**Data Protection Law Revealed: The Right to be Forgotten and Two Western Cultures of Privacy**

**Abstract**

Data protection law has emerged as an important bulwark against online privacy intrusions, and yet its status within privacy law, or more narrowly information privacy, remains awkward. Its starting point of protecting ‘personal’ information rather than ‘private’ information puts it at odds with privacy more generally. Indeed in its very design it caters for public personal information, or personal information which has attained *some* publicness through *some* disclosure. This paper argues that data protection law is not the odd bedfellow of traditional privacy law properly so called but may be understood as a manifestation of Continental European culture of privacy. Its distinctiveness does not lie in its apparent technicality but in its robust openness to privacy-in-public, which puts it on a collision course with the Anglo-American culture of privacy. The discussion builds, with some critical interjection, on James Whitman’s comparative privacy study, which situates American privacy culture in the *literal ‘inner space’ of the home* (building on English common law roots) and Continental European privacy culture in a *metaphorical ‘inner space’ in public*. The latter, but not the former, culture recognises privacy-in-public. Whilst these cultures have long ‘met’ in different jurisdictions, this paper locates their enduring influence *and* antagonism within three contemporary privacy regimes. More specifically, by taking the right to be forgotten - as an archetypal right of privacy-in-public in the challenging context of spent convictions - the article gauges the comparative openness to such claims: (1) by the CJEU as the authoritative voice on GDPR normativity, (2) by the US judiciary as committed to the First and Fourth Amendment, and (3) by the Strasbourg Court on Art 8 of the ECHR 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 those very tensions also offer, as encounters with the ‘Other’, insights and opportunities.

**Table of Contents**

[1. Introduction 2](#_Toc116306475)

[2. Two privacy cultures and one’s ‘inner space’ 5](#_Toc116306476)

[2.1. The Anglo-American literal ‘inner space’ 5](#_Toc116306477)

[2.2. The Continental European metaphorical ‘inner space’ 7](#_Toc116306478)

[3. Contemporary privacy regimes and the right to be forgotten 11](#_Toc116306479)

[3.1. The CJEU on the right to be forgotten within the GDPR 13](#_Toc116306480)

[3.2. US courts on the right to be forgotten 16](#_Toc116306481)

[3.3. The ECtHR on the right to be forgotten within Art 8 19](#_Toc116306482)

[4. Conclusion 28](#_Toc116306483)

# Introduction

Despite the rising prominence of data protection law in contemporary network society and all pervasive data practices, its status in or outside privacy law, or information privacy law, remains contested. Most significantly, 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 attained *some* publicness through *some* disclosure. The argument made in this paper is that data protection law is not an awkward off-shoot of traditional privacy law properly so called, but is a manifestation of the Continental European culture of privacy and its robust openness to privacy-in-public. The discussion takes, as its starting point, James Whitman’s comparative privacy study[[1]](#footnote-1) which situates the heart of American privacy culture in the *literal ‘inner space’ of the home* (building on English common law roots) and the heart of Continental European privacy culture in a *metaphorical ‘inner space’ in public.*[[2]](#footnote-2) The latter, but not the former, culture recognises privacy-in-public. Although these cultures also share much common ground and have long intermingled in different jurisdictions, the discussion shows their enduring influence in three contemporary privacy regimes. Using the right to be forgotten as a new but quintessential example of data protection law’s stance to privacy-in-public, the article assesses the comparative openness to such claims (1) by the CJEU as the authoritative voice on GDPR normativity, (2) by the US judiciary as committed to the First and Fourth Amendment, and (3) by the Strasbourg Court on Art 8 of the ECHR and its fused Anglo-American and Continental European privacy jurisprudence. The Strasbourg jurisprudence in particular highlights the tensions arising from trying to marry the two privacy traditions, or merge data protection and ‘privacy’ law, and yet, these tensions also offer, as encounters with the ‘Other’, insights and opportunities.

The wider background that provides the context for the discussion are 21st century socio-technological developments with enormous privacy-intrusive potentials and which may be categorised as 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 individual flourishing.[[3]](#footnote-3) JD Lasica reflected as early as 1998 on the repercussions of the online accessibility of personal information 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]](#footnote-4) For Jeffrey 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]](#footnote-5) Since then the argument in favour of a right of information bankruptcy,[[6]](#footnote-6) or giving individuals a second chance, has been answered in the EU by the right to be forgotten, first, in the judgment of the Court of Justice of the European Union [CJEU] in *Google Spain* (2014)[[7]](#footnote-7) and then, explicitly in the right to erasure, or the right to be forgotten, in the General Data Protection Regulation [GDPR].[[8]](#footnote-8) This right allows individuals to ‘edit’ their online profile 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]](#footnote-9) In the US, however, this right has not been legally recognised, even though the American ideal of the ‘self-made man’ and the Atlantic crossing served as the metaphor for personal reinvention in the above accounts. Still, from a US perspective it is not for the State to facilitate such reinvention.

These attitudes are reversed when it comes to *covert* information practices, or the ubiquitous and surreptitious collection, aggregation and analysis of personal data, and including governmental surveillance. Here it is the EU that is moving towards creating governmental backdoors into encrypted data,[[10]](#footnote-10) as consistent with its relatively permissive stance towards bulk surveillance. In *Big Brother Watch v UK* (2021)[[11]](#footnote-11) which concerned the legality of the NSA and GCHQ surveillance programmes as revealed by Edward Snowden, the European Court of Human Rights [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 accompanied by end-to-end safeguards against abuses of power.[[12]](#footnote-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]](#footnote-13) Similarly, in La Quadrature du Net and Other (2020)[[14]](#footnote-14) and *Privacy International* (2020)[[15]](#footnote-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]](#footnote-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]](#footnote-17) These are cases that appear to close the door to indiscriminate State surveillance, yet in fact leave it slightly ajar. Meanwhile, the US responded to the Snowden revelations with the rather more pro-active and decisive step of the USA Freedom Act 2015[[18]](#footnote-18) that ended the governmental surveillance programme of domestic telecommunications meta data. Paradoxically, Snowden’s exposure attested to the level of secrecy the US government deemed necessary to engage in bulk surveillance, and the *Freedom* Act in turn showed quite how profoundly State surveillance jars with the American ideal of individual liberty – a privacy sensitivity of a different kind. Here privacy is not about personal reinvention, but still goes towards guarding individual flourishing uninhibited by a sense of being watched.[[19]](#footnote-19) Harm suffered through bulk surveillance may thus also be understood as inroads into self-determination or self-realisation, albeit with accents different from those behind the EU-fashioned right to be forgotten.

The distinction between overt and covert information practices and resultant privacy threats, and the discrepancy in the EU and US responses to them roughly map onto the two Western cultures of privacy as per Whitman’s comparative study. Yet, much as the EU and US responses affirm the continued presence of these cultures, they also contain within themselves the seeds for questioning their standing as insular answers to threats of transnational dimension. As the online environment provokes a sustained encounter with the Other, it raises normative questions about the viability of each legal regimes and their underlying assumptions. The discussion in the second half of the paper on the right to be forgotten shows that for quite some time, the traditional legal cultures have been challenged, reconfigured and even been displaced in response to changing informational demands or economic ordering. This is nowhere more pronounced than in the law of England and Wales which, on the one hand, looks back to long-standing common law privacy roots which are now most prominently present in US law. On the other hand, the law of England and Wales has been strongly influenced by European privacy norms through the UK’s former membership in the EU (and its continued adherence to EU data protection law) and through its ratification of the European Convention of Human Right (and attendant exposure to Art 8 jurisprudence). So although England and Wales does not feature as a separate privacy jurisdiction in this paper, it is implicitly or explicitly present in all the three regimes discussed.

# Two privacy cultures and one’s ‘inner space’

The concept of privacy has been entangled in a rich and complex jurisprudence and grappled both with the incoherence of a great variety of privacy interests and claims (reproductive decisions, sexual orientation, surveillance, pollution, gun ownership, data protection, corporal punishment, search and seizure, just to mention a few[[20]](#footnote-20)) and stark differences in cultural sensitivities about what is or is not ‘private’ and thus what ought to be ring-fenced from, or for, interference.[[21]](#footnote-21) The discussion herebuilds on James Whitman’s framing of privacy along the 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]](#footnote-22) The value of liberty is key to understanding American privacy roots, whilst dignity underwrites the Continental European tradition. These two values help to explain their comparative differences, alongside strong congruencies and significant overlaps between the two privacy traditions.[[23]](#footnote-23) And even in their differences, both traditions seek to establish a literal or metaphorical inner space for self-authorship or self-sovereignty.

## The Anglo-American literal ‘inner space’

Whitman speaks of an *American* culture of privacy as being preoccupied with the home as the key site of protection. Yet, as the inviolability of the home as a place of security and liberty has a far longer common law history in England – a sentiment which would have chimed with American settler sensitivities - , the discussion here references the *Anglo-American* culture of privacy. Going as far back as the *Semayne’s Case* (1604)[[24]](#footnote-24) which dealt with the limits of the Sheriff for entering a house at the suit of a common person, and purported to rely on even older authority,[[25]](#footnote-25) Edward Coke captured the idea of the inviolate home as follows:

‘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]](#footnote-26)

‘My home is my castle’ encapsulates the traditional common law understanding of privacy, even if not under that label.[[27]](#footnote-27) In the home one has a right to be free from outside interferences, as clearly articulated in privacy terms in the US case of *Katz v US* (1967): ‘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]](#footnote-28) The home may be understood as an extension of the body, its armour or protective shell, which has constituted another core personal sphere of inviolability.[[29]](#footnote-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, and have being actionable *per se*, as the interference itself is the injury. In addition, traditional common law has also long guarded secrets through breach of confidence actions, but these need not involve *personal* secrets as opposed to trade secrets. Where such claims have concerned personal secrets, they again have generally concerned home or body.[[30]](#footnote-30) Furthermore, the possibility of a person’s physical seclusion from society within the home lies at the heart of various theories that have sought to explain privacy, such as those centred on the ‘intimate sphere’[[31]](#footnote-31) or the right to be left alone.[[32]](#footnote-32) By extension, privacy claims in public places, such as having one’s photo taken in a public street, are self-contradictory and anomalous, and not easily accommodated within this common law view of privacy.[[33]](#footnote-33) Comparing one’s *personal space* with a territory of a State, Joel Feinberg wrote in 1983: ‘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]](#footnote-34) Retreat, of course, is to the home.

Whilst pursuant to *Semayne’s Case* ‘the liberty or privilege of a house doth not hold against the King,’[[35]](#footnote-35) William Pitt, Earl of Chatham, famously expressed the maxim in a parliamentary speech in 1763 with a different take: ‘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]](#footnote-36)

This variation, according to which the main threat to one’s home comes from the State whose legitimate interventions are presumptively restricted to the realm outside the home, has found strong resonance in America.[[37]](#footnote-37) Although privacy as such is not explicitly recognised in the American Bill of Rights, it emerged from an array of constitutional guarantees, all directed against State exercises of power, but most importantly, the freedom from unlawful searches and seizures 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* (1886)[[38]](#footnote-38)]… issued an aggressive declaration of the “sanctity” of an American home.’[[39]](#footnote-39) He continues 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.’[[40]](#footnote-40) The American anti-State perspective on privacy is deeply inscribed with settler mentality, or a mentality of self-reliance and self-rule, and distrust of government - whether the old-world governments left behind, or the colonial administrations belatedly encountered in the new world. The binary, or conflict, to which this conception of privacy speaks is citizens-versus-government. Government cannot be trusted to not unduly interfere with individuals and thus its power must be curtailed. Privacy as liberty thus consists of liberty *from* government to allow a liberty *to* govern oneself, or self-sovereignty, in the home as the archetypal place where one is one’s own master.

## The Continental European metaphorical ‘inner space’

In the Continental European culture and conception of privacy, it 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 a foundation for self-authorship.[[41]](#footnote-41) This view of privacy is at least as concerned with one’s treatment *within* society as one’s entitlement to withdraw *away* *from* society. It is not about *seclusion* *per se* but rather about *controlling* one’s ‘appearances’ in the public realm. Recognising the social condition of humankind, here privacy sets boundaries on one’s public treatment where such treatment fulfils ‘no reasonable social purpose and serves only to provoke a scandal and personal humiliation…’[[42]](#footnote-42) It is functionally delimited through the *personal* nature of the information, that is image, name, word, and more generally data.[[43]](#footnote-43) Continental information privacy can thus be understood as informational self-determination or autonomy,[[44]](#footnote-44) or as a metaphorical ‘inner space’ protected against unwanted exposures in the outside world. Under the umbrella of dignity or honour, this conception guards against the threat of public *in*-dignities. Its historical background lies in the strict hierarchical nature of European societies where public humiliation was used as a political tool for disempowerment. In *The Politics of Humiliation: A Modern History*[[45]](#footnote-45) the historian Ute Frevert shows how a gradual shift from humiliation to dignity occurred in Europe from the early 19th 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.’[[46]](#footnote-46)

Against this social background, hate speech and anti-discrimination law can also be read as legal regimes that intervene in practices of public humiliation.[[47]](#footnote-47) Equally, the right to privacy – based on the Roman delict of *injuria*, concerned with a person’s ‘fame, reputation and honour’[[48]](#footnote-48) and directed against insult – is deeply inscribed with the idea of levelling up, or democratisation, 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!”’[[49]](#footnote-49) 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, in the first instance, 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*.’[[50]](#footnote-50) This contextualises why, for example, human dignity is the overarching value of the German Constitution (Art 1(1)) followed by ‘the right to free 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,[[51]](#footnote-51) although the underlying threat this conception addresses lies in class divisions and social hierarchies and their formal and informal maintenance through public humiliation.[[52]](#footnote-52) 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.’[[53]](#footnote-53)

Post’s analysis is persuasive in so far as privacy as dignity *is* focused on mutuality or sameness through equal entitlement to respect in the social realm, but 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.’[[54]](#footnote-54) The theoretical starting point for privacy as dignity is the Kantian idea of human personhood whose *inalienable* hallmark is free will,[[55]](#footnote-55) that is the ‘unpredictably individual, creatures whom no science of mechanics or biology could ever capture in their full richness.’[[56]](#footnote-56) So privacy as dignity flows from personal autonomy as a higher order concept.[[57]](#footnote-57) Privacy as dignity also recognises the fact that personal autonomy as a lower-order concept may be infringed, circumscribed or taken away in its entirety in the real world, 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 can only stand with the significant blind spots of Native Americans and African slaves)[[58]](#footnote-58) than in Europe where strict social hierarchies gave some much more choice than others. Thus within Europe the dignity-driven idea of privacy seeks to facilitate equal, dignified engagement, as a matter of process, to allow autonomous participation, as a matter of substance.[[59]](#footnote-59) In respect of the process itself, privacy as dignity gives individuals the autonomy to decide what is and 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.[[60]](#footnote-60) (So privacy here also acts as a form of withdrawal.) Personal autonomy cannot be abandoned or relinquished. Thus Continental European privacy is also deeply concerned with self-authorship or, in Post’s words, the expression of the ‘spontaneous, independent, and uniquely individual aspect of the self,’[[61]](#footnote-61) but asserts that this is only possible where there is equality of dignity in the public realm. This chimes with the fact that humiliation works as a tool of exclusion that denies self-determination at a very basic level; an outcast has few choices. Frevert writes: ‘Shaming is used to punish behaviour that runs contrary to what holds weight for a social group or organisation, it is carried out within that very group. In contrast, humiliation works by distinguishing radically between those who are in and those who are out: we are us, you are different and count for less.’[[62]](#footnote-62)

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. In that sense, not far removed from Post’s comparison, 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.[[63]](#footnote-63) The conceptions also 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 to protecting self-authorship and self-sovereignty[[64]](#footnote-64) which shines through the Continental European privacy culture bright and strong. Meanwhile in the American privacy tradition, being the master in one’s home is synonymous with self-determination,[[65]](#footnote-65) and implicitly with self-authorship, although never put in such ‘vague and grandiose’ ways as Continental European, especially German, jurisprudence will have it.[[66]](#footnote-66) The ‘inner space’ of the person protected by German-style privacy law is the literal ‘inner space’ of the American and English home.

# 3. Contemporary privacy regimes and the right to be forgotten

Whilst in the Anglo-American culture of privacy protection is reserved to the private sphere and private information, in the Continental European culture privacy is neither confined to intimate or secret information nor necessarily based on an *a priori* private sphere.[[67]](#footnote-67) This is quintessentially the case in data protection law, ‘a privacy law all but in name,’[[68]](#footnote-68) which does not deny protection merely because the information is public. Indeed, data protection is based on the assumption of some disclosure of personal information beyond the private sphere and gives individuals some control to oversee and manage that disclosure: ‘there would be no need for data protection if there was a general prohibition of information disclosure.’[[69]](#footnote-69) Consistently, Fuster and Gutwirth have argued that the shift from privacy to data protection is one from *secrecy* to *control*.[[70]](#footnote-70) Data protection law delivers informational self-determination[[71]](#footnote-71) against an understanding that much personal information is necessarily in the public domain and held by public or private institutions, and protection should not be foregone simply because of a delimited public-ness of the information. 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, e.g. employers, and public agencies - against the perceived narrowness of in Art 8 of the ECHR[[72]](#footnote-72) which, as discussed below, draws heavily on the Anglo-American privacy culture. Thus, although data protection law is framed in seemingly technical concepts and language (e.g. ‘data’ instead of ‘information’; ‘data subject’ or ‘data controller’; purpose limitation, or data minimisation) and presents as a type of data management bureaucracy, it was clearly understood as delivering an expanded version of privacy.

With its focus on ‘personal’ rather than ‘private’ information, data protection law generally bypasses controversies based on the private-public binary,[[73]](#footnote-73) and showcases the capacity of privacy to recognise layers of public-ness of personal information. Rights attach to information because it is personal, *i.e.* related to a person, *not* because it is ‘private’, that is personal *and* confidential.[[74]](#footnote-74) Indeed, even personal data that is necessarily in the public domain, such as one’s name or image, is protected, and this is not despite the fact that it is public but because it is.[[75]](#footnote-75) Whilst heightened protection is given to ‘sensitive personal data’[[76]](#footnote-76) even here the information is often *not* confidential or intimate 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.’[[77]](#footnote-77)

Personal information about ethnic origin, political opinions or religious beliefs is generally public, and classifying it as ‘sensitive’ resonates with the Continental European notion of levelling up of dignity in public. 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 that the strong egalitarian overtones of privacy in public as reflected in data protection law.[[78]](#footnote-78) Privacy gives individuals the power to shield themselves from public indignities with generally more pronounced effects on minorities. The exposure of name, image or word in public creates the potential for humiliation and so can be controlled by its ‘owner’ and just because personal information has legitimately entered the public realm for one purpose does not mean it is a free for all forever.[[79]](#footnote-79)

## 3.1. The CJEU on the right to be forgotten within the GDPR

An archetypal data protection right that showcases its privacy-in-public functionality is the right to be forgotten. It is deeply inscribed with the Continental European privacy culture in so far as it allows individuals to withdraw certain personal data already in the public domain and thus to manage their public image. It also expresses the *Zeitgeist* of that tradition by responding to a socio-technical environment that amplifies the public visibilityof personal information, and so its harm potential. When the right was first recognised in *Google Spain* (2014)[[80]](#footnote-80), the CJEU ‘found’ it by interpreting 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.[[81]](#footnote-81) Now it is a fully-fledged right in Art 17 of the GDPR. In *Google Spain* the information about Mr González’ bankruptcy and repossession proceedings a decade earlier which could be found on Google’s search results, had already been public through the Spanish newspaper’s publicly accessible archive. Yet, the visibility of that archive – whether on paper or digitised – was significantly prolonged and increased 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...’[[82]](#footnote-82) The Court thus recognised layers 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 and later audience created by the search engine.[[83]](#footnote-83)

Since then Google has had more than 1.1 million delisting requests.[[84]](#footnote-84) Most relate to private individuals seeking to shield themselves from unwanted public exposure based on ‘innocent’ information that entered the public domain at some point, *e.g.* family or work matters,[[85]](#footnote-85) and remained there beyond its use-by-date. In these ordinary claims privacy as dignity does its core work. A fraction of requests, however, involves 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 interest of the public in accessing the information. These rare cases amplify the tensions underlying the right to be forgotten and the clash between the two conceptions of privacy as they resolve these tensions differently. *On the one hand,* these cases highlight that self-authorship generally is a social affair: individuals define themselves against others, and reflexively respond to other’s perceptions of themselves.[[86]](#footnote-86) The public self is the counterpart to the private self. 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 the community, particularly on public figures or those that entered the limelight due to their wrongdoing. Yet, even traditional common law makes some limited allowances for protecting one’s public self through defamation law. *On the other hand,* 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...’[[87]](#footnote-87) 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. So wiping the slate fully clean cannot but be exceptional. Again, even common law jurisdictions have long made protective interventions through ‘forgetting’ concepts, such as bankruptcy or the idea of spent convictions.[[88]](#footnote-88) These recognise that some past actions have been sufficiently paid for, or carry potentially crippling long-term consequences, and that the community has an interest in reintegrating fallen persons back in society. Yet, the GDPR’s right to be forgotten provides for a more embracing forgetting concept.[[89]](#footnote-89)

An authoritative interpretation of the right to be forgotten through the CJEU – well versed in data protection law and the idea of privacy-in-public even in testing contexts – can be found in *GC and others v CNIL and Google* (2019)[[90]](#footnote-90) [*GC and Ors*]. Here the CJEU was asked whether and how search engines could handle ‘sensitive personal data’ given its heightened compliance requirements under data protection law.[[91]](#footnote-91) The case concerned four separate de-referencing requests:

* a satirical photomontage on YouTube of a former local political figure revealing an intimate relationship with another political figure;
* historic news articles about a suicide by a member of the Church of Scientology and the data subject’s role as a PR officer in that Church which he had since ceased;
* dated news stories about a judicial investigation into the funding of a political party, with no follow-up stories that the proceedings against the data subject had since been closed;
* and a data subject’s criminal conviction for sexual assaults of children under the age of 15.[[92]](#footnote-92)

For the comparative purposes here, the CJEU’s judgment nicely illustrates how the Continental European privacy tradition of managing one’s public images operates, as well as the strength of that tradition in testing circumstances. *First,* the Court reiterated its own holding in *Google Spain* that the individual’s right to be forgotten overrides *‘as a general rule’* the public’s interest in accessing information,[[93]](#footnote-93) that is freedom of expression, even if in the specific case:

‘[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.’[[94]](#footnote-94)

As this privacy is located within the public realm, and acts as a restraint on public communications, it routinely clashes with freedom of expression. If it would not ‘as a general rule’ override freedom of expression, it would not as a rule be functional. Still, a commitment to a right to be forgotten is not insensitive to the public’s interest in accessing information, as underscored, in the first place, by the right’s very focused remedy shielding individuals only from the results of searches of their names, but leaving the information otherwise in the public domain, and, in the second place, by the public interest exception.[[95]](#footnote-95)

*Second,* in the controversies in *GC and Ors*, the personal matters had, with one exception,already been in the public domain, and neither inaccurately nor illegitimately so. By the same token, Google’s privacy duties arose out of its role as search provider through which it creates *a new public* for the information. Its liability was thus not secondary or depending on the wrongdoing by the original publisher, but entirely separate based on its additional dissemination role: ‘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...’[[96]](#footnote-96) Consistently, the Court never inquired whether the sensitive information was in any way ‘private’. *Third* and related, the public role played by the data subject in the past and present went towards deciding whether the public may have a continued interest in the information,[[97]](#footnote-97) but having engaged in activities or behaviours that brought wanted or unwanted public attention does negate any entitlement to be forgotten at a later stage. Activities and behaviours that attract the limelight may legitimise the *initial* processing of the sensitive data by a search engine, as arguably being ‘manifestly made public by the data subject.’[[98]](#footnote-98) Yet, *subsequently* the right to object and the right to erasure, or now the right to be forgotten, return to the individual a power of oversight over their public image.[[99]](#footnote-99) Indeed, the Court’s reasoning is fully cognisant of the sensitivity of privacy to time and context, including *vis-à-vis* criminal investigations and convictions. Yet, what really is changeable is the public’s interest in the information.[[100]](#footnote-100) It is not that personal information somehow re-enters the private domain (descriptive) and thus re-acquires an entitlement to protection (prescriptive); rather the public’s interest may or may not dwindle over time.[[101]](#footnote-101) As will be seen in the discussion around Art 8 ECHR, these points assume significance when information privacy is predicated on the ‘private’ status of the to be protected information.

## 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 US privacy culture or law. At the constitutional level, the ‘negative’ right to be left alone is first and foremost enshrined in the Fourth Amendment that guards against searches and seizures without a warrant, and as such is exclusively focused on *governmental* intrusions of the home and some limited extensions. 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’[[102]](#footnote-102) is virtually unknown in US constitutional law. Meanwhile, intrusions by private actors, such as the media, *are* covered by a selection of privacy tort actions, but these do not recognise invasions through disclosures of personal information that 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 and is unwilling to recognise the possibility of degrees of public-ness that may trigger legitimate privacy demands and restrictions on wider damaging publications. [[103]](#footnote-103)

In William Prosser’s typology of US *tort* privacy claims 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...’[[104]](#footnote-104) – with the fourth category of ‘appropriation… of the plaintiff’s name or likeness’ creating a type of intellectual property rather than privacy. When addressing the second category of ‘public disclosures of private facts’ which Warren and Brandeis had seventy years earlier so strongly proposed,[[105]](#footnote-105) Prosser concluded that it was tightly circumscribed,[[106]](#footnote-106) and certainly required a public disclosure, or publicity beyond a small group, of private facts, not public ones: ‘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 descr**i**ption since this amounts to nothing more than giving publicity to what is already public and what any one present would be free to see.'[[107]](#footnote-107) The same idea underlies the classic understanding of a breach of confidence claims. 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.[[108]](#footnote-108)

Once information is public, privacy entitlements are foregone. It makes no difference that personal information online is available for much longer and to a wider and more diverse audience across social and territorial 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 her ‘reasonable expectations of privacy’[[109]](#footnote-109) – that ‘the matter made public must be one which would be offensive and objectionable to a reasonable man of ordinary sensibilities.’[[110]](#footnote-110) So it is not what the claimant personally considers to be an undue exposure but what the community considers to be such.

For historic convictions it means that they 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* (1971)[[111]](#footnote-111) 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* (2004)[[112]](#footnote-112) that *Briscoe* was no longer good law, given US Supreme Court jurisprudence in the intervening years. So the press could not be liable for publishing information that was neither false nor misleading and the information was either part of a ‘public record’ or otherwise ‘lawfully obtained’[[113]](#footnote-113) and, at times, even unlawfully.[[114]](#footnote-114) Already in *Cox Broadcasting Corp v Cohn* (1975)[[115]](#footnote-115) the Supreme Court had decided that ‘the interests in privacy fade when the information involved already appears on the public record [such as an official court record]’[[116]](#footnote-116) 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.’[[117]](#footnote-117) For the Court in *Gates* this was an ‘absolute right’ of the press and ‘unqualified’ ruling unaffected by the age of the public record.[[118]](#footnote-118)

Prosser explained 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…’[[119]](#footnote-119) In the internet age, however, public exposure is often far more extensive and damaging than the ‘casual observation of one’s neighbours and the passing public’. Still, Americans whose reputation may potentially indefinitely be damaged due to online exposure are left to their own devices and to market-based solutions (with all its attendant inequities) to rectify their public image and to try to regain an honourable position in society.[[120]](#footnote-120) Private initiatives must provide the answer to social rehabilitation, not the State. These private initiatives may come from platforms without any danger of offending US constitutionality. Thus, despite its protest to the EU right to be forgotten, Google has now extended a limited version of the EU right of be forgotten to its users in the US;.[[121]](#footnote-121) Yet there is of course much difference between a legal right (and attached remedies) and a voluntarily granted corporate concession.

This ‘negative’ jurisprudence by US courts on the right to be forgotten is still instructive on how the right could, in theory, exist within a ‘standard’ privacy regime. In other words, it is not intrinsically wedded to data protection law. Indeed, the technicality of data protection law hides that it is, like other privacy frameworks, concerned with striking a balance between competing private and public interests in accessing personal information (transparency) and in controlling such access (non-disclosure). Data protection seeks to deliver a tightly structured, comprehensive framework for that balancing act.

## The ECtHR on the right to be forgotten within Art 8

In contrast to the clarity of the CJEU endorsement of the right to be forgotten and the US rejection of that same right, a more muddled picture emerges from Art 8 jurisprudence on the right, where the ECtHR deliberated on Art 8 privacy claims comparable to the GDPR’s right to be forgotten in ML & WW v Germany (2018)[[122]](#footnote-122) [ML & WW]. Equally English courts have interpreted the right to be forgotten in EU data protection law in light of ECtHR jurisprudence, notably in NT1 & NT2 v Google LLC (2018)[[123]](#footnote-123) [*NT1 & NT2*]. These two samples present two alternative routes in which Art 8 normativity has met data protection law: either by incorporating data protection normativity within Art 8 jurisprudence, or by developing data protection jurisprudence in light of Art 8 jurisprudence.[[124]](#footnote-124) Much like *GC and Ors*, the 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 (reporting on their prosecutions and convictions in a murder case) in the online archives of the media organisations, these were claims against primary publishers and as such more problematic from a public interest perspective than ‘normal’ right to be forgotten cases against platforms or search engines. The redaction of names in primary sources signals the full exit of personal information from the public domain rather than its partial inaccessibility.[[125]](#footnote-125) For present purposes, however, the points of interest lie in how these judgments have sought to bridge the divide between the GDPR and Art 8 – and implicitly between Anglo-American and Continental European conceptions of privacy. Whilst the actual outcomes may well be defensible, the reasoning shows that Anglo-American privacy ideas are not easily grafted onto Continental European privacy roots, or vice versa.

The starting point here is that Art 8 drew – despite its location in the European Convention of Human Rights – in its inception more on American privacy culture and law than on the Continental European one. Whilst Article 8 echoes Art 12 of the Universal Declaration of Human Rights (1948), Art 12 in turn speaks to the American influence in its drafting.[[126]](#footnote-126) Not only was the first draft prepared by John P Humphrey, Director of the United Nation Division of Human Rights, and framed ‘in a language obviously borrowed from the US Constitution’[[127]](#footnote-127) albeit subsequently revised, on the evidence 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.[[128]](#footnote-128) Of course, Article 12 UDHR is not a carbon copy of the Fourth Amendment. Yet undoubtedly, there is a family resemblance between the two: Art 12 ‘No one shall be subject to arbitrary interference with his *privacy, family, home or correspondence*…’; and the Fourth Amendment: ‘the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches, shall not be violated…’. Both conceive of privacy as a bundle of related (privacy) 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 when equality (or equal dignity in Whitman’s terminology) figured as the primary constitutional right, and the inviolability of the home and the secrecy of correspondence appeared much later in the documents as separate and distinct rights.[[129]](#footnote-129) Also consistent with the American conception of privacy, the focus of Art 8 was firmly on State intrusions, with the specific intent of pre-empting the threat of totalitarian governments.[[130]](#footnote-130) It took the ECtHR half a century to recognise privacy-in-public entitlements against private actors. In *Von Hannover v Germany* (2004)[[131]](#footnote-131) that shift finally occurred and was framed by Judge Zupančič as follows:

‘it 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...’[[132]](#footnote-132)

The shift in the interpretation of Art 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.’[[133]](#footnote-133) Unexpectedly, *Von Hannover v Germany* arose from the refusal by German courts to recognise privacy-in-public entitlements of Princess Caroline of Monaco on the ground that she was a ‘figure of contemporary society par excellence’[[134]](#footnote-134) and it took the ECtHR to ‘swing the pendulum back’ and arguably unreasonably so in the particular case.[[135]](#footnote-135) Still, the expansion of Art 8 to privacy-in-public rights led to the creation of a like cause of action in England and Wales,[[136]](#footnote-136) the misuse of private information in *Campbell v MGN* (2004),[[137]](#footnote-137) against a historic reluctance to go over and beyond traditional common law quasi-privacy remedies. Trespass to land and to the person and actions for breach of confidence had until *Campbell* secured the literal inner space of home and body, albeit with a gradually expanded definition of ‘confidential’ to encompass private-public scenarios *e.g.* a kiss in a restaurant.[[138]](#footnote-138)

‘Private’ information and ‘private’ harms Despite the expanded reading of Art 8 and even despite the fact that the ECtHR has for some time included data protection within its ambit,[[139]](#footnote-139) Art 8 has remained firmly wedded to the idea that information must be ‘private’ to attract protection. Notably 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.’[[140]](#footnote-140) This additional ‘private’ element requires a contortionist trick in the case of *public* personal information such as a past conviction or police caution, a trick which the ECtHR has pulled off by holding that such information when it ‘recedes into the past,… becomes a part of the person’s private life which must be respected.’[[141]](#footnote-141) Whether in such cases the ‘private’ categorisation is anything other than the conclusion that the data must be protected rather than a precondition for such protection, is questionable. Certainly it is a legal fiction that such personal information acquires a *confidential* status considering that it remains in the official police records and news archives. Against this contorted Art 8 reading, Warby J in NT1 & NT2 went a step further by liberally adding assumptions from Anglo-American privacy culture to the data protection analysis on 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*.[[142]](#footnote-142)

His reasoning, steeped in Anglo-American privacy culture, as also reflected in Art 8, misconstrues data protection law. For the latter, as mentioned above, information must only be ‘personal’ meaning ‘relating to an identified or identifiable natural person,[[143]](#footnote-143) not meaning secret or 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. Indeed, 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 and thereby negates its functionality.

This misdirection also manifests itself in the different types of harms either targets. Art 8 defines privacy with an Anglo-American gravitational pull of home and family life. Thus even though professional harms are not in principle excluded,[[144]](#footnote-144) 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*.’[[145]](#footnote-145) 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.[[146]](#footnote-146) 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, that is, harms in public that an individual may suffer at the hand of employers or in business.[[147]](#footnote-147) In *Google Spain* Mr Gonzalez’s professional activities as a lawyer suffered,[[148]](#footnote-148) and in *GC and Ors,* the court listed as a relevant factor in the balancing exercise ‘the consequences of publication for the data subject’[[149]](#footnote-149) 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 or employment sphere.

‘Reasonable or legitimate expectation of privacy’ The mismatch between the two traditions is also pronounced in so far as Art 8 jurisprudence imports the concept of ‘reasonable or legitimate expectation of privacy’ to data protection law – either by applying it to personal data claims under Art 8 or alternatively through its incorporation in data protection claims. The concept of ‘reasonable expectation of privacy’ has variously been described as a touchstone for Art 8 entitlement (which it is in the English action of misuse of private information) or as one available route to such entitlement.[[150]](#footnote-150) It has its origins in the US case of *Katz v US* (1967),[[151]](#footnote-151) and has subsequently been adopted with variations in other common law jurisdictions.[[152]](#footnote-152) 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.[[153]](#footnote-153) 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 recognise as reasonable’[[154]](#footnote-154) and, as argued above, the latter is tied to an offensiveness standard.

Whilst *Katz* enlarged traditional American privacy beyond the four walls of the home, it is at odds with the Continental European privacy as instantiated in the right to be forgotten. To start with, considering that the right to be forgotten is invariably directed at personal *public* 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 ‘private’ or confidential nature of the information.[[155]](#footnote-155) In ML & WW the ECtHR found the initiatives taken by the claimants to prove their innocence through reopening the proceedings and to enlist the 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.’[[156]](#footnote-156) Similarly, for Warby J NT1’s engagement of a reputation management business two months after his conviction became spent[[157]](#footnote-157) in order to ‘put forward such clear and gross misrepresentations of his business history and his actual or reputed integrity’[[158]](#footnote-158) 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, Art 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 exposed to a jurisprudence that remains suspicious of the idea of privacy-in-public.[[159]](#footnote-159) So for Warby J the public nature of the information remained 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…’[[160]](#footnote-160)

Data protection law does not require a ‘reasonable expectation to privacy’ as a precondition for entitlement, but creates by and large that expectationby tying entitlements to the *context* or *purpose* for which personal information is taken or given in the first place *e.g.* crime reporting.[[161]](#footnote-161) If access to personal information was given in a particular context or for a particular purpose (*e.g.* purchase, medical treatment, or employment), the reasonable expectation created by data protection law is that the information is not used otherwise. Arguably this privacy approach tied to purpose or context[[162]](#footnote-162) helps to explain various disclosure cases decided under Art 8 privacy,[[163]](#footnote-163) and also chimes with Helen Nissenbaum’s argument for a context-based understanding of privacy.[[164]](#footnote-164)

Furthermore, Continental European privacy sees the individual as being *in control*, or as the key arbiter for delimitating the acceptable boundaries of his or her metaphorical inner space, of granting or denying access to relevant information. Privacy sensitivities vary from person to person, and thus the particularised content of privacy really *is* within the eye of the beholder. Consistently, 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.[[165]](#footnote-165) This means that an objective test based on ‘reasonable expectation of privacy’ which necessarily imports actual or desired community norms[[166]](#footnote-166) is profoundly at odds with the Continental European culture of privacy, and GDPR normativity. Arguably, for the same reason, 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’[[167]](#footnote-167) is also irreconcilable with an understanding of privacy as informational autonomy.

‘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.’[[168]](#footnote-168) This privacy conception does not protect an individual from herself, which echoes the American *laissez-faire* attitude to social consequences of an individual’s actions. 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* (1964)[[169]](#footnote-169) 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.[[170]](#footnote-170) Art 8’s *prima facie* indifference to *self-inflicted* reputational damage provided the background to the assessment of the anonymity claims in ML & WW,[[171]](#footnote-171) 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[[172]](#footnote-172) 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 (2017),[[173]](#footnote-173) 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.’[[174]](#footnote-174) 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.[[175]](#footnote-175) 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 and in particular the right to be forgotten seeks to protect individuals from undeserved and deserved pillorying or 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 derivatively significant to determine the public interest.[[176]](#footnote-176) Otherwise the fame or infamy of the individual does not, of itself, signal his or her ‘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.

Privacy versus freedom of expression The legal concepts compared above instantiate different perspectives on where and how to strike the balance between privacy and free speech. Both are important values in each privacy culture, albeit with different accents. These accents already emerge – regardless of any formal constitutional hierarchy[[177]](#footnote-177) – from the very nature of each privacy conception and their respective places of engagement. Locating privacy entitlements primarily in the sphere of the home minimises the potential for clashes between the two values, with each occupying 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, which explains why for the CJEU in *GC & Ors* and *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’[[178]](#footnote-178) misunderstands the essential speech-editing function of the right to be forgotten, and the informational self-determination that it facilitates in the public realm.[[179]](#footnote-179)

Warby J’s approach is not inconsistent with Art 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.’[[180]](#footnote-180) It thereby follows other jurisdictions that also accord equal standing to privacy and free speech, such as Germany, France or Israel, rather than, for example, the ‘brutal simplicity of the First Amendment.’[[181]](#footnote-181) 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.[[182]](#footnote-182) Thus, for example, in German privacy jurisprudence 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.[[183]](#footnote-183) It has also meant that ‘pictures can only be disseminated or exposed to the public eye with the express approval of the person represented,’[[184]](#footnote-184) unless the photo is generally depicting contemporary society[[185]](#footnote-185) or it is of a public figure, that is ‘a figure of contemporary society’, and even then her legitimate interest in privacy may still trump the public interest in the information.[[186]](#footnote-186) 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 Directive a de-referencing request depended on an individual making out ‘*compelling legitimate* grounds relating to his particular situation’,[[187]](#footnote-187) 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 [continued] processing.’[[188]](#footnote-188) So the GDPR 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 on a compelling legitimate basis.

# Conclusion

It is uncanny how the technical regulatory regime of data protection law should so comfortably embody the values of 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 new right to be forgotten in the context of spent convictions as a testing case study of privacy-in-public, the discussion showed its solid standing in the GDPR and CJEU jurisprudence since its inception in *Google Spain*, its outright rejection by the US judiciary against free speech constitutional demands, and its contorted transformation by the ECtHR against Art 8 jurisprudence that has been exposed to both Western cultures of privacy. What is instructive about the case study is not just how the definition of ‘private’ as meaning ‘personal’ rather than ‘personal and confidential’ necessarily opens 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, the behaviours that may not be disentitling, or the competing values that may be triggered. As aligned with the Continental European culture of privacy, data protection constructs the fundamentally vulnerable individual not just in her private setting of the home, but in the public domain of employment, community and polity and extends an entitlement to basic human dignity to those public realms. This also explains why superimposing Art 8 jurisprudence based on 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 when it emerges as a fine example of Continental European privacy culture. Yet, much as Whitman’s cultural approach presents as a detached non-critical assessment of culturally grounded privacy sensibilities, it also invites criticisms of the 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.[[189]](#footnote-189) 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 paper. 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 the Other, that is other economic, legal and cultural orders. Most notably, Article 8 of the ECHR which is traceable to Art 12 of the Universal Declaration and the 4th Amendment of the USConstitution (which in turn reflects English common law on the inviolability of the home) belatedly got a Continental European privacy make-over in response to the refusal of German Constitutional Court (of all courts) to recognise privacy-in-public in the particular case, and this expanded definition then once more made itself back to England, the cradle of its common law understanding. In short, the evolution of privacy regimes is neither linear nor pure – nor over.

1. James Whitman, ’The Two Western Cultures of Privacy: Dignity versus Liberty’ (2004) 113 *Yale Law Journal* 1151; for an engagement with Whitman’s cultural approach, as opposed to a functional approach to comparative methodology, see Special Issue of *The American Journal of Comparative Law* (2017) Vol 65; see esp: James Gordley, ‘Comparison, Law, and Culture: A Response to Pierre Legrand’ (2017) 65 *The American Journal of Comparative Law* 133*;* Peer Zumbansen, ‘Les Jeux Sont Faits: Comparative Law – As It Really Was Meant to Be?’ (2017) 65 *The American Journal of Comparative Law* 237. See also Robert C Post, ‘Three Concepts of Privacy’ (2001) 89 *The Georgetown Law Journal* 2087; Edward J Eberle, *Dignity and Liberty: Constitutional Visions in Germany and the United States* (Praeger 2001); Guy E Carmi, ‘Dignity Versus Liberty: The Two Western Cultures of Free Speech’ (2008) 26 *Boston University International Law Journal* 277; Basil Markesinis, Colm O’Cinneide, Jorg Fedtke, Myriam Hunter-Henin, ‘Concerns and Ideas about the Developing English Law of Privacy (and How Knowledge of Foreign Law Might be of Help)’ (2004) 52 *The American Journal of Comparative Law* 133. [↑](#footnote-ref-1)
2. For reflection on space and privacy, see Irwin Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding* (Brooks/Cole 1975); Mireille Hildebrandt ‘Privacy and Identity’ in Erik Claes, Antony Duff, Serge Gurwirth (eds), *Privacy and the Criminal Law* (Hart 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 Joel Feinberg, ‘Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution’ (1983) 58 *The Notre Dame Law Review* 445. [↑](#footnote-ref-2)
3. Helen 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 three technological capacities: ‘(1) tracking and monitoring, (2) aggregation and analysis, and (3) dissemination and publication.’ [↑](#footnote-ref-3)
4. J D Lasica, ‘The Net never forgets’ (*Salon*, 26 November 1998) < https://www.salon.com/1998/11/25/feature\_253/> [↑](#footnote-ref-4)
5. Jeffrey Rosen, ‘The Web Means the End of Forgetting’ *The New York Times* (21 July 2010,); Jeffrey Rosen, ‘The Purposes of Privacy: A Response’ (2001) 89 *Georgetown Law Journal* 2117. [↑](#footnote-ref-5)
6. Viktor Mayer Schönberger, *Delete: the Virtues of Forgetting in the Digital Age* (Princeton University Press, 2009) 99f. [↑](#footnote-ref-6)
7. *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* C-131/12 (CJEU, GC, 13 May 2014, ECLI:EU:C:2014:317). [↑](#footnote-ref-7)
8. Art 17 of the 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. [↑](#footnote-ref-8)
9. *Google Spain* (n 7) para 93. [↑](#footnote-ref-9)
10. European Council, ‘Council Resolution on Encryption – Security through encryption and security despite encryption’ (Brussels, 24 November 2020, 13084/1/20). [↑](#footnote-ref-10)
11. *Big Brother Watch and Others v United Kingdom* [2021] ECHR 165; in contrast to earlier authority that insisted on targeted surveillance based on ‘reasonable suspicion’ e.g. *Weber and Saravia v Germany* [2006] ECHR 1173; *Liberty and Others v United Kingdom* [2008] ECHR 568; *Kennedy v United Kingdom* [2010] ECHR 682. [↑](#footnote-ref-11)
12. *Big Brother Watch* (n 9)para 348-350 (majority judgment). [↑](#footnote-ref-12)
13. ibid para 22 (partly dissenting judgment by Pinto de Albuquerque). [↑](#footnote-ref-13)
14. La Quadrature du Net and Other v France C-511/18, C-512/18 (CJEU, GC, 6 October 2020, ECLI:EU:C:2020:791). [↑](#footnote-ref-14)
15. Privacy International v. United Kingdom C-623/17 (CJEU, GC, 6 October 2020, ECLI:EU:C:2020:790). [↑](#footnote-ref-15)
16. Art 7 (privacy), Art 8 (data protection) and Art 11 (freedom of expression) of the Charter of Fundamental Rights of the European Union (OJ C 326, 26 October 2012). [↑](#footnote-ref-16)
17. La Quadrature du Net and Other (n 12) para 134-139, specifically para 135; contrast to Tele2 Sverige and Watson and Others C-203/15 and C-698/15 (CJEU, GC, 21 December 2016, ECLI:EU:C:2016:970). [↑](#footnote-ref-17)
18. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015 114-23, 2 June 2015; see *United States v Moalin* (9th Cir SD Cal, 2 September 2020). [↑](#footnote-ref-18)
19. Daniel Solove, ‘’I’ve got Nothing to Hide’ and Other Misunderstandings of Privacy’ (2007) 44 *San Diego Law Review* 745, 768, discussing the structural shifts and power imbalances that occur as a result of surveillance. [↑](#footnote-ref-19)
20. Council of Europe, *Guide on Article 8 of the European Convention on Human Rights* (Updated 31 August 2020,) [↑](#footnote-ref-20)
21. Ferdinand Schoeman, ’Privacy: Philosophical Dimensions’ (1984) 21 *American Philosophical Quarterly* 199. [↑](#footnote-ref-21)
22. Whitman (n 1), 1160, see also Post and Eberle (n 1), whose comparative analysis based on dignity and liberty preceded Whitman. [↑](#footnote-ref-22)
23. For a comprehensive empirical study of the histories of privacy recognition of EU Member States, see David Erdos, ‘Comparing Constitutional Privacy and Data Protection Rights within the EU’ (2022) 47 *European Law Review* 482. [↑](#footnote-ref-23)
24. *Semayne's Case* (1604) 5 Co Rep 91a, 77 Eng Rep 194. [↑](#footnote-ref-24)
25. As discussed in *Wilson v Arkansas* 514 US 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.”’ [↑](#footnote-ref-25)
26. *Semayne's Case* (n 26) 195. [↑](#footnote-ref-26)
27. Belatedly, the *Semayne’s Case* has been linked to Art 8 ECHR (privacy) in, for example, *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 of long-standing in many Continental European jurisdiction. [↑](#footnote-ref-27)
28. *Katz v United States* 389 US 347, 361 (1967). [↑](#footnote-ref-28)
29. William 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 US 479 (1965) which recognises an implicit right to privacy in the US constitution, here applied to the use of contraception by a couple, and *Roe v Wade* 410 US 113 (1973) (concerning the right to abortion). [↑](#footnote-ref-29)
30. Gavin Phillipson, ‘Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act’ (2003) 66 *Modern Law Review* 726, 733. [↑](#footnote-ref-30)
31. Raymond Wacks, ‘The Poverty of Privacy’ (1980) 96 *Law Quarterly Review* 73; Julie C Innes*, Privacy, Intimacy, and Isolation* (OUP 1992). [↑](#footnote-ref-31)
32. Samuel D Warren, Louis D Brandeis, ‘The Right to Privacy’ (1890) 4 *Harvard Law Review* 193. [↑](#footnote-ref-32)
33. This traditional position has changed in a number of common law jurisdictions, including England and Wales in *Campbell v MGN Ltd* [2004] UKHL 22 (6 May 2004); see also Canada in *Les Editions Vice Versa Inc v Aubry* [1999] BHRC 437. [↑](#footnote-ref-33)
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.’ [↑](#footnote-ref-34)
35. *Semayne's Case* (n 26) 197. [↑](#footnote-ref-35)
36. In Henry Brougham, Historical Sketches of Statesmen who Flourished in the Time of George III (First Series, C.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, e.g. search warrants. [↑](#footnote-ref-36)
37. *Boyd v United States* 116 US 616 (1886). [↑](#footnote-ref-37)
38. ibid. [↑](#footnote-ref-38)
39. Whitman (n 1) 1212. [↑](#footnote-ref-39)
40. ibid 1212f. [↑](#footnote-ref-40)
41. ibid 1161, 1189ff; see also Joseph Kohler, *Das Eigenbild im Recht* (J Guttentag 1903);Warren and Brandeis (n 36). [↑](#footnote-ref-41)
42. Kohler ibid, 10 [translation by author]. [↑](#footnote-ref-42)
43. Typically, see Art 2(1) of the German Basic Law on the right to free development of one’s personality, which includes as part of right to personal dignity (Art1(1)) the right to control the use of one’s image or word e.g. in a news story. Wolfgang 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). [↑](#footnote-ref-43)
44. Recognised in Germany 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 Gerrit Hornung, Christoph Schnabel, ‘Data Protection in Germany I: the Population Census Decision and the Right to Informational Self-Determination’ (2009) 25 *Computer Law & Security Review* 84. For Anglophone privacy theorists who define privacy as informational self-determination, control or autonomy, see Alan Westin, *Privacy and Freedom* (Athenum 1967); Charles Fried, ‘Privacy’ (1968) 77 *Yale Law Journal* 475, 482; Phillipson (n 34) 73; Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP 2014). More generally, on different theories: Schoeman (n 20); Nissenbaum (n 3) 69ff; Helen Fenwick, Gavin Phillipson, *Media Freedom under the Human Rights Act* (OUP 2006) 662ff. [↑](#footnote-ref-44)
45. Ute Frevert, *The Politics of Humiliation: A Modern History* (OUP 2020). [↑](#footnote-ref-45)
46. Ute Frevert, ‘The history of humiliation points to the future of human dignity’ (*Psyche*, 20 January 2021) commenting on her book Frevert (n 49). [↑](#footnote-ref-46)
47. Whitman (n 1) 1164f. [↑](#footnote-ref-47)
48. Niall R Whitty, ‘Overview of Rights of Personality in Scots Law’ in Niall R Whitty, Reinhard Zimmermann (eds), *Rights of Personality in Scots Law: A Comparative Perspective* (DUP 2009) 147, 151ff, 162ff. [↑](#footnote-ref-48)
49. Whitman (n 1) 1166 [emphasis in the original]. [↑](#footnote-ref-49)
50. Lord Hoffman, ‘Mind Your Own Business’ (Goodman Lecture, 22 May 1996, unpublished) cited in Fenwick (n 48) 663 [emphasis added]. [↑](#footnote-ref-50)
51. Whitman (n 1) 1161. [↑](#footnote-ref-51)
52. Frevert (n 49). [↑](#footnote-ref-52)
53. Post (n 1) 2095. [↑](#footnote-ref-53)
54. ibid. [↑](#footnote-ref-54)
55. Whitman (n 1) 1182; see also Whitty (n 52) 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 Immanuel Kant, *Groundwork of the Metaphysics of Morals* (1785, translated and edited by Mary Gregor, Jens Timmermann, CUP 1998, revised 2012) 57: ‘thus a free will and a will under moral laws are one and the same.’ [↑](#footnote-ref-55)
56. Whitman (n 1) 1181 [emphasis omitted]. [↑](#footnote-ref-56)
57. Whitty (n 52) 161, referring to the different levels at which ‘dignity’ can be defined. [↑](#footnote-ref-57)
58. The value of dignity has exceptionally surfaced in the American jurisprudence in the practice of perp walks, see e.g. *Lauro v Charles* 219 F3d 202 (2d Cir. 2000) where it was held that public 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. [↑](#footnote-ref-58)
59. See e.g. accounts that ground the right to informational self-determination ‘in the interest of the public, to guarantee a free and democratic communication order.’ Hornung (n 44) 86; or accounts of privacy and freedom of expression being mutually supportive e.g. Fenwick (n 48) 686. [↑](#footnote-ref-59)
60. Whitman (n 1) 1176. [↑](#footnote-ref-60)
61. Post (n 1) 2095. [↑](#footnote-ref-61)
62. Frevert (n 49) 13. [↑](#footnote-ref-62)
63. See literature on the related topic of identity, or the right to identity, e.g. Hildebrandt (n 2); Serge Gutwirth, “Beyond identity?” (2008) 1 IDIS - Identity in the Information Society 123 1, 1; Paul De Hert, *A right to identity to face the Internet of Things* (Council of Europe Publishing, 2007). [↑](#footnote-ref-63)
64. Whitman (n 1) 1163. [↑](#footnote-ref-64)
65. Feinberg (n 2) 483ff, commenting on the judicial interpretation of the US Bill of Rights in *Griswold v Connecticut* 381 US 479 (1965) speaking of ‘zones of privacy’ which denote zones of individual discretion. [↑](#footnote-ref-65)
66. Whitman (n 1) 1182. [↑](#footnote-ref-66)
67. However, note 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 sphere (thus somewhat reflecting the private/public dichotomy): Markesinis (n 1) 188ff. [↑](#footnote-ref-67)
68. Eric Barendt,’”A Reasonable Expectation pf Privacy”: a Coherent or Redundant Concept?’ in Andrew T Kenyon (ed) *Comparative Defamation and Privacy Law* (CUP 2016) 96, 111. [↑](#footnote-ref-68)
69. *The Queen v Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher, Case* C-369/98 (Opinion of AG Alber ) para 41. [↑](#footnote-ref-69)
70. G Gonzalez Fuster, Serge Gutwirth, ‘Opening up personal data protection: a conceptual controversy’ (2013) 29 *Computer Law & Security Review* 531. [↑](#footnote-ref-70)
71. *Census Case* (n 48); see further Douwe Korff, Marie Georges, ‘The Origins and Meaning of Data Protection’ (SSRN, 13 January 2020). [↑](#footnote-ref-71)
72. Paul De Hert, Serge Gutwirth, ‘Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action’ in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, Sjaak Nouwteds (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 (ETS No 108, 28 January 1981) in response to the perceived limitations of Art 8 (the definition of ‘private life’ and the vertical nature of the protection) in the early 1970s. [↑](#footnote-ref-72)
73. Whilst the GDPR requires the balancing of rights held by ‘private’ actors and public interests, including public health, national security and law enforcement, this in fact is consistent with the Continental tradition in so far as privacy is asserted against private actors, and not just against the State. [↑](#footnote-ref-73)
74. Contrast to English law, e.g. *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 Art 8 (discussed below) and was also endorsed by the CJEU, for example, in *In Joined Cases* C-465/00, C-138/01 and C-139/01 (CJEU, 20 May 2003, ECLI:EU:C:2003:294) para 74-75. See also discussion in Markesinis (n 1) 162ff. [↑](#footnote-ref-74)
75. Note some types of sensitive personal data under the GDPR are data that would traditionally be considered private and thus confidential e.g. ‘data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.’ [↑](#footnote-ref-75)
76. Art 9 of the GDPR, formerly Art 8 of the European Parliament and Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31 [hereafter Data Protection Directive]. [↑](#footnote-ref-76)
77. Art 9(1) of the GDPR. [↑](#footnote-ref-77)
78. Cf De Hert (n 77) 6, 10. [↑](#footnote-ref-78)
79. The ‘purpose limitation principle’ – see Art 5(1)(b) of the GDPR but note as ‘purpose limitation’ is a central concept in data protection law, it appears with high frequency in the Regulation. [↑](#footnote-ref-79)
80. *Google Spain* (n 7). [↑](#footnote-ref-80)
81. Art 14 and Art 12(b) of the Data Protection Directive 95/46/EC. [↑](#footnote-ref-81)
82. *Google Spain* (n 7) para 36. [↑](#footnote-ref-82)
83. ibid para 85-87. [↑](#footnote-ref-83)
84. Google, *Google’s Transparency Report* (accessed August 2021) <<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. [↑](#footnote-ref-84)
85. Sylvia Tippman, Julia Powles, ‘Google has accidentally revealed detailed information of nearly 220,000 ‘right to be forgotten’ requests’ *The Guardian* (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.’ [↑](#footnote-ref-85)
86. The social aspect of privacy has been acknowledged, for example, in *Botta v Italy* (1998) 26 EHRR 241, para 32, referring to ‘the development, without outside interference, of the personality of each individual in his relations with other human beings.’ [↑](#footnote-ref-86)
87. JC Buitelaar, ‘Post-mortem Privacy and information self-determination’ (2017) 19 *Ethics Information Technology* 129, 137; see also Feinberg (n 2) 478; Derek Parfit, 'Later selves and moral principles' in Alan Montefiore (ed), Philosophy and personal relations: an French Study (Routledge & Kegan Paul 1973) 137ff. [↑](#footnote-ref-87)
88. For example, in the UK Rehabilitation of Offender Act 1974. Note, in the UK the effect of rehabilitation in terms of the right to be forgotten is limited, partly, by virtue that not all offences fall within the remit of the Act and partly, by virtue of 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 [2015] AC 49, para 18: ‘the point at which a conviction … recedes into the past and becomes part of a 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.’ [↑](#footnote-ref-88)
89. For similar earlier domestic provisions, see *Segerstedt-Wiberg and Others v Sweden*, no. 62332/00, ECHR 2006-VII) and *Österreichischer Rundfunk v Austria* (ECtHR, No 35841/02, 7 December 2006). The latter case concerned s.7a of the Media Act (Austria): ‘Where publication is made, through any medium, of a name, image or other particulars which are likely to lead to the disclosure to a larger not directly informed circle of people of the identity of a person who… has been the victim of an offence punishable by the courts … and where the legitimate interests of that person [i.e. an interference with the victim's strictly private life or to his or her exposure] are thereby harmed and there is no predominant public interest in the publication of such details on account of the person's position in society, of some other connection with public life, or of other reasons, the victim shall have a claim against the owner of the medium (publisher) for damages for the injury suffered.’ [↑](#footnote-ref-89)
90. GC, AF, BH, and ED v Commission Nationale de l’Informatique et des Libertes (CNIL), Premier ministre, and Google LLC C-136/17 (GC, 24 September 2019, ECLI:EU:C:2019:773) [↑](#footnote-ref-90)
91. Art 9 of the GDPR which prohibits processing unless one of the exceptions, such as express consent and another legitimate-interest alternative, is satisfied. [↑](#footnote-ref-91)
92. *GC and Ors* (n 95) para 25-28. [↑](#footnote-ref-92)
93. *GC and Ors* (n 95) para 53, 66; *Google Spain* (n 7) para 81, 97. See also Stephan Kulk, Frederic Borgesius, ‘Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe’ in E Selinger, J Polonetsky, 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. [↑](#footnote-ref-93)
94. *GC and Ors* (n 95) para 66, see also 67, noting the strengthened privacy interests in the case of sensitive personal data. [↑](#footnote-ref-94)
95. *Google Spain* (n 7) para 81; now Art 17(3)(a) of the GDPR. [↑](#footnote-ref-95)
96. *GC and Ors* (n 95) para 36; *Google Spain* (n 7) para 35-37. [↑](#footnote-ref-96)
97. *GC and Ors* (n 95) para 66. [↑](#footnote-ref-97)
98. Art 8(2)(e) of Data Protection Directive and Art 9(2)(e) of GDPR; *GC and Ors (n 91)* para 63. Information Commissioner’s Office, *Guide to the General Data Protection Regulation (GDPR*) *- Special Category Data* (1 January 2021, 1.1.139, <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/>>): ‘[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.’ [↑](#footnote-ref-98)
99. *GC and Ors* (n 95) para 69: a search 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* unless the data subject has the right under Article 14(a) of the directive to object to that processing on compelling legitimate grounds relating to his particular situation.’ [emphasis added] [↑](#footnote-ref-99)
100. *GC and Ors* (n 95) para 77. [↑](#footnote-ref-100)
101. Art 29 Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on “Google Spain and Inc v. Agencia Espanola de Proteccion de Data (AEPD) and Mario Costeja Gonzalez” 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.’ [↑](#footnote-ref-101)
102. Ruth Gavinson, ‘Privacy and the Limits of the Law’ (1980) 89 *Yale Law Journal* 421, 438 [emphasis in the original]. See also Stephen Gardbaum, ‘The “Horizontal Effect” of Constitutional Rights’ (2003) 102 *Michigan Law Review* 387. [↑](#footnote-ref-102)
103. Daniel J Solove, Neil M Richards, ‘Privacy’s Other Path: Recovering the Law of Confidentiality’ (2007) 96 *Georgetown Law Journal* 123. [↑](#footnote-ref-103)
104. William L Prosser, 'Privacy' (1960) 48 *California Law Review* 383, 389; see also Neil M Richards, Daniel J Solove, ‘Prosser’s Privacy Law: A Mixed Legacy’ (2010) 98 *California Law Review* 1887. For its continued relevance, see e.g. Amy Gajda, ‘Privacy and the Right to Be Let Alone’ in William R Davie, T Michael Maher (eds), *First Amendment Law in Louisiana* (University of Louisiana Press, 2015) [↑](#footnote-ref-104)
105. Warren and Brandeis (n 36). [↑](#footnote-ref-105)
106. When Prosser constructed this category as 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, the Supreme Court’s reluctance to restrain truthful (personal) information had not yet materialised. See also Nissenbaum (n 3) 103ff (on privacy in public). [↑](#footnote-ref-106)
107. Prosser (n 104) 394f [internal notes omitted; emphasis added]. [↑](#footnote-ref-107)
108. ibid 396 [internal notes omitted]. [↑](#footnote-ref-108)
109. Discussed further below. [↑](#footnote-ref-109)
110. Prosser (n 104) 396. The test has also been adopted in Australia: *Australian Broadcasting Corporation v Lenah Game Meats* (2001) 208 CLR 199, para 42: ‘highly offensive to a reasonable person of ordinary sensibilities’; contrast to the position in England and Wales: *Campbell v MGN Ltd* (n 37) para 121, 135, but 94-96; discussed in Barendt (n 73) 98ff. [↑](#footnote-ref-110)
111. *Briscoe v Reader's Digest Association* 4 Cal 3d 532 (1971); see also *Melvin v Reid* 112 Cal App 285, 297 Pac 91 (1931). [↑](#footnote-ref-111)
112. *Gates v Discovery Communications Inc* 34 Cal 4th 679 (2004). [↑](#footnote-ref-112)
113. *Cox Broadcasting Corp v Cohn* 420 US 469 (1975); *Oklahoma Publishing Co v District Court* 430 US 308 (1975); *Smith v Daily Mail Publishing Co* 443 US 97 (1979); *The Florida Star v BJF* 491 US 524 (1989). These cases all concerned the identities of the victims of a crime, rather than that of the offender. [↑](#footnote-ref-113)
114. *Bartnicki v Vopper* 532 US 514 (2001). [↑](#footnote-ref-114)
115. *Cox Broadcasting Corp v Cohn* 420 US 469 (1975). [↑](#footnote-ref-115)
116. ibid 494f. [↑](#footnote-ref-116)
117. *Smith v Daily Mail Publishing Co* 443 US 97, 103 (1979) summarising *Oklahoma Publishing Co v District Court* 430 US 308 (1975), approved in *The Florida Star v BJF* 491 US 524, 535 (1989). [↑](#footnote-ref-117)
118. *Gates v Discovery Communications Inc* 34 Cal 4th 679 (2004). See also Eberle (n 1) 191f describes 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 US 652 (1925). Note too the curtailing of defamation claims by public officials in *New York Times Co v Sullivan* 376 US 254 (1964). [↑](#footnote-ref-118)
119. Prosser (n 104) 396f. [↑](#footnote-ref-119)
120. See discussion below on the disentitling effect of such self-help actions under Art 8 ECHR. [↑](#footnote-ref-120)
121. Virginia Dressler, ‘Google Quietly Rolls Out the Right to be Forgotten mechanism in the US’ (14 June 2022) *Office for Intellectual Freedom of the American Library Association* <<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. [↑](#footnote-ref-121)
122. ML and WW v Germany [2018] ECHR 554. [↑](#footnote-ref-122)
123. NT1 & NT2 v Google LLC *(The Information Commissioner intervening)* [2018] EWHC 799 (QB); for other recent cases on public disclosure of spent convictions, see *Hayden v Duckworth* [2021] EWHC 1033 (QB); *Hayden v Dickenson* [2020] EWHC 3291 (QB). [↑](#footnote-ref-123)
124. Juliane Kokott, Christoph Sobotta, ‘The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR’ (2013) 3(4) *International Data Privacy Law* 222; De Hert (n 77) 3. An arguably preferable approach to their relationship has been taken in the EU Charter of Fundamental Rights where privacy and data protection exist slide by side as distinct and independent rights in Art 7 (privacy) and Art 8 (data protection). [↑](#footnote-ref-124)
125. *ML & WW* (n 128) para 97, acknowledging the difference. [↑](#footnote-ref-125)
126. Oliver Diggelmann, Maria Nicole Cleis, ‘How the Right to privacy Became a Human Right’ (2014) 14 *Human Rights Review* 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). [↑](#footnote-ref-126)
127. Ibid 445. [↑](#footnote-ref-127)
128. Ibid 446, 449. ‘The Statement of Essential Human Rights’ (1945) itself was drafted by a multi-national committee (with a strong US presence i.e. 12 out of 25 members) and included Art 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.’ [↑](#footnote-ref-128)
129. See, for example, the Greek Constitution of 1911: Art 3 The Greeks are equal in the eye of the law and contribute without distinction to the public burdens according to their ability; Art 12 The dwelling is inviolable; Art 20 The secrecy of letters is absolutely inviolable; the Weimar Constitution of 1919 (Germany): Art 109 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 115 The home of every German is his sanctuary and is inviolable...; Art 117 The secrecy of letters and all postal, telegraph, and telephone communications is inviolable… [↑](#footnote-ref-129)
130. Ed Bates, *The Evolution of the European Convention on Human Rights* (OUP 2010) 5ff. [↑](#footnote-ref-130)
131. *Von Hannover v Germany* 59320/00 [2004] ECHR 294 (24 June 2004); discussed in NA Moreham, ‘Privacy in public places’ (2006) 65(3) *The Cambridge Law Journal* 606; Fenwick (n 48) 671ff. For important forerunners, see *Peck v the United Kingdom* App No 44647/98 [2003] ECHR 44; *PG and JH v United Kingdom* App No 44787/98 [2001] ECHR 550. For subsequent decisions on the positive obligations of States to guard against horizontal violations, see, *KU v Finland* App No 2872/02 [2008] ECHR, para 42-51; *Ageyevy v Russia* App No 7075/10 [2013] ECHR 346, para 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.’ [↑](#footnote-ref-131)
132. *Von Hannover v Germany* (n 133) [emphasis added]. [↑](#footnote-ref-132)
133. *Von Hannover v Germany* (n 133) para 57, citing in support: *X and Y v the Netherlands - 8978/80* [1985] ECHR 4, para 23; *Stjerna v Finland -18131/91* [1994] ECHR 43, para 38; *Verliere v Switzerland* - *41953/98* [2001] ECHR 2001-VII. [↑](#footnote-ref-133)
134. Meaning an ‘absolute public figure’, see *Von Hannover v Germany* (n 133ko) para 19, 23, 25. [↑](#footnote-ref-134)
135. See quote (n 130) (excerpted from *Von Hannover v Germany* (n 135)), one might query whether ‘back’ is the appropriate term in case of Art 8. 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 (n 48) 674; Markesinis (n 1) 146f, 185ff. [↑](#footnote-ref-135)
136. Based on Art 8 and 10 the ECHR; and the duty imposed by the Human Rights Act 1998 that public authority must act compatibly with both parties' Convention rights, and in the case of courts interpret the law consistently with Convention Rights. [↑](#footnote-ref-136)
137. *Campbell v MGN Ltd* (n 37) 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.’ [↑](#footnote-ref-137)
138. Phillipson (n 30) 735ff. [↑](#footnote-ref-138)
139. *Z* v *Finland* (1998) 25 EHRR 371, para 95-97; *Rotaru v Romania* *28341/95* [2000] ECHR 192, para 43; *Amann v Switzerland* 27798/95 [2000] ECHR 88, para 65. [↑](#footnote-ref-139)
140. Kokott (n 124) 224. [↑](#footnote-ref-140)
141. *MM v United Kingdom 24029/07* [2012] ECHR 1906, para 188, discussed in Kokott (n 124) 224; see also *Rotaru v Romania* (n 141): ‘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.’ [↑](#footnote-ref-141)
142. NT1 & NT2 (n 129) para 140 [emphasis added], see also para 170. [↑](#footnote-ref-142)
143. Art 2(a) of the Data Protection Directive, and now Art 4(1) of the GDPR. [↑](#footnote-ref-143)
144. While Art 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 141); *Amann v Switzerland* (n 137). For the significant body of ECtHR jurisprudence of privacy entitlements in respect of professional and business activities, see Guide on Art 8 (n 20) 23ff. [↑](#footnote-ref-144)
145. ML & WW (n 128) para 88 [emphasis added] [↑](#footnote-ref-145)
146. NT1 & NT2 (n 129) para 154-55, 167; in relation to NT2, the balance was 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 para 224, 226]. [↑](#footnote-ref-146)
147. *Volker und Markus Schecke and Eifert Joined Cases C–92/09 and C–93/09* (CJEU, GC, 9 November 2010, ECLI:EU:C:2010:662) para 59: ‘It is of no relevance in this respect that the data published concerns activities of a professional nature…’ [↑](#footnote-ref-147)
148. *Google Spain* (n 7). [↑](#footnote-ref-148)
149. *GC and Ors* (n 95) para 77. [↑](#footnote-ref-149)
150. *In re JR 38* [2015] UKSC 42 contrast majority and minority judgement; discussed in Joe Purshouse, ‘The Reasonable Expectation of Privacy and Criminal Suspect’ (2016) 79(5) *Modern Law Review* 871 commenting that the ECtHR has not used the test as a touchstone test; see also Barendt (n 73) 104. [↑](#footnote-ref-150)
151. *Katz v United States* (n 32). [↑](#footnote-ref-151)
152. Australia: *Australian Broadcasting Corporation v Lenah Game Meats* (n 116) (‘highly offensive to a reasonable person of ordinary sensibilities’ para 42); New Zealand: *Hosking v Runting* [2005] 1 NZLR1; England and Wales: *Campbell v MGN Ltd* (n 37) para 21 (Lord Nicholls): ‘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 73), critiques the test as artificial and importing ‘free speech’ interests both at the first and second stage of the privacy analysis. [↑](#footnote-ref-152)
153. Barendt (n 73) 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. [↑](#footnote-ref-153)
154. *Katz v United States* (n 32). [↑](#footnote-ref-154)
155. In English jurisprudence the test has been used at the second of a three-stage approach to Art 8 - after deciding whether the alleged Art 8 intrusion is serious enough, and before determining whether it is outweighed by other (public) interests; see *R (Wood) v Commissioner of Police of the Metropolis* [2010] 1 WLR 123, 136. Both Barendt (n 71) 102f, and Purshouse (n 154) 881, persuasively argue that the test should, if at all, only figure at that third/balancing stage. [↑](#footnote-ref-155)
156. ML & WW (n 128) para 109. [↑](#footnote-ref-156)
157. NT1 & NT2 (n 129) para 125, 130, 168 and 170. [↑](#footnote-ref-157)
158. ibid para 168. [↑](#footnote-ref-158)
159. ibid para 130, where Warby J somewhat acknowledges the unfairness of the position. See also *In re JR3* [2015] UKSC 42 where the UK Supreme Court unanimously dismissed the appeal of a 14-year-old minor that the publication of his image taken by police during a sectarian riot, violated his Art 8 entitlement, with a majority holding that Art 8 was not engaged, discussed in Purshouse (n 154). [↑](#footnote-ref-159)
160. NT1 & NT2 (n 129) para 170 [emphasis added]. [↑](#footnote-ref-160)
161. The GDPR 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. [↑](#footnote-ref-161)
162. In *GC and Ors* (n 95), 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. [↑](#footnote-ref-162)
163. For an obvious example, see *Peck v UK* [2003] EMLR 15 (where CCTV footage that included the applicant and was collected by the council was later passed on to the media for a *Crime Beat* programme). [↑](#footnote-ref-163)
164. Nissenbaum (n 3). [↑](#footnote-ref-164)
165. On consent, especially Art 6(1)(a), 7, 9(2)(a) of the GDPR, see Chapter III of the GDPR on data subject rights. [↑](#footnote-ref-165)
166. As supported by some common law privacy lawyers, e.g. Moreham (n 135) 617ff. [↑](#footnote-ref-166)
167. Fenwick (n 44) 663, citing with approval WA Parent, ‘A New Definition of Privacy for the Law’ (1983) 2 *Law and Philosophy* 305, 306f [emphasis added]. [↑](#footnote-ref-167)
168. *Axel Springer AG v Germany 39954/08* [2012] ECHR 227, para 83; cited with approval in *ML & WW* (n 128) para 88; *N1 & N2* (n 129) para 111. However, see also *Sciacca v Italy* *50774/99* (2006) 43 EHRR 20, para 29, where the ECtHR noted that the fact that the applicant was subject to criminal proceedings cannot curtail the scope of Art 8. [↑](#footnote-ref-168)
169. *Daily Times Democrat v Graham* 162 So 2d 474 (1964). [↑](#footnote-ref-169)
170. For a critique, see Gavin Phillipson, ‘Press Freedom, the Public Interest and Privacy’ in Andrew Kenyon (ed), *Comparative Defamation and Privacy Law* (CUP 2016) 136, 150. See also Lloyd L Weinreb, ‘The Right to Privacy’ (2009) 17 *Social Philosophy & 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]. [↑](#footnote-ref-170)
171. *ML & WW* (n 128) para 88. [↑](#footnote-ref-171)
172. *N1 & N2* (n 129) para 110-113; Schedule 3, Condition 5 of the Data Protection Act 1998, following *Townsend v Google Inc* [2017] NIQB 81. Art 8(2)(e) of the Data Protection Directive (upon which Condition 5 is based) refers to ‘*manifestly* made public by the data subject’ [emphasis added]. [↑](#footnote-ref-172)
173. *Townsend v Google Inc & Anor* [2017] NIQB 81. [↑](#footnote-ref-173)
174. ibid para 62; *N1 & N2* (n 129) para 110. [↑](#footnote-ref-174)
175. *N1 & N2* (n 129) para 113, where Warby J had to gloss over the wording of ‘manifestly made public by the data subject’ in the Directive. [↑](#footnote-ref-175)
176. *GC and Ors* (n 95), see n 98 – is also a cross reference to GC and Ors and accompanying text – maybe spell out/repeat? Cross reference to a cross reference is unclear…. [↑](#footnote-ref-176)
177. Frederick Schauer, ‘The Exceptional First Amendment’ (2005) *KSG Working Paper No RWP05-021* 1, 20ff (‘as a manifestation of the strong libertarian and individualistic aspects of American society itself’). [↑](#footnote-ref-177)
178. NT1 & NT2 (n 129) para 133. [↑](#footnote-ref-178)
179. Fiona Brimblecome, Gavin P Phillipson, ‘Regaining Digital Privacy? The New “Right to be Forgotten” and Online Expression’ (2018) 4 *Canadian Journal of Comparative and Contemporary Law* 1. [↑](#footnote-ref-179)
180. *Axel Springer AG v Germany* (n 170) para 87; *Von Hannover v Germany (No 2) 40660/08* [2012] ECHR 228, para 106; Mityanin and Leonov v Russia 11436/06 [2019] ECHR 327, para 108; followed in NT1 & NT2 (n 129) para 132f. [↑](#footnote-ref-180)
181. Markesinis (n 1) 155. [↑](#footnote-ref-181)
182. ibid. [↑](#footnote-ref-182)
183. Carmi (n 1) 334ff; Ronald J 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 *Tulane Law Review* 1549, 1581ff. [↑](#footnote-ref-183)
184. Section 22 of the German Copyright Act, discussed in *Von Hannover v Germany* (n 135). [↑](#footnote-ref-184)
185. Under s 23(1) of the same Act, the publication of pictures portraying aspects of contemporary society are exempted from the obligation to obtain the consent of the person concerned within the meaning of s 22. [↑](#footnote-ref-185)
186. ibid referring to s 23(2) of the German Copyright Act. See also comparative discussion of ‘public figures’ in Markesinis (n 1) 144ff. [↑](#footnote-ref-186)
187. Art 14(a) of the Data Protection Directive. [↑](#footnote-ref-187)
188. Art 21(1), Art 17(1)(c) of the GDPR. [↑](#footnote-ref-188)
189. Zumbansen (n 1) 252f. [↑](#footnote-ref-189)