclosure of private or confidential facts:

> The 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.[105]

The same idea underlies the classic understanding of a breach of confidence claim. Personal information in the public domain—including public records of personal information—has irretrievably lost its entitling 'private' quality, and even a significant lapse of time cannot alter that fact:

> The difficult question is as to the effect of lapse of time, and the extent to which forgotten records, as for example of a criminal conviction, may be dredged up in after years and given more general publicity. As in the case of news, with which the problem may be inextricably interwoven, it has been held that the memory of the events covered by the record, such as a criminal trial, can be revived as still a matter of legitimate public interest.[106]

Once information is public, privacy entitlements are foregone. It makes no difference that personal information online is available for much longer and to a much wider and more diverse audience across social and physical spheres than information in the analogue world. Once public, always public. To be successful, the claimant also has to show—as part and parcel of their

[102] WL Prosser, 'Privacy' (1960) 48 CalLRev 383, 389; see also NM Richards and DJ Solove, 'Prosser's Privacy Law: A Mixed Legacy' (2010) 98 CalLRev 1887. For its continued relevance, see eg A Gajda, 'Privacy and the Right to Be Left Alone' in WR Davie and TM Maher (eds), *First Amendment Law in Louisiana* (University of Louisiana Press 2015).

[103] Warren and Brandeis (n 32) 195f (referring to photographs and newspaper enterprise invading 'the scared precincts of private and domestic life' and to 'the evil of the invasion of privacy by newspapers') and 205 (on the 'inviolate personality').

[104] Prosser constructed this category—as an extension of libel that would protect against mental distress and reputational damage, with the main difference being that the disclosed information was private, rather than false—at a time when the Supreme Court's reluctance to restrain truthful (personal) information had not yet materialised. See also Nissenbaum (n 3) 103ff (on privacy in public).

[105] Prosser (n 102) 394f (internal notes omitted; emphasis added).

[106] ibid 396 (internal notes omitted).

https://doi.org/10.1017/S0020589323000258 Published online by Cambridge University Press

'reasonable expectations of privacy'[107]—that 'the matter made public must be one which would be offensive and objectionable to a reasonable man of ordinary sensibilities'.[108] So what matters is not what the claimant considers to be an undue exposure but what the community view is or would be.

By implication, historic convictions can be unearthed indefinitely by the press, no matter how damaging the revelation may be for the rehabilitated offender. In *Briscoe v Reader's Digest Association*,[109] the Californian Supreme Court allowed a privacy claim against a newspaper for its revelation of the claimant's long-forgotten criminal past as a hijacker which had the effect of alienating his daughter and friends from him. Yet, three decades later the same court held in *Gates v Discovery Communications, Inc.*[110] that *Briscoe* was no longer good law, given the US Supreme Court jurisprudence in the intervening years. The press could not be liable for publishing information that was neither false nor misleading and such information included information that was either part of a 'public record' or otherwise 'lawfully obtained'[111] and, at times, even unlawfully obtained.[112] In *Cox Broadcasting Corp. v Cohn*[113] the US Supreme Court already had decided that 'the interests in privacy fade when the information involved already appears on the public record [such as an official court record]'[114] and then restated this more firmly in subsequent decisions: 'once the truthful information was "publicly revealed" or "in the public domain," the court could not constitutionally restrain its dissemination'.[115] For the Court in *Gates* this was an 'unqualified' ruling of an 'absolute right' of the press which was unaffected by the age of the public record.[116]

Prosser explained the US hostility to privacy in public on the basis that anyone 'who is not a hermit must expect the more or less casual observation of his neighbours and the passing public as to what he is and does, and some reporting of his daily activities … The law of privacy is not intended for the protection of any shrinking soul …'.[117] In the internet age, however, public exposure is often far more extensive and damaging than the 'casual

[107] Discussed further below.

[108] Prosser (n 102) 396. The test has also been adopted in other common law countries, see n 150 below; see also discussion in Barendt (n 66) 98ff.

[109] *Briscoe v Reader's Digest Association, Inc.* 4 Cal.3d 532 (1971); see also *Melvin v Reid* 112 Cal.App 285, 297 P. 91 (1931).

[110] *Gates v Discovery Communications, Inc.* 34 Cal.4th 679 (Cal. 2004).

[111] *Cox Broadcasting Corp. v Cohn* 420 U.S. 469 (1975); *Oklahoma Publishing Co. v District Court* 430 U.S. 308 (1975); *Smith v Daily Mail Publishing Co* 443 U.S. 97 (1979); *The Florida Star v B.J.F.* 491 U.S. 524 (1989). These cases all concerned the identities of the victims of a crime, rather than that of the offender.

[112] *Bartnicki v Vopper* 532 U.S. 514 (2001).

[113] *Cox Broadcasting Corp.* (n 111).

[114] ibid 494f.

[115] *Smith v Daily Mail Publishing Co.* (n 111) 103 summarising *Oklahoma Publishing Co. v District Court* (n 111), approved in *The Florida Star v B.J.F.* (n 111) 535.

[116] *Gates v Discovery Communications, Inc.* (n 110). See also Eberle (n 1) 191–2 describing how free speech was elevated to its status as the 'premier fundamental freedom' through its incorporation into other rights/freedoms starting with the Due Process Clause (14th Amendment) in *Gitlow v New York* 268 U.S. 652 (1925). Note also the curtailing of defamation claims in *New York Times Co. v Sullivan* 376 U.S. 254 (1964).

[117] Prosser (n 102) 396f.

observation of one's neighbours and the passing public'. Still, Americans whose reputation may potentially be damaged indefinitely due to online exposure are left to their own devices and to market-based solutions, with all their attendant inequities, to restore their public standing as honourable members of society.[118] Private initiatives must provide the answer to social rehabilitation, not the State. These private initiatives may come from platforms themselves, without any danger of offending US constitutionality. Despite its protest at the EU right to be forgotten, Google has now extended a limited version of the right of be forgotten to its users in the US.[119] Yet, there is, of course, a significant difference between a legal right and remedies, and a voluntarily granted corporate concession.

US jurisprudence on the right to be forgotten shows that the right could, in principle, exist within a standard privacy regime, assuming that regime recognised a legitimate privacy interest in public personal information. In other words, the right to be forgotten is not wedded to data protection law. Indeed, the technicality of data protection law merely obscures the fact that it is, like other privacy frameworks, concerned with striking an appropriate balance between competing private and public interests in accessing personal information (transparency) and in controlling such access (non-disclosure). Data protection law seeks to provide a tightly structured, comprehensive framework for that balancing act.

C. *The ECtHR on the Right to be Forgotten within Article 8*

In contrast to the clarity of the CJEU endorsement of the right to be forgotten and of the US rejection of the same right, a more muddled picture emerges from the jurisprudence on the right to privacy in Article 8 of the ECHR. A 'merger' of Article 8 privacy and data protection law (and its right to be forgotten) occurred in *ML & WW v Germany*[120] where the ECtHR deliberated on Article 8 privacy claims comparable to the GDPR's right to be forgotten. Such a merger has also occurred in cases decided by English courts on the right to be forgotten in data protection law, which they interpreted in light of Article 8 jurisprudence, as for example in *NT1 & NT2 v Google LLC*.[121] In other words, traditional Article 8 jurisprudence has responded to data protection law either by incorporating data

[118] See discussion below on the disentitling effect of such self-help actions under ECHR, art 8.

[119] V Dressler, 'Google Quietly Rolls Out the Right to be Forgotten Mechanism in the U.S.' (Office for Intellectual Freedom of the American Library Association, 14 June 2022) <https://www.oif.ala.org/oif/google-quietly-rolls-out-the-right-to-be-forgotten-mechanism-in-the-us/>. The right is limited to information such as phone numbers, email or physical addresses, handwritten signatures, non-consensual explicit or intimate personal images, involuntary fake pornography, or personal content on websites with exploitative removal practices.

[120] *ML and WW v Germany* App No 60798/10 and 65599/10 (ECtHR, 28 June 2018) (*ML & WW*).

[121] *NT1 & NT2* (n 82); for similar cases on public disclosure of spent convictions, see *Hayden v Duckworth* [2021] EWHC 1033; *Hayden v Dickenson* [2020] EWHC 3291.

https://doi.org/10.1017/S0020589323000258 Published online by Cambridge University Press

protection normativity within Article 8 jurisprudence, or by developing the jurisprudence on data protection law in light of Article 8.[122]

Much like *GC and Ors*, these two cases concerned sensitive personal data, and, in particular, prior criminal convictions that were kept fresh in the public's mind through their online availability. As *ML & WW* dealt with the claimants' possible right to be anonymised in news articles which reported their prosecutions and convictions in a murder case in the online archives of the media organisations, these were claims against the primary publishers. As such, they were more problematic than 'normal' right to be forgotten cases against search engines, as the redaction of names in primary sources signals the full exit of the personal information from the public domain rather than its partial inaccessibility.[123]

For present purposes, however, the points of interest lie in how these judgments have sought to bridge the divide between the GDPR and Article 8 jurisprudence—and implicitly between Anglo-American and Continental European cultures of privacy. Whilst the actual outcomes may well be defensible, the reasoning shows that Anglo-American ideas of privacy are not easily grafted onto Continental European privacy roots, or vice versa.

The starting point here is that, despite its location in the ECHR, Article 8 finds its roots in the American culture of privacy rather than in the Continental European tradition. Whilst Article 8 echoes Article 12 of the Universal Declaration of Human Rights (UDHR, 1948), Article 12 in turn speaks to the American influence in its drafting.[124] Not only was the first draft prepared by John P Humphrey, Director of the United Nations Division of Human Rights, and framed 'in a language obviously borrowed from the US Constitution',[125] albeit subsequently revised, the final draft followed recommendations by the US and was particularly guided by the 'Statement of Essential Human Rights' drafted under the auspices of the American Law Institute.[126]

Article 12 of the UDHR is not a carbon copy of the Fourth Amendment, but there is, undoubtedly, a family resemblance between the two. Article 12 provides that '[n]o one shall be subject to arbitrary interference with his

[122] J Kokott and C Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3(4) IDPL 222; De Hert and Gutwirth (n 70) 3. An arguably preferable approach to their relationship has been taken in the EU Charter of Fundamental Rights (n 16) where privacy and data protection exist side by side as distinct and independent rights in art 7 (privacy) and art 8 (data protection). See Lynskey (n 88).

[123] *ML & WW* (n 120) para 97, acknowledging the difference.

[124] O Diggelmann and MN Cleis, 'How the Right to Privacy Became a Human Right' (2014) 14 HRLRev 441, 452: 'The UDHR was clearly the most important point of reference.' (tracing the unusual birth of privacy as a human right internationally despite not having enjoyed explicit recognition in any constitutions).

[125] ibid 445.

[126] ibid 446, 449. Note that 'The Statement of Essential Human Rights' (American Law Institute 1945) itself was drafted by a multi-national committee with a strong US presence (ie 12 out of 25 members) and included Article 6 on Freedom from Wrongful Interference: 'Freedom from unreasonable interference with his person, home, reputation, privacy and, activities, and property is the right of every one.'

privacy, family, home or correspondence …'; whilst the Fourth Amendment provides that 'the right of the people to be secure in their *persons, houses, papers and effects*, against unreasonable searches, shall not be violated …' (emphases added). Thus both conceive of privacy as a bundle of related rights grounded in the overlapping concepts of person/privacy, house/home (family) and papers/correspondence. That family resemblance becomes more pronounced in comparison with Continental European constitutional grants of quasi-privacy rights at the time. Notably, equality—or equal dignity in Whitman's terminology—figured as the primary constitutional right and foundation of privacy, and the inviolability of the home and the secrecy of correspondence appeared much later in the documents as separate and distinct rights.[127]

Furthermore, consistent with the American conception of privacy, the focus of Article 8 was firmly on State intrusions, with the specific intent of pre-empting the threat of totalitarian governments.[128] It took the ECtHR half a century to recognise privacy-in-public entitlements against private actors. In *Von Hannover v Germany*[129] that shift finally occurred, and Judge Zupančič expressly framed that recognition in terms of rolling back the American influence on Article 8:

> [I]t is impossible to separate by an iron curtain private life from public performance. The absolute *incognito* existence is the privilege of Robinson; the rest of us all attract to a greater or smaller degree the interest of other people. Privacy … is the right to be left alone. One has the right to be left alone precisely to the degree to which one's private life does not intersect with other people's private lives. In their own way, legal concepts such as libel, defamation, slander, etc. testify to this right and to the limits on other people's meddling with it. The German … doctrine of *Persönlichkeitsrecht* testifies to a broader concentric circle of protected privacy. Moreover, I believe that the courts have to some extent and under American influence made a fetish of the freedom of the press. The *Persönlichkeitsrecht* doctrine imparts a higher level of civilised interpersonal deportment. It is time that *the pendulum swung back to a different kind of balance* ...[130]

[127] See, for example, the Greek Constitution of 1911: 'The Greeks are equal in the eye of the law and contribute without distinction to the public burdens according to their ability …' (art 3); 'The dwelling is inviolable …' (art 12); 'The secrecy of letters is absolutely inviolable.' (art 20). See also the Weimar Constitution of 1919 (Germany): 'All Germans are equal before the law. Men and women have the same fundamental civil rights and duties. Public legal privileges or disadvantages of birth or of rank are abolished …' (art 109); 'The home of every German is his sanctuary and is inviolable …' (art 115); 'The secrecy of letters and all postal, telegraph, and telephone communications is inviolable …' (art 117).

[128] Ed Bates, *The Evolution of the European Convention on Human Rights* (OUP 2010) 5ff.

[129] *Von Hannover v Germany* App No 59320/00 (ECtHR, 24 June 2004); discussed in NA Moreham, 'Privacy in Public Places' (2006) 65(3) CLJ 606; Fenwick and Phillipson (n 43) 671ff. For important forerunners, see *Peck v the United Kingdom* App No 44647/98 (ECtHR, 28 January 2003); *P.G. and J.H. v United Kingdom* App No 44787/98 (ECtHR, 25 September 2001).

[130] *Von Hannover v Germany* ibid (emphasis added).

The shift in the interpretation of Article 8 towards the recognition of privacy-in-public and, by implication, towards the express recognition of privacy threats emanating from the media, necessarily also prompted a more emphatic endorsement of the State's 'positive obligations … [that] may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves'.[131] Unexpectedly, the case arose from the (partial) refusal of the German Constitutional Court to recognise the privacy-in-public entitlements of Princess Caroline of Monaco on the ground that she had—as a 'figure of contemporary society par excellence'—only limited privacy rights in public.[132] The ECtHR, however, intervened to affirm her privacy-in-public entitlement and thereby also expanded the sphere of protection of Article 8 more generally (even if some commentators argue that the ECtHR's decision went too far in the specific case[133]).

This expansion led to the creation of a similar cause of action in England and Wales[134] in *Campbell v MGN*.[135] Prior to this, there was a historic reluctance to extend privacy remedies beyond traditional common law quasi-privacy protections, which mainly covered the literal inner space of the home and body. However, there had been a gradual expansion of the concept of 'confidential' in recognition of the need to protect private–public scenarios, such as a kiss in a restaurant.[136]

[131] *Von Hannover v Germany* ibid, para 57, citing in support: *X and Y v the Netherlands* App No 8978/80 (ECtHR, 26 March 1985) para 23; *Stjerna v Finland* App No 18131/91 (ECtHR, 25 November 1994) para 38; *Verliere v Switzerland* App No 41953/98 (ECtHR, 28 June 2001). For subsequent decisions on the positive obligations of States to guard against horizontal violations, see *K.U. v Finland* App No 2872/02 (ECtHR, 2 December 2008) paras 42–51; *Ageyevy v Russia* App No 7075/10 (ECtHR, 18 April 2013) paras 194–195: 'although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life … These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.'

[132] *Princess Caroline of Monaco* 1 BvR 653/96 (BVerfG, 15 December 1999) paras 102–113 affirmed the decision of the Federal Court of Justice in favour of the publication: *Princess Caroline of Monaco* 13 A 5005/95 (BGH, 19 December 1995) (holding that figures of contemporary society 'par excellence' were entitled to privacy outside their home but only in secluded places away from prying eyes).

[133] The decision has been rightly criticised for cutting the margin of appreciation to a 'vanishing point' and for misunderstanding the nuanced privacy entitlements of public figures in German jurisprudence: Fenwick and Phillipson (n 43) 674; Markesinis et al (n 1) 146f, 185ff.

[134] Based on Articles 8 and 10 of the ECHR; and the duty imposed by the Human Rights Act 1998 on public authorities to act compatibly with both parties' Convention Rights and, specifically in the case of courts, to interpret the law consistently with Convention Rights.

[135] *Campbell v MGN Ltd* (n 33) para 51, where the House of Lords explicitly recognised the new privacy cause of action and expressed its distinct underlying values in Continental European privacy terms: 'Instead of the cause of action being based upon the duty of good faith applicable to confidential personal information and trade secrets alike, it focuses upon the protection of human autonomy and dignity—the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people.'

[136] Phillipson (n 30) 735ff.

1. 'Private' information and 'private' harms

Despite the expanded reading of Article 8 and the fact that the ECtHR has for some time included data protection within its ambit,[137] Article 8 has remained firmly wedded to the idea that information must be 'private' in order to attract protection. Juliane Kokott, Advocate General at the CJEU, observed that 'on closer inspection, it appears that Strasbourg requires an additional element of privacy in order for personal information to be included in the scope of private life'.[138] This additional 'private' element requires a contortionist trick in the case of public personal information, such as a criminal conviction or police caution. The ECtHR has pulled off this trick by holding that when such public information 'recedes into the past, … [it] becomes a part of the person's private life which must be respected'.[139]

It is questionable whether in such cases the 'private' categorisation is anything other than the conclusion that the information must be protected rather than a precondition for such protection. It is, however, a legal fiction that such personal information can acquire a confidential status considering that it remains in official police records and news archives. Against this contorted interpretation of Article 8, Warby J in *NT1 & NT2* went a step further by liberally adding assumptions from the Anglo-American culture of privacy to his data protection analysis of whether the claimant's criminal record was 'sensitive personal data' as a counterweight to the public's interest in it. Not surprisingly, it had none of the 'private' hallmarks:

> The rest of the information ('the crime and punishment information') is 'sensitive', but *it is not intrinsically private in nature*. The criminal behaviour has a private aspect in that it was undertaken *in secret*, and *not intended for public view. But it was not intimate or even personal. It was business conduct, and it was criminal.* Having been identified and then made the subject of a public prosecution, trial and sentence, it all became essentially public. The authorities do show that information that begins as public may become private, and that Article 8 may be engaged by dealings with information, of whatever kind, that have a grave impact on the conduct of a person's private life—for instance by undermining their 'personal integrity'—or by interfering with their family life … But the *essential nature of the crime and punishment information in this case was public, not private*.[140]

His reasoning, steeped in the Anglo-American culture of privacy as reflected in Article 8, misconstrues data protection law. For the latter, information must only

[137] *Z* v *Finland* App No 22009/93 (ECtHR, 25 February 1997) paras 95–97; *Rotaru v Romania* App No 28341/95 (ECtHR, 4 May 2000) para 43; *Amann v Switzerland* App No 27798/95 (ECtHR, 16 February 2000) para 65.

[138] Kokott and Sobotta (n 122) 224.

[139] *M.M. v United Kingdom* App No 24029/07 (ECtHR, 13 November 2012) para 188, discussed in Kokott and Sobotta ibid 224; see also *Rotaru v Romania* (n 137): 'Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past.'

[140] *NT1 & NT2* (n 82) para 140 (emphasis added). See also para 170.

https://doi.org/10.1017/S0020589323000258 Published online by Cambridge University Press

be 'personal' which, once more, means 'relating to an identified or identifiable natural person',[141] and not secret, confidential, intimate, family- rather than business-related, or 'innocent'. Thus, when the right to be forgotten applies, the information need not have become 'private' before it can be 'forgotten' which would make the right all but redundant. The right to be forgotten envisages that the relevant personal information is, and will, remain in the public domain, but should not be so easily traceable to the data subject. The problem with this Anglo-American inflection on data protection law is that it misdirects the engagement of the right to the private sphere and thereby undermines its functionality.

This misdirection also manifests itself in the different types of harms that both rights target. Article 8 defines privacy with the Anglo-American gravitational pull of home and family life. Thus, even though professional harms are not in principle excluded,[142] in *ML & WW* the ECtHR stated that '[i]n order for Article 8 to come into play … an attack on a *person's reputation* must attain a certain level of seriousness and in a manner causing prejudice to personal enjoyment of the right to respect *for private life*'.[143] Transposed onto data protection law, Warby J in *NT1 & NT2* looked for harms derivatively suffered by the claimant's innocent and thus deserving family members, and in the absence of such derivative interests, the entitlement would be more difficult to establish.[144]

Yet, data protection law guards against harms which lie—in the first instance—in the interference with one's personal, meaning autonomous, zone, and—in the second instance—in harms widely defined, including professional harms, or harms in public, that an individual may suffer at the hand of employers or in business.[145] In *Google Spain* Mr González's professional activities as a lawyer suffered,[146] and in *GC and Ors*, the court listed as a relevant factor in the balancing exercise 'the consequences of publication for the data subject'[147] with no mention of home or family life. Re-integration in society, as opposed to social exclusion based on continuing stigmatisation, requires more than anything else a footing in the social and employment sphere.

[141] Data Protection Directive (n 74) art 2(a), and now GDPR (n 8) art 4(1).

[142] While Article 8 is primarily directed at 'private' harms, the ECtHR has held that 'there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life"': *Rotaru v Romania* (n 137); *Amann v Switzerland* (n 137). For the ECtHR jurisprudence of privacy entitlements in respect of professional and business activities, see Council of Europe (n 20) 23ff.

[143] *ML & WW* (n 120) para 88 (emphasis added).

[144] NT1 & NT2 (n 82) paras 154–155, 167. In relation to NT2, the balance tipped in favour of removal partly because he had a young family: 'Moreover, unlike NT1, this claimant has a young family, and the impact of disclosure of his old conviction is capable of having an adverse impact. His case on interference with family life is stronger.' (para 222; see also paras 224, 226).

[145] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* EU:C:2010:662, para 59: 'It is of no relevance in this respect that the data published concerns activities of a professional nature …'.

[146] *Google Spain* (n 7).

[147] *GC and Ors* (n 88) para 77.

2. 'Reasonable or legitimate expectation of privacy'

The mismatch between the two traditions is also pronounced in so far as Article 8 jurisprudence imports the concept of 'reasonable or legitimate expectation of privacy' to data protection law. The concept of 'reasonable expectation of privacy' has variously been described as a touchstone for Article 8 entitlement (which it is in the English action of misuse of private information) or as one available route to such entitlement.[148] It has its origins in the US case of *Katz v US*,[149] and has subsequently been adopted with variations in other common law jurisdictions.[150] In *Katz* the US Supreme Court extended the ambit of the Fourth Amendment prohibition of warrantless 'searches and seizures' to eavesdropping beyond the strict enclosures of the home to other spaces where one may have 'reasonable expectations of privacy', here an enclosed public telephone booth. The case thus concerned a covert intrusion, rather than a disclosure.[151] Pursuant to *Katz*, the test requires 'first that a person … [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable'[152] and, as argued above, the latter is tied to an offensiveness standard.

Whilst *Katz* expanded traditional American privacy beyond the four walls of the home, it is wholly at odds with data protection law and its right to be forgotten, and implicitly the Continental European culture of privacy. To start with, considering that the right to be forgotten is invariably directed at *public* personal information, it would often be difficult to satisfy that there was an actual or legitimate expectation of privacy, particularly if—as has been the case—the test is also conditional upon proof of the confidential nature of the information.[153]

In *ML & WW* the ECtHR found that the initiatives taken by the claimants to prove their innocence through reopening the proceedings and to enlist the

[148] *In re JR38* [2015] UKSC 42 contrast majority and minority judgment; discussed in J Purshouse, 'The Reasonable Expectation of Privacy and the Criminal Suspect' (2016) 79(5) ModLRev 871, commenting that the ECtHR has not used the test as a touchstone test; see also Barendt (n 66) 104.

[149] *Katz v United States* (n 28).

[150] Australia: *Australian Broadcasting Corporation v Lenah Game Meats* Pty Ltd [2001] HCA 63, para 42 ('highly offensive to a reasonable person of ordinary sensibilities'); New Zealand: *Hosking v Runting* [2005] 1 NZLR 1 ('the existence of facts in respect of which there is a reasonable expectation of privacy'); England and Wales: *Campbell v MGN Ltd* (n 33) ('the touchstone of private life is whether in respect of the disclosed facts the person in question had a reasonable expectation of privacy'); Barendt (n 66) critiques the test as artificial and importing free speech interests both at the first and second stages of the analysis.

[151] Barendt ibid 103f also notes that the Strasbourg court has been relying on the test in intrusion cases, arguably on the basis of a lack of an alternative test given the victim's absence of knowledge.

[152] *Katz v United States* (n 28).

[153] In English jurisprudence the test has been used at the second of a three-stage approach to Article 8—after deciding whether the alleged Article 8 intrusion is serious enough, and before determining whether it is outweighed by other (public) interests; see *R (Wood) v Commissioner of Police for the Metropolis* [2010] 1 WLR 123, 136. Both Barendt (n 66) 102f, and Purshouse (n 148) 881, persuasively argue that the test should, if at all, only figure at that third/balancing stage.

support of the press for that purpose meant that they 'had only a limited legitimate expectation … of obtaining anonymity in the reports or even a right to be forgotten online'.[154] Similarly, for Warby J NT1's engagement of a reputation management business two months after his conviction became spent[155] in order to 'put forward such clear and gross misrepresentations of his business history and his actual or reputed integrity'[156] was one of the reasons why he could not possibly entertain a legitimate expectation of privacy. American privacy encourages self-help as a means for rehabilitation; Continental European privacy gives legal remedies for that purpose. Yet, Article 8 falls between the two chairs as claimants risk foregoing a legal remedy should they take their online reputation into their own hands but are, at the same time, exposed to a jurisprudence that remains suspicious of the idea of privacy-in-public.[157] The public nature of the information remained for Warby J the main stumbling block:

> It was information about business crime, its prosecution, and its punishment. It was and is *essentially public in its character*. NT1 did not enjoy any reasonable expectation of privacy in respect of the information at the time of his prosecution, conviction and sentence. My conclusion is that he is not entitled to have it delisted now. It has not been shown to be inaccurate in any material way. It relates to his business life, not his personal life …[158]

Data protection law does not require a 'reasonable expectation to privacy' as a precondition for entitlement, but creates that expectation by tying privacy entitlements to the context or purpose for which personal information is taken or given in the first place, as for example crime reporting.[159] If access to personal information was given in a particular context or for a particular purpose, such as a purchase, medical treatment, or an employment contract, the reasonable expectation created by data protection law is that the information is not to be used otherwise. An approach to privacy which is tied to purpose or context[160] helps to explain various disclosure cases decided under Article 8 privacy,[161] and supports a context-based understanding of privacy.[162]

[154] *ML & WW* (n 120) para 109.
[155] *NT1 & NT2* (n 82) paras 125, 130, 168, 170.
[156] ibid, para 168.
[157] ibid, para 130, where Warby J somewhat acknowledges the unfairness of the position. See also *In re JR38* (n 148) where the UK Supreme Court unanimously dismissed the appeal of a 14-year-old minor who argued that the publication of his image taken by police during a sectarian riot, violated his Article 8 entitlement, with a majority holding that Article 8 was not engaged, discussed in Purshouse (n 148).
[158] *NT1 & NT2* (n 82) para 170 (emphasis added).
[159] The GDPR (n 8) refers to the reasonable expectations (see Recital 47) but links those expectations to the purpose of the use of the data, rather than its disclosure or dissemination per se.
[160] In *GC and Ors* (n 88), the term 'private' does not appear at all in the Opinion of the Advocate General, and only three times in the judgment of the Court in the course of the balancing exercise.
[161] For an obvious example, see *Peck v UK* [2003] EMLR 15 (where closed circuit TV footage that included the applicant and was collected by the council was later passed on to the media for a *Crime Beat* programme).
[162] Nissenbaum (n 3).

More significantly, in the Continental European culture of privacy, the individual is prima facie in control, and certainly the key arbiter for delimitating the acceptable boundaries of his or her metaphorical inner space, and thus of granting or denying access to relevant information. Privacy sensitivities vary from person to person, and thus the particularised content of privacy is within the eye of the beholder. Thus, consent is the touchstone of informational privacy under data protection law, and even for uses of personal information that are permitted without consent, individuals retain or regain some control through the right to object or the right to be forgotten as tools for their informational self-determination.[163] This means that an objective test based on 'reasonable expectation of privacy' which imports actual or desired community norms[164] misconstrues GDPR normativity. By the same token, any test that seeks to define 'private' and thereby imports notions of what 'most individuals in a given time do not want widely known about themselves'[165] seems also irreconcilable with an understanding of privacy as informational autonomy.

3. *'Foreseeable consequences of one's actions'*

Article 8 privacy does not shield individuals from 'the foreseeable consequence of … [their] own actions such as … the commission of a criminal offence'.[166] This privacy conception does not protect an individual from themself, which echoes the American laissez-faire attitude to social consequences of one's behaviour. It is not for the State to intervene in social relations on dignity grounds and protect individuals from communal judgment. This idea has found expression in the distinction drawn between voluntary and involuntary events as in the US case of *Daily Times Democrat v Graham*[167] concerning a wind gust blowing up the dress of an ordinary woman exposing her body waist down, and also in the concept of implied consent or waiver of privacy entitlements.[168]

[163] On consent, GDPR (n 8) arts 6(1)(a), 7, 9(2)(a); on data subject rights, see GDPR (n 8) Chapter III.

[164] As supported by some common law privacy lawyers, eg Moreham (n 129) 617ff.

[165] Fenwick and Phillipson (n 43) 663, citing with approval WA Parent, 'A New Definition of Privacy for the Law' (1983) 2 Law&Phil 305, 306f (emphasis added).

[166] *Axel Springer AG v Germany* App No 39954/08 (ECtHR, 7 February 2012) para 83; cited with approval in *ML & WW* (n 120) para 88; *NT1 & NT2* (n 82) para 111. However, see also *Sciacca v Italy* App No 50774/99 (ECtHR, 11 January 2005) para 29, where the ECtHR noted that the fact that the applicant was subject to criminal proceedings cannot curtail the scope of Article 8.

[167] *Daily Times Democrat v Graham* 162 So.2d 474 (1964).

[168] For a critique, see G Phillipson, 'Press Freedom, the Public Interest and Privacy' in A Kenyon (ed), *Comparative Defamation and Privacy Law* (CUP 2016) 136, 150; also LL Weinreb, 'The Right to Privacy' (2009) 17 Soc Philos Policy 43: 'The so-called "waiver," however, which rarely is explicit, consists of nothing but the fact that the information is not, in the circumstances, regarded as private.' (internal marks omitted).

https://doi.org/10.1017/S0020589323000258 Published online by Cambridge University Press

Article 8's prima facie indifference to self-inflicted reputational damage provided the background to the assessment of the anonymity claims in *ML & WW*,[169] and was injected into the data protection claims in *NT1 & NT2*. Warby J held that individuals who commit crimes may be assumed to have taken deliberate steps to be in the limelight[170] and so cannot complain about the availability of the information that had been 'manifestly made public' by them. Citing Stephen J in *Townsend v Google Inc.*,[171] he reasoned that 'legally as a consequences of the open justice principle by committing an offence he [the offender] is deliberately taking steps to make the information public'.[172] Considering that most offenders hope not to get caught and many do not, this interpretation of 'deliberately' stretches not only its natural meaning but also the legal understanding of intentionality.[173] It is, however, explicable against the Anglo-American expectation that individuals ought to bear the reputational consequences of their actions.

In contrast, data protection law generally and the right to be forgotten specifically seek to protect individuals from undeserved *and* deserved humiliation and stigmatisation, and acts as a restraint on prolonged communal disapprobation, bar countervailing public interests. Such countervailing public interests may lie in open justice or crime reporting, but once those interests are expended, there is a public interest in granting individuals reprieve even from the foreseeable consequences of their actions.

By the same token, where the public interest legitimises the continued presence of personal information in the public domain over and beyond what was necessary for the purposes of its initial lawful processing, the current 'role played by the data subject in public life' is invariably but only derivatively significant to determine the public interest.[174] Otherwise the fame or infamy of the individual does not, of itself, signal their 'implied consent' to public exposure for all times. In short, the right to be forgotten intervenes in what would otherwise be the foreseeable consequences of one's actions.

4. *Privacy versus freedom of expression*

The different interpretations of 'harm', 'legitimate expectations of privacy' or 'foreseeable consequences of one's actions' discussed above instantiate different perspectives on where to strike the balance between privacy and free speech. Both privacy and free speech are important values in each privacy

[169] *ML & WW* (n 120) para 88.

[170] *NT1 & NT2* (n 82) paras 110–113; Schedule 3, Condition 5 of the Data Protection Act 1998, following *Townsend v Google Inc. & Anor* [2017] NIQB 81. Data Protection Directive (n 74) art 8 (2)(e) (upon which Condition 5 is based) refers to '*manifestly* made public by the data subject' (emphasis added).

[171] *Townsend v Google Inc. & Anor* ibid.

[172] ibid, para 62; *NT1 & NT2* (n 82) para 110.

[173] *NT1 & NT2* ibid, para 113, where Warby J had to gloss over the wording of 'manifestly made public by the data subject' in the Directive.

[174] *GC and Ors* (n 88) and see text accompanying n 95.

culture, yet, when in conflict, are resolved differently. Those resolutions are—regardless of any formal constitutional hierarchy[175]—already implicit in the very nature of each conception of privacy and their respective places of engagement.

Locating privacy entitlements in the sphere of the home minimises the potential for clashes between privacy and freedom of expression, as they each occupy separate and distinct social spheres. It creates a framework within which privacy claims beyond the home—such as Prosser's category of 'public disclosure of private facts'—require very special circumstances indeed to justify curtailing free speech. In contrast, where privacy has its principal field of engagement in the social or public domain and is concerned with the levelling up of dignity *in public*, it acts routinely and deliberately as a restraint on freedom of expression.[176]

This explains why for the CJEU in *GC & Ors* and in *Google Spain* the privacy interests of the data subject would 'as a general rule' override the collective interest of the public in accessing the information. Warby J's insistence in *NT1 & NT2* that 'the "general rule" to which the court [the CJEU in *Google Spain*] was referring was a descriptive, not a prescriptive one'[177] misunderstands the essential speech-editing function of the right, and the informational self-determination which it facilitates in the public realm.[178]

Having said that, Warby J's approach is not inconsistent with Article 8, where privacy and freedom of expression have formally been placed on an equal footing: 'as a matter of principle these rights deserve equal respect'.[179] It thereby follows other jurisdictions that also accord equal standing to privacy and free speech, such as Germany, France or Israel, in contrast to the 'brutal simplicity of the First Amendment'.[180] On closer inspection, however, this equality of rights may be understood as no more than the requirement to balance the respective rights against each other, rather than the idea that there are no presumptive preferences in particular cases.[181]

In German privacy jurisprudence, for example, in cases of speech targeted at private individuals, privacy rights have generally won out, whilst in cases of harm to more diffuse dignitary interests, freedom of expression has carried the day.[182] It has also meant that 'pictures can only be disseminated or

[175] F Schauer, 'The Exceptional First Amendment' in M Ignatieff (ed), *American Exceptionalism and Human Rights* (Princeton University Press 2005).
[176] See also n 65.
[177] *NT1 & NT2* (n 82) para 133.
[178] F Brimblecome and GP Phillipson, 'Regaining Digital Privacy? The New "Right to be Forgotten" and Online Expression' (2018) 4 CJCCL 1.
[179] *Axel Springer AG v Germany* (n 166) para 87; *Von Hannover v Germany (No 2)* App No 40660/08 (ECtHR, 7 February 2012) para 106; *Mityanin and Leonov v Russia* App No 11436/06 (ECtHR, 7 May 2019) para 108; followed in *NT1 & NT2* (n 82) para 132f.
[180] Markesinis et al (n 1) 155.
[181] ibid.
[182] Carmi (n 1) 334ff; RJ Krotoszynski Jr, 'A Comparative Perspective on the First Amendment: Free Speech, Militant Democracy, and the Primacy of Dignity as a Preferred Constitutional Value in Germany' (2004) 78 TulLawRev 1549, 1581–3; see also n 65 and accompanying text.

exposed to the public eye with the express approval of the person represented',[183] unless the photograph is generally depicting contemporary society[184] or shows a public figure, and even then their legitimate interest in privacy may still trump the public interest in the information.[185] By extension, in data protection claims where the conflict between privacy and freedom of expression necessarily involves an identified or identifiable individual (as part and parcel of the definition of personal data), it makes sense that 'as a general rule' freedom of expression should yield to a 'grounded' claim of a right to be forgotten.

Consistently, whilst under the Data Protection Directive a de-referencing request depended on an individual making out 'compelling legitimate grounds relating to his particular situation',[186] under the GDPR the data subject only needs 'grounds relating to his or her particular situation' to assert their right to be forgotten, and it is the controller who has to demonstrate 'compelling legitimate grounds for [the continued] processing'.[187] So the GDPR now shows a presumptive preference for accepting an individual's justified take-down request, putting the onus on controllers to justify the continued accessibility of the data for compelling legitimate reasons.

IV. CONCLUSION

It is uncanny how the technical regulatory regime of data protection law should so comfortably embody the values of the Continental European culture of privacy with its focus on protecting one's public image—a tradition which Whitman described as 'vague and grandiose', and which has its philosophical roots in Kantian idealism and inalienable personal autonomy. Yet, the evidence is incontrovertible. Using the relatively new right to be forgotten in the context of spent criminal convictions as a case study for privacy-in-public, this discussion has revealed the right's comfortable standing in data protection law and CJEU jurisprudence since its inception in *Google Spain*; its outright rejection by the US judiciary in the face of free speech constitutional demands; and its contorted transformation by the ECtHR in its Article 8 jurisprudence that has been exposed to both Western cultures of privacy.

What is instructive about the case study is not just how protection based on 'personal' rather than 'personal and confidential' information necessarily opens

[183] Section 22 of the German Copyright Act, discussed in *Von Hannover v Germany No 2* (n 179).

[184] Under section 23(1) of the same Act, the publication of pictures portraying aspects of contemporary society is exempted from the obligation to obtain the consent of the person concerned within the meaning of section 22.

[185] German Copyright Act, section 23(2). See also comparative discussion of 'public figures' in Markesinis et al (n 1) 144ff.

[186] Data Protection Directive (n 74) art 14(a).

[187] GDPR (n 8) arts 21(1), 17(1)(c).

https://doi.org/10.1017/S0020589323000258 Published online by Cambridge University Press

the protective regime up to the public realm, but the significant consequences that flow from it for the types of harm that may be recognised, for the behaviours that may or may not be disentitling, or for how the competing values may be considered. Data protection law, within which the Continental European culture of privacy manifests itself, constructs the fundamentally vulnerable individual not just in the private setting of their home, but in the public domain of employment, community and polity and extends an entitlement to basic human dignity to those public realms. This explains why superimposing Article 8 jurisprudence based on its Anglo-American privacy roots on data protection law short-changes the right to be forgotten and severely restricts its operation to private information and the private sphere, which is not where it is meant to do its work.

James Whitman's comparative study of privacy cultures does heavy explicatory lifting of the fundamental difference in the privacy regimes in Continental Europe and the US (and other common law jurisdictions). Data protection law manifests as an odd privacy creature until it is positioned within Whitman's comparison from which it emerges as a fine sample of the Continental European culture of privacy. Yet, much as Whitman's approach presents as a detached non-critical assessment of culturally grounded privacy sensibilities, it also invites criticisms of the continued validity of the resultant regimes against their cultural myths.

So one might argue that contemporary social and economic relations in the US are so beset by inequalities that a privacy regime which is—in its essence—based on the cultural myths of the equal settler with equal dignity and of the State as the main enemy of liberty profoundly fails in its corrective mission today.[188] Meanwhile there may also be critical reflections on Continental European privacy regimes premised on the myth of the trustworthiness of the State, especially in the era of mass surveillance and its possibilities for governmental abuse, albeit not discussed in this article. By the same token, Whitman's approach focusing on the historic cultural contingencies of the privacy differences also (deliberately) understates the continuing dynamic nature of privacy regimes in their conversations with each other, that is other economic, legal and cultural orders.

It seems rather remarkable how Article 8 of the ECHR as traceable to Article 12 of the UDHR and the Fourth Amendment of the US Constitution (which in turn reflects the English common law on the inviolability of the home) belatedly got a Continental European privacy make-over in response to the refusal of the German Constitutional Court (of all courts) to recognise privacy-in-public in the particular case, and how this expanded definition then, once more, made its way back to England, the cradle of its common law understanding. In short, the evolution of privacy regimes is neither linear nor pure—nor is it over.

[188] Zumbansen (n 1) 252f.

https://doi.org/10.1017/S0020589323000258 Published online by Cambridge University Press