An enquiry into the scope of the right to be forgotten under Article 17 of the General Data Protection Regulation 2016/2769: A right to erasure or an entitlement to informational self-determination?

Doctor of Philosophy (PhD)

Faculty of Law

University of Reading

Evelyn Patricia Kirkwood

March 2021

Research Question

To what extent does the right to be forgotten as recognized in the Google Spain case and codified in Article 17 of the General Data Protection Regulation provide for an individual to determine how to portray themselves online ?

Acknowledgements

To my incredible supervisor Stavroula Karapapa whose endless patience and encouragement was vital, whose support made this possible;

To my second supervisor Rosa Freedman for her wise words and insightful input;

To my colleague Zoi Krokida whose friendship and encouragement was so important on this journey together;

To the wonderful teams at the University of Reading, both at the School of Law and the Graduate School;

To Dr Jane Ward for her help in proof -reading the final draft of my thesis;

To all my friends and family who were so bewildered by this strange desire of mine to study (what at your age ?!) but were always there if I needed them;

Finally to my incredible husband who not only saw my need to do this but was able to support me in every step I took, not forgetting my endlessly forgiving children Josh and Shannon who were constantly neglected whilst I pursued my research.

'You have been in every line I have ever read' …….and written
'Great Expectations' -Charles Dickens

My very grateful thanks and appreciation for all your invaluable support

ABSTRACT

To many a key question now is how can you control how to portray yourself online ? Increasingly availability of information linked to an individual can create an everlasting digital memory which may not be acceptable to you. Awareness of loss of privacy due to the increasing flow of personal data has newly focused concern on the accessibility and retention of personal data. In line with the fundamental right of data protection, the General Data Protection Regulation (GDPR), following a seminal ruling of the Court of Justice in *Google Spain v Gonzalez*, recognized a new right for individuals to have personal data erased. Here the Court of Justice of the European Union interpreted the Data Protection Directive (DPD) in light of the European Charter of Human Rights, finding that a right to be forgotten existed, thus enabling Senor Gonzalez to de-link information. This right was ultimately formalized within the EU through implementation of Article 17 of the GDPR.

Much literature exists examining the status of the right to be forgotten, however this thesis argues that the scope of the right is wider than debated, revealing its true importance in informational self-determination. The court's decision created what was declared to be a new right not only with origins in applying data protection through Articles 12 and 14 of the DPD to support privacy but also evoking rights of dignity and reputation. This provides for an individual to control access and availability to personal data, ultimately creating an option to determine how they are portrayed on the Internet. The potential for Informational self-determination to be exercised through this right could provide an unprecedented ability for an individual to use it portray themselves as they may so determine.

By examining the historical underpinnings of human rights ultimately leading to the fundamental right of data protection, the importance of the Google Spain case, prior to article 17 and subsequent significant EU case law, this thesis aims to contribute to an analysis of the wider scope and use of the right to be forgotten. It draws on normative reviews and positivist conclusions towards arguments that this new right can be considered to provide this new form of informational self-determination and specifically to enable an individual to determine how they are portrayed online. This use then supports not only privacy but dignity and

reputation, enabling rehabilitation into a society where past events no longer have relevance in the portrayal of an individual through the Internet.

TABLE OF CONTENTS

Chapter 1- Introduction

1.1 Contextual background

In preceding decades, since the advent of the Internet, the flow and accessibility of personal data with its impact on an individual's life has increased beyond all recognition.[1] This is despite growing awareness[2] of the need for protection of personal data as well as privacy; both being essential in such a changing landscape. For individuals the ability to comprehend the extent that their data is being made available and resultant impact has been slow. Recognition of this impact by the law has struggled to provide necessary solutions to situations where personal data is being misapplied. The requirement to balance the needs of data subjects with the economic benefits of data has been gradually recognized within the EU and increasingly by other states.[3] Within this argument, the issue of how such information can be erased, together with the removal of links to information, has become increasingly important, not least because the holding of such information has created a new phenomenon, that of the digital personality, a virtual self. From initial intentions to control the holding and processing of personal data in electronic format during the 1980s [4] to the current position where the operation of internet based communications, such as social media, is based on the accumulation of an individual's personal details, the key question 'who controls such data?' is now supplemented by considering 'how does it represents who I am ?' The holding of information potentially portrays an individual in a way they have little control over. Control,

[1] 'Almost 4.57 billion people were active internet users as of July 2020, encompassing 59 percent of the global population. China, India and the United States rank ahead all other countries in terms of internet users.' https://www.statista.com/statistics/617136/digital-population-worldwide/

[2] 'Market leader Facebook was the first social network to surpass 1 billion registered accounts and currently sits at more than 2.7 billion monthly active users. Sixth-ranked photo-sharing app Instagram had over 1 billion monthly active accounts.' see https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ last accessed 20 Feb 2021

[3] Despite the US having no federal data protection laws very recent movements have taken place in the US among other countries to develop its own data protection programme, see California Consumer Privacy Act 2018 which law came into effect in January 2020

[4] UK Data Protection Act 1984 c-35 (repealed) The Act included eight principles of data protection including 1. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully and 2. Personal data shall be held only for one or more specified and lawful purposes. In addition, more relevantly it included provision under the 5th principle that Personal data shall be accurate and, where necessary, kept up to date and under 6. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

as such, now rests in the hands of the entities controlling data, and this may not allow an individual to be seen as the person they wish to appear.

How can the subsequent impact on individuals affected by the widespread use and easy availability of such data be considered and managed? It is clearly vital to ensure protection is in place to provide for an individual to be able to control the collection and ultimate accessibility of personal details, or at least influence how they are portrayed through such information.

In Europe, protection of data and personal information has been at the forefront of such developments with initial provisions stretching over several decades. In 1995, a directive[5] was passed forming the first cohesive regulation within the member states, although this still required implementation and interpretation by each such state. The European Commission (EC) subsequently attempted resolution of these issues by proposing a new form of legislation recognizing how changes to the holding and processing of data have taken place over the preceding years. A regulation with direct effect has recently been introduced, namely the General Data Protection Directive (GDPR)[6]. This, after several years of debate and discussions between the member states, was approved on 14 April 2016.[7] The intent behind this is to supersede and develop the coverage of data protection to meet the requirements of a new technological era.

The progressive growth of global entities with the power to control and potentially dominate use of individuals' personal information exemplified by search engines, social media such as Facebook and Instagram, as well as buying conglomerates such as Amazon, has become of increasing concern. As debate has grown,[8] it has become apparent that the fact that 'the

[5] The Data Protection Directive, 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[7] The General Data Protection Regulation became effective on the 25 May 2018. Although this has direct effect it is currently being implemented where necessary by individual member states.

[8] See Mariarosaria Taddeo, Luciano Floridi, 'The Debate on the moral responsibility of Online Service Providers, (2016) 22 Sc &Engineering Ethics, pp 1575,1592

Internet never forgets' concerns many with regard to not only potential loss of privacy but of such closely associated rights of dignity and reputation. This is irrespective of contra debate[9] which argues that this challenge is not a true reflection of the Internet's capabilities. Complicating the situation even further, recognition of the value of such data for both commercial and non-commercial uses means that there has been initial reluctance by both individuals and corporations as well as states to inhibit its flow. The lure of the world of 'Big Data' and its commercial advantages[10] means that those with the resources to do so can oppose any such restrictions to a free flow of data irrespective of individual's desire for change.

Since the decision in the case of Google Spain Sl Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (Google Spain)[11] in 2014 which defined the right to be forgotten, there has been global interest in what has even been termed a new human right.[12] Yet the exact scope of this right as now included in Article 17, GDPR and the extent of protection offered through its exercise has been the subject of much debate by the media, legal commentators and privacy campaigners. For some the right can be argued to have been based primarily on pre-existing rights mirroring these, such as the *Droit a l'oubli* in France[13]

[9] Layal McCay, 'The Internet never forgets; how to live in the 21st Century' (2012) available at; https://www.huffingtonpost.com/dr-layla-mccay/the-internet-never-forgets_b_1460110.html June 30, 2012

[10] 'Even as the contemporary world becomes increasingly digital, and data volumes increase opportunities for exploiting data will grow the percentage of data that would be useful for analysis will rise from 22% to more than 35%. The Worldwide market in big-data technology and services is expected to increase at a compound annual growth rate of about 23% between 2014 and 2019, and worldwide revenue for big data and business analytics has been forecast to increase more than 50% from almost US$ 122 billion in 2015 to more than US $187 billion in 2019. The largest sectors for big data include manufacturing, banking and insurance, government, professional services, tele-communications, health, transport and retail.' Source European Parliament Briefing September 2016, 'Big data and data analytics The potential for innovation and growth,' http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589801/EPRS_BRI(2016)589801_EN.pdf last accessed 8 Jan 2018

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

[12] See for example Andrew Neville, 'Is it a human right to be forgotten? Conceptualising the World view', Santa Clara Journal of Int Law [2017] vol 15 Iss 2 p 157- 172

[13] Although considered an old right it is provided under French Law under Law No. 78-17 *Informatique & Libertés* Law (the law on data processing and liberties): 6 Jan 1978; This states that there is an entitlement to access, alter, correct or delete personal information. It has also been argued that the right exists by virtue of various laws; 'Article 9 of the French Code Civil, Article 7 of the Charter of Fundamental Rights of the European Union, and Article 8 of the European Convention on Human Rights, which all enshrine the right to respect for private life; but also Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data.' see Maryline Boizard, 'The right

and the Italian *Diritto al'oblio.*[14] These national predecessors of Article 17 provided similar rights in limited circumstances primarily connected to the ability to allow fading of the awareness of past events through archiving or removing information, just as human memory fades, particularly regarding 'forgetting' of past misdemeanors. Recognition of such a need was made by several respected commentators focused on the impact of the digital memory.[15] The ability to allow events to fade during the passage of time was highlighted by Victor Mayer Schönberger in his book 'delete'[16] where he debated the necessity of a right to be forgotten to be established in an era of digital memory. He argued that information should be automatically 'forgotten' in line with the ability of human memory. Such a right, which could be applied in parallel with other human rights, could help to maintain fundamental requirements for a human such as dignity, privacy and autonomy. To help this situation, he proposed the equivalent of a 'use by' date to be attached to information which would no longer be available after such date as a solution. At a similar time, the EU was airing its concerns that the existing data protection regime was no longer sufficient to meet new concerns.[17] The UK's Information Commissioner's Office also commissioned a report arguing that existing data protection laws were inadequate to deal with new issues, particularly a lack of clarity with regard to privacy and data.[18]

By the end of 2009, there was a formal announcement by the European Union (EU) recognizing concerns with regard to the retention of personal information or 'data'[19] within its proposal to update existing, but no longer appropriate, data protection rules in recognition

---

to respect for private life: an effective tool in the right to be forgotten?' (2015) 1 Montesquieu Law Review issue 2, available at http://www.montesquieulawreview.eu/review.htm

[14] As early as 1991 reference was made to the existence of such a right by Xavier O'Callaghan Munoz, *Libertad de Expresion Y sus limites, honour intimidad e imagen*: 54 1991: translated to Freedom of expression and its limits, honor, privacy and image: Editorials of Derecho Reunidas, EDERSA

[15] Jeffrey Rosen, 'The Web means the End of Forgetting' [2010] The NY Times, 25 July 2010

[16] Viktor Mayer Schonberger, '*delete, The Virtue of Forgetting in the Digital World*', (Princeton Press, 2009)

[17] The Article 29 Working Party undertook its review in October 2009 looking at various topics following the EU Commission's conference on 'Personal Data -more use more protection ?' available at https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2009/pr_13_10_09_en.pdf last accessed 25 October 2020

[18] The Review of the Data Protection Directive by the ICO in 2009 in the UK was made available at https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf

[19] A report was prepared by the Article 29 Working Party (WP29) and the Working Party on Police and Justice (WPPJ) the "Future of Privacy" paper in response to the invitation for consultation issued by the European Commission on new challenges for personal data protection, see n16 above)

of the longevity and availability of digital information. In 2012, the EU announced its intention to reform the protection offered together proposing the draft regulation[20]. Its intention was to include formally the ability for information to be removed or at least 'forgotten'[21]. However, this concept was not accepted, with debate focusing on the issues that this may have caused, not only to the free flow of data seen as crucial to economic activities, but to freedom of expression.[22]

Following increased interest in the necessity of protecting privacy, and also providing control over how personal information is made available, the Court of Justice of the European Union (CJEU) heard the case of Google Spain. This case determined that under the terms of the Data Protection Directive (DPD) there could be a right to be forgotten. It held that the right could also be exercised against search engines with regard to the de-listing of links to personal information if they impacted the privacy of an individual. Such right was however subject to a balancing act between rights of privacy and the right of freedom of expression. The result was a difficult exercise of competing interests in an environment where the free flow of data was considered vital for the economic interests of the EU.[23] Such a balancing act, as it was referred to in the case, also exacerbated the tension between differing approaches towards data being applied by the EU and the US. [24] The European approach of increased privacy protection was clearly at odds with the US approach where freedom of expression, particularly for the press, was paramount. The sanctity of this right is reflected by it being

[20] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation) COM (2012) 11 Final

[21] Viviane Reding, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age 22 Jan 2012 available at https://europa.eu/rapid/press-release_SPEECH-12-26_en.htm https://ec.europa.eu/justice/article-29/press-material/press_release/art29_press_material/2009/pr_01_12_09_en.pdf last accessed 17 Mar 2019

[22] George Brock, *The Right to be Forgotten, Privacy and Media in the Digital Age*, (IB Tauris, 2016) 36. Here Brock argues that the rewrite of EU law 'created expectations beyond those which data law should be able to achieve' calling the Internet the most important element of the infrastructure of free expression with digital communications an 'engine of opportunity'

[23] The explanatory memorandum to the DPD had identified areas where the free flow of personal data was essential for member states naming business transactions amongst such objectives. It aimed to ensure the free flow of data via integration of a harmonized data protection regime

[24] This will be discussed in more detail in chapter 3, p 135

considered important enough to be included within the First Amendment in the US constitution.[25]

In this case, the CJEU not only found that a search engine could be construed as a data controller, but that under Articles 12b and 14 of the DPD [26] an individual had a specific right to request deletion of links to certain information concerning them.[27] This fulfilled the fundamental rights provided under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the Charter).[28] However, it was noted that such right only existed where the balancing act between the potentially competing rights of privacy and freedom of expression resulted in a position where public interest was not threatened. The lack of clarity in an otherwise detailed decision initially reduced the effectiveness and potential impact of the right. Although establishing the existence of the right, its extent and the scope of how the right could be exercised was left unclear. What was also not considered was that other rights could be similarly adversely affected by the accessibility of personal data and that whether these should be considered within the establishment of the right to be forgotten.

Finalization in 2016 of the long awaited GDPR potentially compounded the right by providing in Article 17, the 'right of erasure.'[29] This was considered a wider right to remove, as opposed to forgetting,[30] information in certain circumstances where applied, as set out in the article[31].

[25] The inclusion of freedom of expression with the freedoms guaranteed under the Amendments to the US's constitution was originally intended to protect citizens from interference by the Government sanctions limiting autonomy and liberty to express views. This has been widely interpreted by the US Supreme Court , see https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does

[26] The Data Protection Directive, 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31

[27] Such links were often provided in the results of an online search in this instance when there was a search carried out against the name of Senor González

[28] The Charter of Fundamental Rights of the European Union, [2000] OJ C 364/1 Art 7, Respect for private and family life, Art 8 Protection of personal data

[29] GDPR, Art 17 1. Right of Erasure (right to be forgotten) provides in Para 1 'The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: / available at https://gdpr-info.eu/art-17-gdpr/ accessed 15 April 2020

[30] National exercise by member states of the right based on Google Spain principles prior to this had shown varying approaches which the GDPR was aiming to provide more clarity on.

[31] Art 17 provides; a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for

Within the more technical approach, the balancing act remained a key component in assessing whether links to, or even information itself, could be removed or, in the GDPR's terms, 'erased'.

This enhanced right could be seen to be addressing claims of privacy as well as data protection with the ability to remove links to potentially valid but no longer relevant information.[32] This gave an individual the hypothetical ability to not only protect their private life but also personal information which could impact how such a person was viewed within society or their community. Such action would ultimately lead to the potential to manage the way they were perceived in public and to do so specifically online. As a result, the right may be argued to create an opportunity for a form of self-determination where an individual could potentially choose how they wish to be portrayed on the Internet by the control of access to personal information. This concept was initially successfully described by the Constitutional Court of Germany as the right to information self-determination (*informationelle selbstbestimmung*) in its 1983 judgment [33]. The court here ruled that: "[…] the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights in the German constitution. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data.' Limitations to this idea of informational self-determination are allowed only in the case of an overriding public interest. The impact of information available on the Internet since 1983 has increased the desirability of this ability and also increased the value of being able to use such rights to protect not only privacy but dignity as well as reputation.

---

the processing; c).the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); d) the personal data have been unlawfully processed e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

[32] As was noted by the CJEU in Google Spain where it found that search engine results particularly concerns 'a vast number of aspects of [one's] private life'

[33] 1983 Population Census Decision, Germany, 15 Dec 1983 BvR 209/83, BVerf G 65 (*Volkszahlungs- Ureil* translated to English ,Eib Rieder 5 HRLJ 94, 94- 116 1984)

The ability to use the right to be forgotten to provide the wider option of informational self-determination illustrates that the roots of the right are not only based in the balancing act carried out between privacy and freedom of expression[34] , but in underlying rights of dignity and, ultimately, reputation. This possibility to present oneself as desired through the control of the accessibility or availability of personal information increases interest in the scope of such right.[35] Not only have concerns relating to privacy intensified with increased awareness of the growth of the dominance of the Internet by what are referred to as the 'tech giants' or the companies often referred to as FAANGS,[36] but also the need for effective control of what information is connected. This might be through linking, not only by search engines, as was the case in Google Spain, but ultimately more widely through various other forms of social media. The intensification of personal data being made available through forms of access to the Internet has led to an unimaginable impact of the way people lead their lives. There is no doubt that the influence of such an organization as Google.com, not only on privacy but on how a person is portrayed digitally, is immense. Despite Google's initial response accepting the outcome of Google Spain and acknowledging a need that there should be clarity on how to determine what information should be removed,[37] the reality was accepting a form of regulation being bought to the Internet within legal norms. This resulted in an unprecedented impact on Google as well as other internet service providers. It would then challenge the stance taken at the time where search engines were not considered responsible for contents of searches.[38] This promoted that internet service providers, particularly search engines, must be protected to continue to provide services considered necessary to enable the free flow of information with the commercial and societal benefits that this would bring.

---

[34] Google Spain para 81

[35] See Orla Lynskey, *The Foundations of EU Data Protection Law*, (OUP 2015) pp 95, 178-179, see also Antoinette Rouvroy, Yves Poulet, *The Right to Information Self determination and the value of self development, Reassessing the importance of privacy for democracy*, in (eds) Serge Gutwirth et al *Reinventing Data Protection* (Springer 2009) p 45-76

[36] "FAANG" is an acronym that refers to the stocks of five prominent American technology companies: Facebook , Amazon , Apple , Netflix, Alphabet (formerly known as Google).available at https://www.investopedia.com/terms/f/faang-stocks.asp last accessed 28 Feb 2020

[37] David Drummond, Chief Legal Counsel, Google http://www.the guardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate

[38] Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf

The apparent lack of clarity in the Google Spain decision has resulted in the right not being automatically widely accepted.[39] To many, this right already existed within data protection,[40] despite the issuance of guidelines from the European Commission[41] and therefore its value is still subject to debate.[42] The right of erasure (as the right to be forgotten became referred to) contained in Article 17 of the GDPR did not offer increased certainty, not only to the scope of the recourse which still required a balancing of fundamental rights, but also as to its status, again despite such guidelines being published to add clarity.[43] This was notwithstanding the right being argued to be a right potentially in line with the fundamental right to data protection as contained in the European Charter of Fundamental Rights (the Charter) [44] and furthermore linked to specific human rights in the European Convention of Human Rights (ECHR).[45] The value of the right is undeniable but its scope, as yet, has not been fully determined. Specifically, how it can be used to provide the best protection for individuals in pursuit of increased control over personal information and how this is used to portray them requires greater examination. This thesis aims to add clarity to the situation and to argue that the right to be forgotten also provides for the ability to exercise a new form of informational self-determination.

1.2 The significance of and contribution to the issue

An examination of the roots of the right to be forgotten, or the newly termed right to erasure, will enable a better understanding of its theoretical underpinnings and, as such, facilitate informed discussions on the scope and extent of the right and the opportunity it presents for

[39] see Christiana Markou, '*The Right to be Forgotten' : Ten Reasons why it should be forgotten' in* (eds) Serge Gutwirth, Ronald Leenes, Paul de Hert *Reforming European Data Protection Law* (Springer 2015)

[40] see Gabriela Zanfir, 'Tracing the Right to be Forgotten in the Short History of Data Protection Law: The 'New Clothes' of an Old Right' (October 2013). Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2501312 last accessed 24 Jan 2029

[41] Article 29 Data Protection Working Party, 'Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' c-131/12 14/ENWP 225

[42] see n 40

[43] Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf

[44] The Charter of Fundamental Rights of the European Union [2000] OJ C 364/1

[45] European Convention on Human Rights 1950 as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13

its wider application to providing an individual with the ability to shape how they are perceived. Although there has been much commentary on the right to be forgotten I believe that this had not raised the ability of it to provide such a wider remedy to project individual control in respect of personal information beyond privacy and data protection.

This examination will also establish whether the right can perform as a human right to provide a combination of the de-listing of search results as well as the erasure of information, thus enabling informational self-determination for an individual. This may be achieved by formal recognition[46] that the right is not limited to the removal of links to information or to the deletion of information itself. It can also be considered to provide recourse for prejudiced reputation and rehabilitation. Being able to utilize the right on a more extensive premise through the balancing of rights could provide the potential to ensure that the way an individual is perceived by society meets that individual's expectations, thereby incorporating existing human rights of privacy and dignity as well as providing for the protection of reputation within rehabilitation and the maintenance of dignity. Despite much analysis of the decision made in Google Spain and the use that will be made of Article 17, this has been limited primarily to debate as to privacy over freedom of expression. Until the scope of the right, its extent and application are fully understood, it is not possible to assess its full potential value and what it can add to the protection offered.

The roots of the right to be forgotten have been argued to be primarily based on privacy. As such the initial views of Brandeis and Warren[47], in response to an increase in technological developments such as photography and recordings, led to wider recognition of intrusion into a person's right of privacy. Subsequently, Alan Westin[48], the originator of the most accepted concept of privacy, 'the right to be left alone', initiated views that have relevance despite being devised before the current technological environment and emerging issues with regard to the accessibility of personal data.[49] Westin's view of an ability for self-determination, i.e.

[46] This may be by way of amendment to regulations or incorporating this into new regulations or even by precedence of determined cases

[47] SD Warren & LD Brandeis , 'The Right to Privacy', [1890] 4 HARV.L. REV. 193

[48] Alan Westin, *Freedom and Privacy,* New York (Atheneum, 1967)

[49] "He transformed the privacy debate by defining privacy as the ability to control how much about ourselves we reveal to others." Jeffrey Rosen see obituary available at https://www.nytimes.com/2013/02/23/us/alan-f-

'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'[50], also provides an understanding of how the scope of the right can be subject to broader interpretation as the way society is conducted changes.

However, commentators such as Orla Lynskey have argued for the right to be forgotten to be linked to the fundamental right of data protection,[51] thereby limiting it to control over personal information or data rather than being considered a subset of the universally accepted human right of privacy. She proposed that Google Spain provided implicit support for the recognition of 'individual control over personal data', irrespective of whether such data are 'private' or not, as being a central aspect of the right of data protection.[52] This view has been counter-argued with claims that the right is merely an old right wrapped in 'new clothes' [53] and the recognition of it is no more than an authoritarian attack on entities such as Google within the clear ambition of the EU to reduce the power of such an entity to impact the rights of European citizens or data subjects.

Lynskey also recognised the view that there is a 'tug of war' between those organizations and governments who look to claim not only the commercial advantages and value of the information, but also its importance for decision making.[54] This may be against the interests

---

westin-scholar-who-defined-right-to-privacy-dies-at-83.html last accessed 4 Oct 2021 See also Prof. Fred H. Cate in the Foreword to the 2014 republication of Alan Westin, 'Freedom and Privacy', "Almost all data-protection laws adopted since 1967 have reflected (*Privacy and Freedom's*) definition (of privacy), including the influential Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted by the Committee of Ministers of the Organization for Economic Cooperation and Development (OECD) in 1980; the European Union's Data Protection Directive adopted in 1995; and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework adopted in 2004." Prof. Fred H. Cate in the Foreword to the 2014 republication of Alan Westin, 'Freedom and Privacy',

[50] n 48, Alan Westin, 7

[51] The Charter of Fundamental Rights of the European Union [2000] OJ C 364/1

[52] Orla Lynskey, 'Control over Personal Data in a Digital Age: Google Spain V AEPD and Mario Costeja Gonzalez', [2015] 78 (3) MLR, 522 -548

[53] Gabriela Zanfir, 'Tracing the Right to be Forgotten in the Short History of Data Protection Law: The 'New Clothes' of an Old Right' (October 2013). Available at SSRN: https://ssrn.com/abstract=2501312 last accessed 10 Jan 2019

[54] This could be seen in the case taken against Facebook by the highest constitutional court in Germany Federal Court of Justice in Karlsruhe. This followed action taken by the German Data Protection Authority with regard to the vast collection of personal data by the social media giant. Andreas Mundt, head of the Federal Cartel Office, said the ruling outlines how data and competition interplay. "Data is a crucial factor for economic power and for judging market power on the internet," he said. "If data is collected and used illegally, antitrust law must be able to step in to impede misuse of market power." The case reflected that in December 2018,

of individuals looking for enhanced individual control.[55] There is further conflict with these data subjects, as they are now termed, wanting to control their personal information whilst also making it freely available, particularly through social media outlets. Consequently, and possibly inadvertently, this increases the value of the data to its holder to unforeseen levels.[56]

In addition, debate has taken place as to whether the right should be limited to search engines, as in the Google Spain case, to effectively 'delink' information usually available in search results, or should it be considered on a wider basis linked to both data protection and privacy. In this scenario the right would therefore be applicable to other entities retaining and permitting the availability of information which potentially should have been long 'forgotten'.

In considering the right to be forgotten, the question of applying data protection with the balancing of freedom of expression and privacy, has been widely debated. There was also mixed reaction to the finding of Google as an internet service provider being held to be a data controller.[57] However, there has been little analysis into whether the true scope of the right exceeds both the principles of the case which established a right to be forgotten and the recourse under Article 17 of the GDPR. Recognition that the right can be interpreted to provide wider protection, linking privacy to dignity and reputation as rights that may be impacted by the retention and availability of personal information, would ultimately have an impact on the ability to apply informational self-determination. The principles established in

---

Facebook had 1.52 billion daily active users and 2.32 billion monthly active users. The company has a dominant position in the German market for social networks. With 23 million daily active users and 32 million monthly active users Facebook has a market share of more than 95% (daily active users) and more than 80% (monthly active users) available at;
https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html last accessed 12 Oct 2020 The case was unreported in English available at ;
https://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=bedd4af3c9d89a4dcaa64fc85d244e9e&nr=109506&pos=0&anz=107

[55] Orla Lynskey, *The Foundations of EU Data Protection Law*, (OUP 2015). Here she talks about the dual economic and rights -based objectives that underpin the GDPR. Opponents of a rights based approach see such regulation as needing to prioritise the economic interests of data.

[56] In 2015 Facebook was recorded as having 1.36 billion active users providing data for free notwithstanding the potential loss of control over personal information. At the Initial Public Offering of its shares in 2012 Facebook was then valued at US$104 billion rising to over US$50 billion by July 2017
https://money.cnn.com/2017/07/27/investing/facebook-amazon-500-billion-bezos-zuckerberg/index.html last accessed 12 January 2018

[57] for example, see Stuart Hargreaves, 'The Trouble with using Search Engines as a Primary Vector of Exercising the Right to be Forgotten' [2016] Pandora's Box 83-106 available at
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2873391 last accessed 15 Jan 2020

Google Spain and formalised in Article 17 can be argued to support such a broader interpretation. These would offer not only the ability to protect an individual's right to a private life, but also that individual's chances of being rehabilitated into society, to maintain their reputation and to present themself as their 'best self.'

Other jurisdictions looking at additional forms of data protection, including the deletion of inaccurate or out of date information, as well as information no longer relevant, are considering the impact not just on privacy but also on reputation.[58] However, the ability to determine the level of protection afforded by the right remains onerous whilst the extent and scope of the right to be forgotten and its ability to be applied to this element of self-determination in respect of personal data remains unexamined.

The challenges of establishing the true nature of the right to be forgotten relate to the extent of coverage so that such right is not merely confined to the type of situation, as arose in the Google Spain case, but has a wider perspective. This becomes more relevant with the increasing use of automated data collection and use of through automated means. The trend to furthering disclosure of information can be seen with the increasing growth of data intensive tools, including the use of algorithms, accumulating and retaining all forms of personal information. Data subjects could look not just to have data concerning themselves removed, but also patterns of information that may be used specifically through techniques involving artificial intelligence or such algorithms which can mean identities are revealed. For example, if a pattern of information shows interest and reveals potential membership of a specific organization, this may then cast aspersions on a person's political bias even where they have denied affiliation. With the acknowledged existence of a right to be forgotten, although primarily focused on the ability to request the delinking of URLs,[59] the

[58] This can be seen in the developments of principles in Canada where a reference to the Federal Court under subsection 18.3(1) of the Federal Courts Act investigated a complaint made against Google by an individual for the linking of information in a search result which breached their privacy under the Personal Information Protection and Electronic Documents Act. This was referred to as Canada's first steps towards a right to be forgotten. see https://www.mondaq.com/canada/privacy-protection/826224/the-privacy-commissioner-search-engines-and-the-media-a-battle-over-the-right-to-be-forgotten last accessed 20 Feb 2020
Similar actions have also been taken in Argentina and Brazil for example

[59] This was established in the Google Spain case where the request was for the de-linking to specific information revealed in search results.

implementation of Article 17 of the GDPR may provide more opportunities for a wider interpretation of the right which this thesis argues is essential in providing protection in the form of informational self-determination.

An analysis of the theoretical nature of the right to be forgotten, and whether it meets any requirements in connection with being viewed a fundamental right, is therefore valuable. This will provide further understanding of how the extent of the right can be developed to bring clarity to the ability to use it for informational self-determination. The inclusion of an appraisal of other factors affecting its recognition and actual scope will also be beneficial. The right to be forgotten may provide an opportunity for individuals to benefit from the recourse it offers in a digital age where every aspect of a past life, once published on the internet, may be viewed, examined in detail, copied and dissembled.

1.3 Clarification of the legal issue

Key to obtaining greater clarity on the scope of the right is the premise that, not only does the right provide for an individual to protect privacy and control availability of personal information, but it also offers the ability to present the persona or public presentation of the form of self so desired. Potentially determining how an individual is presented through access to personal information is linked to the ability to maintain a reputation. Critically, the issue is about more than just safeguarding a reputation or maintaining dignity but is also about securing the ability for an individual to restrict the public availability of private information and leave behind past events. This potentially combines ideas of rehabilitation and status or reputation within a community. With this comes deeper recognition of the need to not allow past events to prejudice the future of the individual concerned. Before the decision in Google Spain by the CJEU, other courts had already hinted at the need for such recognition.[60] A case against Wikipedia was bought by two convicted killers, Wolfgang Werlé and Manfred Lauber, who wished to have their names removed from online coverage of their crimes. During the case, heard by the Federal Court of Germany in 2009, their lawyer argued "They should be

[60] An example was shown in a Paris case in 2010 where the claimant's name was linked to words such as 'rapist' and 'Satanist' when searches were carried out. Here the liability in respect of algorithms was a key issue. see M.X v Google & Eric Schmidt, *Tribunal de grande instance de Paris*, 2010 available at http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2985 last accessed 25 Jan 2021

able to go on and be re-socialized, and lead a life without being publicly stigmatized" for their crime, adding "A criminal has a right to privacy, too, and a right to be left alone."[61] Although it took place seven years before the right to be forgotten was introduced in the GDPR, this case raised initial challenges as to how the right to be forgotten can provide an element of self-determination required without prejudicing freedom of expression. In this case, the claimants were unsuccessful in obtaining suppression of their names, despite this being permitted under German law, once it was considered their debts to society had been paid. Awareness of the crime and the conviction was clearly in the public interest. In various cases, the impact on a convicted criminal's life of the information being readily available has always be balanced with the public's right to receive information. However, how this is determined and by whom requires clarity. The Electronic Frontier Foundation, an online civil liberties group commenting on this case[62] stated 'He who controls the past controls the future." Jennifer Granick, a lawyer for the group, confirmed the view that the case was "really is about editing history." [63]The idea that history could be changed by such deletion has become one of the main criticisms of the right to be forgotten. With increased focus on the controversial value of re-writing the past and portraying past events through a different lens, it has become necessary for additional clarity on how the law can provide such removal of information, or the reduction of access to such information to provide an individual with the necessary tools to maintain privacy, dignity and reputation.

1.4 Methodology of the research

Using primarily doctrinal methods I will look initially at the development of human rights and how they have arisen in the light of human rights theories. This will be undertaken through consideration of the normative aspects of relevant rights. In particular, this will focus on the recognition, whether formal or not, of a right of privacy in its various guises within such theories whilst considering whether these were designed to protect an individual or society

[61] The case was reported in the New York Times amongst others recognising the US interest in the European approach to privacy and reputation, see Two German Killers Demanding Anonymity Sue Wikipedia's Parent' John Schwartz available at https://www.nytimes.com/2009/11/13/us/13wiki.htm,l last accessed 20 Feb 2021

[62] This is a non for-profit organization involved with the protection of digital privacy and free speech founded in 1990 https://www.eff.org

[63] The New York Times, Nov 12 2009, https://www.nytimes.com/2009/11/13/us/13wiki.html?_r=1 last accessed 3 October 2020

as a whole. Looking initially at the historical development of the right to private life, I will then consider the gradual recognition of offering fundamental rights protection to personal information or data. This will be key to exploring the extent of the right to be forgotten as the aforementioned rights form its theoretical and historical underpinnings. This discussion will explore the perceived need of societies both for privacy and data protection but also the protection of public interest in the retention and access to certain information made publicly available. [64]

This will lead to a review of recent developments relating to the right to be forgotten in light of the difficulty of combining the economic interests of the EU with its principles in promoting protection of data protection rights and privacy of its citizens. This review will include specific analysis of the regulatory approach through the EU's DPD to the subsequent GDPR and its impact on the member states of the EU, as well exploring, by way of comparison, a selection of legal and regulatory approaches taken by other jurisdictions. There will be a critical consideration of the judicial approach post the Google Spain case and the challenges of differing approaches.

In providing a doctrinal review, this thesis will take a positivist approach to the Google Spain case, exploring this and also the implications of Article 17. Whilst looking at the principles of existing case law and its interpretation, there will be some critical analysis to draw normative conclusions as to what the right to be forgotten has established. Within a study of the historical evolution of certain fundamental rights to the right to be forgotten, there is recognition and critical reflection of the steps taken. This reflects the need for the creation and development of relevant laws in line with political or social influences, which must reflect the rapid technological changes affecting societies. There will also be an analysis of the strength of the commercial forces at play. The combined economic strength or potential monopolies of the internet giants within the FAANGS grouping will be considered under

[64] Whilst not key this may also include consideration of the availability of personal data with ultimate recognition of the necessity for a right to be forgotten which led Senor González to take on the case even once it was clear it would have a far-reaching impact and his name would forever be linked publicly to the very information he was seeking to make less accessible.

existing regulation or laws with regard to their position in leading, or potentially controlling, the approach to the re-writing of privacy. An examination of such power can be useful in reviewing how the subsequent exposure on the Internet of information previously not so freely accessible, can be filtered as appropriate to meet the needs of the users. On a comparative basis, any action taken by the regulators as to how activities of such entities can be curtailed to ensure where responsibility exists and how this can be potentially enforced will be included. Where appropriate I will also look at how other legal jurisdictions are now implementing the concept of a right to be forgotten and examine the response by them to such a right, i.e. whether it has just been the subject of debate or whether it has been absorbed within data protection to become a more formal remedy.

Where relevant, reference will be made to empirical studies or reports that have considered the nature and volume of applications by individuals under the 'right to be forgotten' procedure set up by Google. For instance, this will involve looking at requests to Google and other search engines to identify any common factors affecting the volume, such as the nationality of applicants and whether there is correlation between states within the EU with strong data protection authorities, in order to assess the usage of the purported right and analyse which member states have actively developed the concept within their own jurisdictions. The response by other jurisdictions, such as the United States where the impact of the Google Spain case has continued to be debated despite a differing legal system, will also be examined.

1.5 Outline of the thesis

Following this introduction, the thesis consists of a further six chapters. Chapter 2 will examine and analyse how the concept of privacy and related rights, such as dignity and reputation within human rights, has evolved, why and how they can be considered fundamental human rights. The initial emphasis on privacy reflects that this is a key element in the finding of a right to be forgotten whilst acknowledging it is not the only right impacted by the evolving of a digital memory. Various key human rights theories will be considered to assess the validity and development of rights, with an evaluation as to how the concept of privacy, which was key in the determining the right to be forgotten, has been supported by

such different theories. I will also consider how such ideas of privacy, dignity and reputation within human rights have evolved according to the needs of a changing society and to meet the challenges of technology. This will include examination as to why such rights have been considered fundamental, for example from biblical stories to the most recent recognition in the International Covenant on Civil and Political Rights[65] and again to specific arrangements specifically to include data protection such the Charter[66]. This will form the background to understanding recognition of the right to be forgotten and how this has evolved. Where recognition has varied from state to state, this analysis will help to identity a universality of approach. Where it is relevant to do so, I will look at additional rights, such as autonomy, its influence, and where such rights develop protection for an individual to portray themselves within society with the level of control needed.

Chapter 3 will address the legal recognition of the right to be forgotten leading to formal acceptance of this right within the GDPR and primarily within the EU. This will show how this new era of technology has brought wider concerns with regard to protection, not only for privacy and family life, but also for personal communications. The need for individuals to be able to control information held and transferred through progressive electronic means is explored, leading to the desire for remedies to provide for rectification of inaccurate information, or removal of information which is out of date or no longer relevant. I will consider how protection was primarily focused on preventing government intrusions and then increasingly against commercial exploitation which was reflected in early data protection measures. I will also explore how commercial enterprises and manipulations of personal data has led to the devolvement of newer regimes and, finally, to the introduction of the GDPR with its acceptance of the right to be forgotten in Article 17. I will consider if the nature of privacy is expanding to fill the void created by new technology and to meet the needs of individuals who, whilst initially accepting the reduction of privacy through the usage of social media, are now becoming increasingly aware of the heightened risks to their private lives.

[65] International Covenant on Civil and Political Rights 16 Dec 1966 Art 17 '1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.'
[66] The Charter of Fundamental Rights of the European Union [2000] OJ C 364/1

In Chapter 4, the Google Spain case will be highlighted as the foundation for recognition of the right to be forgotten, including an analysis of the media response to the birth of a new right. I will examine the factors that led to the bringing of the case, and also the opinion delivered by Advocate General Jääskinen.[67] I will in addition investigate the debate that followed the decision by the CJEU, together with the critiques offered post case. The reaction to the Google Spain outcome will be the subject of an analysis of specific subsequent cases within EU member states as well as, where relevant, other jurisdictions. This will provide useful insight into where such a right is situated within the current position on human rights and perceived remedies to breach of privacy, or where there is a lack of compliance with data protection regimes. By comparison, a consideration of the response of the US to the case, in particular relating to the position of Google.com, will shed light on the differing privacy and data protection approaches between Europe and the US in particular.

Chapter 5 will look more critically at how the scope and extent of the right to be forgotten is developing following its acceptance and whether this can provide for a form of informational self-determination. This will include an examination of the response to the Google Spain case and also consider the effectiveness of Article 17. This identifies the need for control over the removal of information and specifically links to information to reflect the ability for an individual to decide how they wish to be portrayed on the Internet, particularly in order to protect not only reputation but other facets of their identity. I will consider how the right can now be argued to provide not only for deletion or erasure of information (or links to information) but also a benefit that can be expanded to provide an ability to define 'who you are' so a person can use this to not only protect their privacy and ultimately dignity, but also to shape their reputation or even their digital identity. As part of a wider right, I will look at whether the right to be forgotten can now be considered to have given society a new tool to meet individuals' concerns relating to links to data held on them. An examination will be made as to how the right would be applied portray an individual in a different light and if this provides the ability for an individual to reinvent themselves. This will be considered in the

[67] Case C -131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, [2013] ECLI: EU:C:2014:317, Opinion of Advocate General Jääskinen

light of the public's right to receive information and how far this should be prioritised, particularly where offences against societal norms are involved, such as criminal convictions.

In Chapter 6 the current position with regard to the application of the right to be forgotten and its enforcement will be explored with particular emphasis on the control and protection of data by the use of the right for informational self-determination as an enforceable right, potentially a fundamental right, enabling an individual control over how they are portrayed online. Within this chapter will be an examination of the level of acceptance of the right to be forgotten and the growing understanding of its place with regard to the provision of data for use online. I will look at reactions to increasing awareness of how privacy, dignity and reputation can be impacted. Next, I will review how the right is being shaped, considering as part of this the impact of the implementation of the GDPR. The importance of the GDPR could be considered to enable new players in the technological market to provide protection to individuals in line with the EC stated objectives to safeguard privacy, and this may bring about wider acceptance of the formal right of erasure. I will also evaluate how the attitude of both regulators and law makers is now evolving towards the activities of internet giants. In particular, this will consider how an individual can request erasure of information available through the search engine with the right of appeal to an appropriate data protection authority, and ultimately a court, and the wider implications of this.

I will also evaluate the issues concerning the right to be forgotten being left in the hands of a third party and whether it can be applied appropriately, even independently, by such a dominant commercial entity. I will question whether this alters the significance of the right and its application, whether through the Google process or under the implementation of the GDPR, particularly noting the position of the Internet entities applying the right. Consideration of the role of the Internet entities in the application of a form of digital rights or ethics will also be undertaken to establish whether it contributes to increasing the use of the right.

Finally, the conclusion will summarize the thesis and address the research question. It considers whether the status of the right to be forgotten can be considered in line with the

fundamental right of data protection to protect not only privacy but associated human rights, and provide the ability for an individual to portray themselves online as they so desire. In light of changing expectations of privacy, I will assess the need for the ability for an individual to portray themself in a different light, or even to reinvent themself. If the right to be forgotten can be a right to enable a scenario where history can be rewritten, as has been claimed by those opposing its development, can this be acceptable or does the impact seriously prejudice freedom of expression and limit the ability of the public to be informed on relevant matters? I will argue further that a right to be forgotten should not mean only limited recourse, for example that potential records of youthful demeanours are removed but provide an essential remedy to enable individuals to take part in society unhindered by past events or reputational impact. Following my research, I conclude that the scope of the right to be forgotten should be considered to provide a wider right in the form of a new fundamental right, albeit a limited one, to protect not only privacy and data protection but to maintain dignity and reputation where impacted by the accessibility of personal information balanced with freedom of expression only in circumstances where the interest of the public can be clearly seen to be paramount. The extent of this evaluation can be seen to provide the use of the right to achieve informational self-determination in respect of information made available and accessed particularly through the Internet to enable a person to exercise autonomy to protect privacy as well as their dignity and reputation. To restrict the ease of accessibility to data to impact how you are seen and viewed is key. This requires a delicate balancing act between the effect of loss of privacy and freedom of expression being carried out in favour of individuals' rights in respect of information relating to them and any resultant adverse impact arising from such information. The right itself is closely linked to other rights and so must be left to develop, whether organically under case law and through potential additional regulation of the technical giants, to take shape in a way that reflects the changing approach to privacy and data protection and to provide a necessary ability to ensure that the person you are is validly portrayed in the absence of information no longer necessary or essential for public perusal.

Chapter 2 -An historical and theoretical account of the roots of the human rights of privacy and how this, together with reputation and dignity, has influenced the right to be forgotten.

2.1 Introduction

When the right to be forgotten emerged in the EU as a result of the decision in the Google Spain case,[1] the right of privacy was seen as being key to its existence. It was noted that the purpose of data protection provided within the EU was to secure protection of 'fundamental rights and freedoms of natural persons'.[2] Specific reference was made to protection of the right of privacy in respect of the processing of personal data contained in Article 7 of the Charter of Fundamental Rights of the European Union 2000. This provided that '[e]veryone has the right to respect for his or her private and family life, home and communications.'[3]

The increasing retention and access of data developed through new technology has increased opportunities for any right of privacy to be compromised. Information relating to a person is now made more available either through social media on the Internet or through commercial entities' data gathering. This results not only in an immediate loss of privacy but also, through the everlasting nature of the availability and access to such information, potential damage to an individual's reputation and ultimately their dignity. The increasing use of technology in respect of information or data does not of itself, mean that such concepts needs to be reinvented or transformed but, as put succinctly by Lisa Austin,[4]

> '…[t]echnology need not force us to reinvent privacy although we must sharpen and clarify what we mean by privacy and why we are concerned about losses of privacy.'

There are various ways in which to approach how privacy can be defined. However it is clear that before the role and scope of any acclaimed 'right to be forgotten' may be properly considered, the concept of privacy, together with rights pertaining to reputation and dignity also impacted by the disclosure and accessibility of information, must be examined in the

[1] Case C- 131/12 Google Spain Sl Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González Case, [2014] ECLI: EU:C:2014:317 (Google Spain)

[2] Google Spain, Para 53 'Furthermore in the light of the objective of Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect of the processing of personal data, those words cannot be interpreted restrictively …'

[3] The Charter of Fundamental Rights of the European Union [2000] OJ C 364/1

[4] Lisa M Austin, 'Privacy and the Question of Technology' (2003). Law and Philosophy, Vol 22, September 1 2003 available at SSRN: https://ssrn.com/abstract=2016965 last accessed 12 Feb 2019

context of human rights. The questions that arise include the challenge of what are they, where did they come from and where would this right to be forgotten fit within them. The capacity to forget forms part of a biological cognitive behavior for mankind and should be considered a natural process, however this is now being replaced by digital memory. Does the ability to request an artificial form of remembering which can overtake human recollection gain credibility as a fundamental right to balance out the mechanical yet artificial process now being formed? Understanding the beginnings of human rights is a first step to understanding how the right to be forgotten supports a right to a private life with the ability to maintain dignity and reputation. Steps taken to recognize and develop this with regard to personal data and information involve keeping certain information private thereby protecting a person's reputation and dignity. This chapter will also look at how such elements have directly contributed to the creation of data protection and ultimately to the right to be forgotten to see where such right 'fits' into the understanding of human rights.

In accepting that the right to be forgotten initially involves protection of privacy, the Oxford Dictionary defines privacy as ;

> 'The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion.'[5]

In the context of the right to be forgotten, key words might be 'free from public attention as a matter of choice or right'. Where personal information is constantly made publicly available, the ability to exercise choice seems compromised without the ability to 'forget' information. This is where the ability to exercise control over the availability of personal information becomes vital. If a definition of privacy is sought from the legal conventions on human rights, then the Universal Declaration states; [6]

> 'A right to privacy is explicitly stated under Article 12 of the Universal Declaration of Human Rights: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation.'

[5] available online https://www.oed.com/view/Entry/151596?redirectedFrom=privacy#eid last accessed 12 Feb 2018

[6] Universal Declaration of Human Rights 1948

This definition includes reputation being interwoven with privacy. It is therefore useful in this context to look at the evolution of the formalization of international human rights and how privacy in particular was often included based on the overreaching right of dignity. This leads to consideration of the role of privacy as a human right and its contribution to the formation of data protection as being key to understanding the depth of the right to be forgotten.

The evolution of the right to be forgotten has not only evoked the application of human rights such as right of privacy as balanced with rights of freedom of expression and the public's right to receive information, but also brought about realization that reputation is also at risk without the ability to erase or 'forget' information. The first stage in considering the legitimacy and scope of the right to be forgotten must be to determine its composition. Then, it could be construed and utilized in a similar way as a human right to provide the protection necessary. In order to achieve this, an examination of human rights, including arguments concerning their formation, the theories around the protection they offer, and the formalization of such rights over the centuries is vital. It may then be possible to establish whether they are inherent rights or rights that were only granted under legal remedies[7]. Looking at the foundations of human rights such as dignity provides understanding not only of the acceptance of privacy as a right and the value it provides but also of how other rights, such as reputation and identity, have also influenced the scope of the right to be forgotten.

In this chapter I propose to look at the various stages and development of privacy as a human right and its relationship with dignity, as well as its scope in providing an ability for individuals to be able to protect their dignity and, ultimately, their reputation.[8] This will build an understanding as to the value of the right to be forgotten and start the process of establishing its scope and potential ability. As part of this, I will also consider where dignity as a potential foundation right has influenced the right to be forgotten building to recognition that the right to be forgotten also protects reputation.

[7] Following on from the Universal Declaration the International Covenant on Civil and Political Rights, 16 December 1966 and the International Covenant on Economic, Social and Cultural Rights, 16 December 1966 state 'recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world,'

[8] Developments in how reputation is affected through digital activities will also be considered in Ch 5

For the purposes of examining the acceptance of human rights, it is proposed that there are various 'stages' of recognition of their existence, application and indeed value. The first stage is the early philosophies and teachings relating to human rights, the second is the Enlightenment period and the last is the beginning of formalities in respect of human rights which followed the Second World War. These led ultimately to the recognition of privacy as a right but with an underlying focus on dignity and the ability to be autonomous. Within these categories I will consider privacy, reputation and dignity in the context of the right to be forgotten. I will then outline the progress towards securing protection with regard to personal information and data, and the relationship with such rights, particularly privacy. This provides a platform for understanding the foundations of the right to be forgotten and what part human rights have played in establishing not only data protection but also the increased scope of such right.

2.2. An overview of how early concepts of privacy and associated rights, such as dignity and reputation, were formed within human rights

2.2.1 Early teachings and philosophies

If the concept of privacy was not fully accepted as such until post World War II and the Universal Declaration despite earlier ideas expressed by Brandeis and Warren [9], it was certainly not captured as a concept in the early teachings leading to human rights. In societies based on hierarchies, which included slavery and the subservient position of women, ideas of privacy could not flourish until there was recognition of a right to freedom of ownership not of property but that of one's own body and a sense of self.[10] These initial ideas centered around dignity and even reputation as integral to dignity and were apparent in early cultures and practices which led to theories developing the importance of such rights. [11]

[9] Samuel D Warren & Louis D Brandeis, 'The Right to Privacy' [1890] 4 HARV.L. REV. 193

[10] Julie E Cohen, 'Turning Privacy Inside Out Turning Privacy Inside Out' (2018). Theoretical Inquiries in Law 20.1 available at SSRN: https://ssrn.com/abstract=3162178 last accessed 17 May 2019

[11] Pico della Mirandola in 1486 argued that at the root of Man's dignity is the ability to choose to be what he wants to be, that this is a gift from God. 'It is given to him to have that which he chooses and to be that which he wills.' See D. Kretzmer, E. Klein, *The Concept of Human Dignity in Human Rights Discourse* (2002). Kluwer Law International, 2002 see also Giovanni Bognetti, 'The Concept of Human Dignity in European and U.S. Constitutionalism', in G. Nolte (ed.), European and US Constitutionalism, Science and Technique of Democracy No. 37 (2005), at 75, 79. Another example of this was within the teachings of Immanual Kant, *Metaphysics of Morals* which has become the source for the belief that his understanding of human dignity required that

In considering the progress from human rights, sometimes termed as a theoretical offering to man's conscience towards formal, internationally recognized concepts which reflect changing social need, it is useful to understand the earliest acknowledgement of human rights and how they arose. This can, in turn, help to see where new rights can come into existence as societies change and evolve. such understanding enables recognition of the value of the right to be forgotten potentially as a concept initially founded in such early reasonings and beliefs and entwined with ideas of reputation and dignity.

From examination of early readings and teachings, it is clear that acceptance of human rights is not straightforward. Such rights often evoke a moral step in defining what is good or bad and are therefore subject to multi-faceted influences.[12] This is turn provides for philosophies to be developed to provide explanations for the reasons and moral basis for such rights. For example, if it can be argued that killing people is wrong, there will always be counter claims, for example that it may be necessary to kill for self-defence or other arguably justifiable means.[13] However, it is also clear that many people believe that the concept of human rights is essential to provide the background for a morally protective society.[14] The origins of the development and recognition of human rights subsequently within certain theories reveal how the need for such rights arose and how many of these focused on dignity as underlying certain rights including privacy.

The earliest record of known rights was contained in the Law Code of Hammurabi declared by the King of Babylon Hammurabi in eighteenth century BC setting out initial entitlements. However, in the opinion of Micheline Ishay, in her work on the history of human rights,[15] stoic philosophy was key to early thoughts on rights for mankind. This was widely provided for

individuals should be treated as ends and not simply as means to an end.see Kant, 'Metaphysics of Morals', Section 38 of the *Doctrine of Virtue* (Ak. 6:462).

[12] Besson argues that there may be moral justifications of legal human rights that are different to justifying moral rights, ie moral interests recognized by law as sufficiently to generate moral duties.

[13] There can be seen that in certain instances killing may be permitted other than at times of war, for example abortion, assisted suicide, protection of property. These are often emotive and can be linked to cultural or religious views.

[14] Joseph Raz, 'Human Rights Without Foundations' (March 2007). Oxford Legal Studies Research Paper No. 14/2007, Available at SSRN: https://ssrn.com/abstract=999874 last accessed 15 May 2019
Raz argues that human rights are rights held by individuals, but individuals only have the benefit of them if conditions are appropriate for governments to fulfill them

[15] Micheline Ishay, *The History of Human Rights,* (University of California Press, 2nd Ed 2008) p 81- 87

through early Greek philosophers, namely Chrysippus, Zeno, Herodotus Seneca and the Roman, Cicero. These thinkers put forward arguments that a Roman slave was not enslaved by virtue of 'divine law' but by manmade law, or *jus gentium,* resulting in that person being deprived of any form of autonomy.[16]

With regards to the instincts of natural laws, Ishay argues that ideas of Christianity developed the initial thinking of Stoicism to echo the concept of dignity as being an inherent characteristic of man, one that underlies the need for human rights. This may also be claimed to be fundamental to the development of a right to be forgotten, where such a right could be argued to protect not only privacy but other rights such as dignity. Such idea was in force as early as 381 AD as followed by the Roman Empire, but was not restricted to one culture or one philosophy, as this was mirrored within various religions. The writer Norani Othman, writing on Islam, wrote broadly:

> 'The *Qur'anic* term *ibn alsabil* refers to someone who is forced to move from place to place in order to seek a more peaceful life free from oppression. Having to endure oppression involves a double violation of divinely ordained human nature and autonomy: by the oppressor and by the victim. Implied in this is a profound affirmation of human freedom, dignity, and autonomy.' [17]

It seemed that key similarities with regard to what is essential to the wellbeing of man are based on an individual's need for dignity and autonomy. Various approaches to the level of dignity or autonomy that would be afforded differ where, for example, the value placed on an individual was based on social order. In this instance, different castes would be treated as

[16] Norman Weiss, *The Human Right to a Dignified Existence in an International Context* in (eds) Logi Gunnarsson, Ulrike Mürbe, Norman Weiß, *Legal and Philosophical Perspectives* (Hart Publishing 2019) It could be argued that such loss of autonomy would then be considered to impact a person's dignity and even how they were positioned in society, a concept which would in future take the form of reputation. Plato and Socrates, perhaps the initiators of the Stoic movement, argued that universal goodness lies within each person so as to provide for altruistic behaviour. Such philosophy leant heavily towards the teachings of Buddha and Confucius, which proposed the need for a balance between such elements as intellect, emotion and desire with a just government needed to keep this balance to ensure that harmony in society prevails.

[17] Norani Othman, *Grounding Human Rights Arguments in Non Western Culture sharia and the citizenship and rights of women in a modern Islamic state,* in (eds) Joanne R Bauer, Daniel A Bell, *East Asian Challenge for Human Rights*, (CUP 1999) 189

having different requirements or the distinction between enslaved persons and a property owner would result in an acceptance of differing values within that society. This also signposted very early ideas of reputation within society based on social standing. Philosophers attempted to provide ideals behind the reasoning for the need for such rights to be recognised and the subsequent benefit to humanity examined.

In older readings of Manu and Buddha there were similar ideas focused on the morality of mankind again providing support for followers of a natural law theory. Keown[18] looks at the teachings of Buddhism in the context of linked understandings. He also notes that the usage of the word 'right' has Western origins in the word 'rectus', meaning both physically and, in the moral sense, upright, with similar words being found in Sanskrit.[19] Although the Burmese use of the words to represent human rights (lu a-khuin-aye) only appeared in colonial times, Keown believes that this does not mean the concept of human rights was not understood and that key to its development was the linkage to the use of the term 'Dharma.' This term refers to the recognition and belief in doing what is right and due in any situation necessary for the dignity of a human being, and can be viewed as an early acceptance of human rights.

The teachings of Confucius, over two thousand years ago, were also based on ideas of human rights illustrating them in a way that could be comparable to modern thinking. He viewed education as leading the way to self-awareness which then built the basis of successful human relationships with the family, the community and even the state. Thus protecting dignity and ensuring that peace and order could prevail. His belief was that if a state protected a people's economic and moral welfare, then it and its people would thrive. Linking the validity of rights to enforcement by the state built on the need for a clearer understanding of the value of rights and therefore the philosophies behind them enabling formalization in some way. From such origins, religions then developed ideas of furthering such protection for mankind.

[18] Damien Keown, 'Are There Human Rights in Buddhism', Buddhism and Human Rights (eds) D Prebish, C Husted, (Curzon Press London 1998) 16

[19] An example in Sanskrit is 'ju' with the equivalent meaning of upright and as in pāli iju (straight forward honest)

2.2.2 Religious beliefs in relation to human rights

A path to wider recognition beyond the ideals of such philosophers was often associated with the teaching of religious interpretations. Ishay investigated whether certain rights seemed to be common to all, albeit in different forms. She looked at how each religion or teaching saw the need for a form of moral protection for men and considered whether certain rights were given as often for protection against unjust kings or states as against other people.
In her view, examples of what could be considered more obvious rights, such as the sanctity of life which are seen in most teachings, could be compared to the ideas of impartial judiciary seen as early as the first bible and in ancient Indian texts, such as Arthashastra around 300 BC. [20]

Key to the philosophy behind the Christian religion was the notion that each human being is created in the image of God, irrespective of race, sex, origin and status, which added the concept of equality in its broadest form. [21] The work of Rene Cassin, a delegate on the League of Nations and involved in the drafting of the Universal Declaration of Human Rights (the UDHR) [22], also explored the concept that human rights transcend ideas from various religions and ideologies, although these must also be considered to have formed the basis from which human rights became recognized. In Cassin's view the recognition that all men should be treated as belonging to the same 'brotherhood' began from creeds expressed in the Bible to 'love thy neighbour as you love yourself.' Taking the view that human rights came from not only the Bible but within the Old Testament, the Ten Commandments and other chapters he argued that these could also be found in other forms of religion expressed in both church, synagogue and mosque or even earlier codes such as Hammurabi's Code as referred to previously.[23]

---

[20] The Arthashastra is the title of a handbook for running an empire, written by Kautilya (also known as Chanakya, c. 350-275 BCE) an Indian statesman and philosopher, chief advisor and Prime Minister of the Indian Emperor Chandragupta, the first ruler of the Mauryan Empire. The title *Arthashastra* is a Sanskrit word which is normally translated as *t*he Science of Material Gain*,* although Science of Politics *or* Science of Political Economy are other accepted translations for Kautilya's work. http://www.ancient.eu/Arthashastra/

[21] Genesis 1:26 Then God said, "Let us make man in our image, after our likeness. And let them have dominion over the fish of the sea and over the birds of the heavens and over the livestock and over all the earth and over every creeping thing that creeps on the earth. So God created man in His *own* image; in the image of God He created him; male and female He created them'

[22] The Universal Declaration on Human Rights 1948 (General Assembly resolution 217 A)available at https://www.un.org/en/universal-declaration-human-rights/

[23] Micheline Ishay , *The History of Human Rights,* (University of California Press, 2nd Ed 2008) ch 1 p 19

For Christians, the teaching in the Bible of the Ten Commandments laid down the premise on which many strived to live by, forming a basic human code including concepts such as 'Thou shall not kill' and shall not steal.[24] However, protection of human dignity is not found as such in the Bible, although Donnelly expresses the view that Genesis provides an understanding of dignity that continues to be a powerful presence in contemporary discussions.[25] In most cultures, particularly those based on hierarchies, there was different treatment of those who were enslaved or women, who were still considered to be property, rather than ranked in the same way as a free man. It was not until centuries later that there could be full consideration given to the idea that all people should be treated equally and given the same rights. Ideas of freedom of thought or expression and autonomy do not appear to have formed part of these early ideas of human rights. However, clear reference was made to religious experiences that could be experienced only when the individual was alone or indeed experiencing privacy.[26] Although seclusion was considered important there was, as yet, no recognition of this as a right or a necessity. Stories from all cultures also showed that a curiosity towards invading such seclusion or privacy, in the form of unveiling secrets, seemed to be an integral part of man's psyche.[27]

In the western world, the Magna Carta in England was often viewed as one of the precursors to modern formal human rights. Despite an acceptance of what could be considered as moral obligations towards the 'needy' as set out within it,[28] this was not a true formalization of rights. It merely set out various agreed provisions given by the King to certain members of society, such as the reflected interests of the merchant class. However, it did provide a restriction on kings for the first time in the modern age and began the change which became the key focus of the Enlightenment. The subsequent Habeas Corpus Act could almost be considered as a trial 'Bill of Rights' in the UK; a forecast of laws ahead. For the first time a form of stated rights was being made available to nearly all citizens for the law to protect them and to provide them with autonomy.

[24] This could be argued to be following on the early beliefs starting with Aristotle and Plato.
[25] James Donnelly, *Universal Human Rights in Theory and Practise,* (Cornell University Press. 3rd ed 1989) p124
[26] For example as was recorded in the Bible when Jesus went into the wilderness.
[27] Consider also the story of Pandora's Box in Greek mythology and the biblical story of Lot's wife.
[28] The Magna Carta 1215 was issued by King John as the Great Charter

What becomes clear on examination of such concepts is that there are certain key themes considered essential to many with early ideas of privacy and protection of personal and family life. This could be argued to be based on ideas of dignity and autonomy as well as position in the community, leading to awareness of the need for formal recognition of rights. This gradually built the idea of the importance of personhood as expressed by Griffin[29] which will be explored further on in this chapter.

2.3 Towards formal recognition of rights: Natural law to the age of Enlightenment

2.3.1 Ideas of natural rights

Within such teachings of the need for dignity and autonomy, there was recognition of the ability of mankind to acknowledge the necessity for human rights and for such to be provided initially by way of inherent goodness, as was shown in early teachings. Natural rights were considered formed from beliefs that rights were shared equally by everyone merely due to being human. However, to others, this was considered too simplistic and it was believed that the only way human rights could be bought into existence was by formal recognition. Even for those believing in the idea of natural law, there were other arguments that legal rules are only a response to formalizing what are considered inherent natural rights, thereby making such rights fixed and resolute. As primitive societies grew, so did the need for rules to be more clearly defined and societal roles determined. This was the start of wider recognition that an individual's protection was key to ensuring that the values of a society could be upheld. Within this it was also accepted that the autonomy of such individual to make decisions to ensure their place in society was essential.

For example, the English Bill of Rights in 1689 only spoke of 'ancient rights and liberties' with no declaration of equality, universality or the naturalness of rights nor any detail as to what legal protection could be offered through the courts. Lack of clear rules relating to the rights of citizens led the way for theories being developed to support, initiate and ultimately formalize such rights. This led to the birth of the Enlightenment, a time for emphasising

[29] James Griffin, *On Human Rights* (OUP reprinted 2013) ch 13.1 , 225

reason and individualism. Both of these factors would become key to underpinning ideas behind the right to be forgotten by way of individual control.

2.3.2 The Age of Enlightenment

The philosopher John Locke[30], believed to be the founder of what has been called the Age of Enlightenment, was considered fundamental to the subsequent development of ideas relating to the acceptance of human rights, often reflecting what is termed 'western' ideas. His views on self and identity were believed to be the initiators of movements in philosophy led by Rousseau and Kant. He believed that man is fundamentally good and that all men are equal and independent but need a civic society in order to resolve conflicts in a just way. His view was that:

> '[m]en being as has been said by nature all free equal and independent that no one can be put out of this estate and subjected to the political power of another without his own consent. The only way whereby anyone divests himself of his natural liberty and puts on the bonds of civil society is by agreeing with other men to unite into a community for their comfortable safe and peaceable living one amongst another in a secure enjoyment of their properties and a greater security against any that are not of it.' [31]

Following Locke, the French developed their own ideas of society and the responsibilities of individuals within it. By the 1760s, the French had formed the 'Droits de l'homme', the rights of man, with Rousseau drawing up a social contract in 1762.[32] Despite the lack of universality, important steps were being taken to increase the scope of protection offered to individuals. In 1789, the French Declaration of the Rights of Man and Citizen, known as the 'natural inalienable and sacred rights of man', was claimed to be the foundation of 'any and all government.' It declared the principle of universality of claims despite controversy with 'incarnated promise of universal rights.'[33] Included within such rights was the earliest

[30] John Locke, *The Second Treatise of Government* ,1690, (reprinted New York MacMillan 1986)
[31] ibid John Locke, Ch 8, 766
[32] Jean-Jacques Rousseau, *The Social Contract*, originally published as On the Social Contract; or, Principles of Political Rights (French: Du contrat social; ou Principes du droit politique) 1762
[33] Lynn Hunt, *Inventing Human Rights, (*WW Norton & Co. 2007) ch 2, 82

example of an acceptance that, in order for freedom to be available for an individual, there needs to be a right to be forgotten, or a *droit d'oubli*, a right of oblivion.[34] This evoked concepts of autonomy over how one was portrayed to society, reflecting dignity and ultimately the ability to cast one's past behind to make one's way in society as a good citizen. This is often considered to be the foundation of the right to be forgotten.[35]

Following the intent for 'universality of claims', it became increasingly clear that the formalization of rights was primarily aimed at certain sectors of society with particular groups notably absence from such provisions. The greatest impact on rights was in 1794 where, with the abolishment of slavery, there was at last some form of recognition of freedom of the body or self, leading to clearer notions of autonomy.[36] This movement also promoted the recognition of dignity as an inherent right for each person, beginning the argument that dignity was the foundation of all human rights.[37]

The Age of Enlightenment could be considered to be an era where the needs of the people against the power of the state, however comprised, were recognized. There was acknowledgement that all individuals were entitled to specific rights with a government made up of the people's representatives to protect them. This was contrary to the previous hierarchy of aristocrats and other nobles. Louis Henken takes the view that individuals effectively gave, or pooled, their autonomy when the 'people' were formed and were then

[34] There was also an underlying idea of 'ce droit à une seconde chance', the right for a second chance which explained an acceptance of society to let people get on with their lives once they had been punished, a form of rehabilitation which still exists today. This right reflected acceptance of an ability to put past events behind oneself so that there could be a form of rehabilitation into society

[35] See Ignacio N Cofone, *The right to be forgotten, A Canadian and Comparative Perspective* (Routledge Focus, 2020)

[36] Whereas the French abolished slavery in the National Convention by a decree this was restored in1802 by Napoleon. However, the movement which had begun continued with the British abolishing the slave trade in its colonies in 1807. Ultimately the Thirteenth Amendment in the US Constitution outlawed slavery in 1870.

[37] Jergen Habermas, '*The concept of Human Dignity and the Realistic Utopia of Human Right , The crisis of the European Union: A Response,* (2010, Wiley online), Metaphilospohy Volume 41, Issue 4 July 2010 Pages 464-480' [T]he idea of human dignity is the conceptual hinge which connects the morality of equal respect for everyone with positive law and democratic lawmaking….' available at; https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1467-9973.2010.01648.x?saml This article also noted that the protection of human dignity has led to judges wishing to protect human dignity in light of technological advancements by the introduction of new rights such as the right to informational self-determination see p 4

subjected to the majority rule.[38] This gave a level of autonomy to the government who could be said to secure such rights for its citizens.

Despite what could be considered as a reluctance to accept ideas of universal human rights, in the opinion of Louis Henken, there were two clear channels working towards clarification of social consciousness leading to current understandings of an individual's right for dignity and ultimately privacy in which to exercise such right. The first was the French position referred to earlier and the second was the movement in the United States. The beginning of such remedies in the US could be said to have begun with the Virginia Declaration of Rights 1776, which offered specific rights, such as freedom of the press and freedom of religious opinion. The American Declaration of Independence 1776[39], following the war of independence, gave an opportunity to detail aspirations in respect of rights of citizens with a declaration of equality. This was credited to the philosophy of Thomas Jefferson and considered as the precursor to the proposed US Bill of Rights. [40] The concept appeared to place more focus on the rights, or even needs, of an individual, and on his own needs rather than on people as a whole. This was initial recognition of the idea of individuality, or 'personhood', which would be explored by other writers in the context of many aspects of rights, namely dignity and autonomy. This idea involved elements of privacy and ultimately reputation. The approach took the view that two forms of government were required, the first being the representative government and the other being individual rights with the constitution consisting of a set of instructions from the people to their representatives. Henken's view was that acceptance of human rights implies obligations on a society which must then provide a system of remedies for benefit or compensation as formulating claims upon society[41].

[38] Louis Henkin, *The Age of Rights*, (Columbia University Press 1990) 5

[39] Declaration of Independence, July 4th 1776,' We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.--That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed,' available at https://www.archives.gov/founding-docs/declaration-transcript last accessed 14 Dec 2020

[40] US Bill of Rights, December 15, 1791 This proclaimed certain inalienable rights of life and liberty with the width of approach can be seen in the example where Jefferson looked to a 'right to pursue happiness', which would, if accepted, have even included a right to divorce. available at; https://billofrightsinstitute.org/founding-documents/bill-of-rights/

[41] See n38 Louis Henken ch 3, 43-50

Thomas Jefferson[42] also spoke of hopes that 'a wise and frugal government restrains men from hurting each other otherwise free to regulate their own pursuits of industry'. Ideally a government should secure moral rights and help men to carry out such moral obligations through laws and institutions. Such a political society must therefore protect individual's rights against private invasion. This was considered idealistic to many as it did not include the position of slaves and how their rights could be enforced. These concerns are still relevant today, with states still taking a back seat with regard to enforcing rights, often leaving this in the hands of non-state actors. This continues to be relevant when looking at the potential enforcement of the right to be forgotten by such entities.

The development of self and autonomy led to the progression of ideas of privacy within the path to the proposed Bill of Rights. The bill was created to protect rights that American citizens believed were automatically theirs. This included the right that no government would intrude into their own personal and private affairs. From the abolition of slavery and recognition that no man should 'own' another came a movement increasingly towards autonomy so that an individual could be seen as an independent being. Lynn Hunt argues that there was an underlying transformation of society whereby the community was no longer the centrepoint representing all acceptable actions, but an individual stood alone using self-discipline and behaving in a way considered appropriate for the benefit of the society.[43] This again linked to reputation and how an individual was publicly portrayed. A further comparison can be made with the recognition of torture as an aberrant practice. It was accepted that it was no longer permissible to abuse an individual's body, even if for the good of the community or potential good of the society, with recognition that an individual 'owned' their own body and could therefore not be treated in such a way. This represented acceptance of a degree of separateness of the individual from general society unless on the terms agreed. However, this may be the point that reputation and the ability to portray oneself as a 'respected' member became truly significant.

[42] Thomas Jefferson, First Inaugural Address, 4th March 1801
http://avalon.law.yale.edu/19th_century/jefinau1.asp last accessed 17 April 2017

[43] Lynn Hunt, *Inventing Human Rights, (*WW Norton & Co. 2007) Here she expresses that rights are not merely 'rights of humans' but 'rights of humans in society' pp 21,22

Henkin[44] argues that this now led to confirmation that 'liberty' and 'due process' could imply individual autonomy through realisation of the Age of Enlightenment. Henkin also believes that contemporary constitutional jurisprudence has not defined individual autonomy but instead has linked certain rights during the process, thereby balancing private rights and public needs through government and the courts.[45] This provides a platform for the acceptance of an individual not only being granted such rights, but also the potential to enforce them.

2.4 The next steps of recognition within international human rights law

2.4.1. Initial steps towards universal acceptance and the inclusion of privacy

Recognition of the need for formalization of agreed human rights really began in 1918. Here US President Wilson voiced his desire 'to create a world dedicated to justice and fair dealing'. The creation of the Fourteen Point Programme[46] then formed the basis of the Versailles Peace Treaty of 1919.[47] Further progress was made in 1941 with the Atlantic Charter[48] and with the UN Charter in 1945[49], although it is questionable whether this was more concerned with the punishment of war crimes than the actual development of rights. Despite the formation of the League of Nations,[50] the rise of fascism in Italy and the support for Nazis in Germany led to crimes against humanity and the atrocities of the Second World War. This again focused attention on the need to protect the rights of human beings. Although earlier movements towards the recognition of rights of liberty and dignity had already taken place, which will be considered later on in this chapter, formal approaches to protection of privacy and reputation only took place constructively after the end of the Second World War. The catastrophic abuse

[44] see n38 Louis Henkin, ch 7 113,114

[45] See as an example that in the US under the 5th Amendment the State was forbidden to deprive any person of life liberty or property without due process of law. Under the 14th Amendment this was extended to include the federal states. This was expanded upon under the Virginia Declaration of Rights and No 84 of the Federal Papers confirmed that despite no formal bill of rights the individual was free and independent except as far as the government is 'instructed' by the people to provide otherwise.

[46] This set out the principles for peace to bring about the end of war as outlined by Woodrow Wyatt.

[47] Versailles Peace Treaty 1919 intended to secure the terms of peace was signed at the end of World War I by the Allied Forces (Britain, France, Russia, Italy, Japan and the US and associated powers) and by Germany in the Hall of Mirrors in the Palace of *Versailles*, France, on June 28, 1919;

[48] This was a statement issued on 14 Aug 1941 setting out the goals for the world at the end of WWII

[49] Charter of the United Nations, 26 June 1945 which became the founding document of the UN

[50] A precursor to the United Nations this was formed after the Fourteen Point Programme and implemented by the Treaty of Versailles into what was considered an international diplomatic group

of the most fundamental of human rights once again focused the attention of the great powers and other nations in attempting to address the need to formalize this protection for all persons. Following the war, it could be considered that the atrocities against specific people and the indignities suffered led directly to dignity becoming a more prominent and vital aspect of human rights,[51] and potentially a significant contributor to the development of the right to be forgotten.

Post war, more modern-day developments again fell into US hands with Eleanor Roosevelt campaigning for the proposed Universal Declaration of Human Rights (UNHR). Deciding that Western states should not wholly influence the development of this proposal to the detriment of the East, and recognizing the criticism that had been raised of the dominance of such Western influences, the Human Rights Commission (the Commission) was developed, comprising of what Ishay[52] refers to as members of 'starkly contrasting cultural backgrounds'[53]. The intention was to involve other aspects, such as religious teachings and philosophies based on aspects of natural law.[54] Despite this, Clapham argues that the formalization of rights has come to be what he calls a 'Western story', particularly arising from the aftermath of the Second World War, and that if the story had begun in Africa or Asia, it would have been different irrespective of the underlying belief in protection against injustice and inhumanity represented by the loss of autonomy or freedom over self.[55] Within the Commission was an acceptance that they would be able to discover common ground for mutual good.

[51] James Q Whitman 'The Two Western Cultures of Privacy: Dignity versus Liberty' [2004] Faculty Scholarship Series Paper 649, Here he talks about contemporary continental dignity being the product of a reaction against fascism and Nazism and the traumatization of Europe when the full horrors of the indignities suffered by people just by virtue of their race or religion were realized . Also see discussions in: Gabrielle S Friedman, James Q Whitman, 'The European Transformation of Harassment Law: Discrimination Versus Dignity' [2003] 9 Columbia J Eur L 241 available at http://cjel.law.columbia.edu/print/2003/the-european-transformation-of-harassment-law-discrimination-versus-dignity/?cn-reloaded=1

[52] Micheline Ishay, *The History of Human Rights,* (University of California Press, 2nd Ed 2008) 16

[53] ibid Micheline Ishay , at p 221

[54] For example, there was the addition of Malik, who was a supporter of natural law and who was able to challenge some of the pre-conceived and who held an important role in clarifying some of the conceptual issues. Ishay refers to 'is man merely as social being, is he merely an animal, is he merely an economic being' challenging assumptions made as to the nature of the rights. p 221

[55] Andrew Clapham, *Human Rights: A Very Short Introduction,* (Very Short Introductions, OUP, 2nd edn 2015)

Although Cassin identified four foundation blocks of the UDHR as dignity, liberty, equality and brotherhood,[56] it can now be seen that the Declaration actually formed two 'sets' of human rights. These included firstly, rights that could be considered 'traditional', namely civil and political rights, such as the rights to life and liberty, and the right to vote. Secondly were additional rights classified as economic, social and cultural to reflect non-western countries' influences and traditions.[57] A review of the overall process to obtain acceptance of such rights helps understand the importance attached to various human rights concepts including the key right of dignity. It also notes the introduction of wider rights and more culturally based rights. The Drafting Committee[58], led by the Secretariat John Humphrey, produced an initial working paper, the 'Secretariat Outline'. Even at this early stage, privacy was included in the draft as a traditionally accepted additional right. This could be considered as the first attempt to bring the concept of privacy into formal rights. An analysis of the work around the formalization of this and the discussions as to its impact on dignity and reputation is key to understanding the nature of the right, its relationship with dignity and indeed how any offshoots of privacy would develop. [59]

This initial drafting, largely considered to have followed the wording of the US constitution, included 'classic' concepts of privacy such as protection of one's home. It also contained a catchall mention of 'privacy' as a whole.[60] The reasoning behind the wording was not clarified despite the Drafting Committee then making substantial amendments to it. However, the Committee provided, in effect, a full guarantee to the right of privacy which was not originally

[56] n 52 see Ishay's commentary on this pp 222,223

[57] These would be reflected in the form of the that the International Covenants and Protocols to such Covenants would take as will be examined in subsequent chapters.

[58] The original members were Eleanor Roosevelt, Peng-chun Chang and Charles Habib Malik but was later was enlarged to include representatives of Australia, Chile, France, the Soviet Union and the United Kingdom, in addition to the representatives of China, France, Lebanon and the United States after representations were made by the Commission on Human Rights to the President of the Economic and Social Council. http://research.un.org/en/undhr/draftingcommittee last accessed 10 March 2017

[59] Document E/CN.4/AC.1/3, Draft Outline of International Bill of Rights. This document contains forty-eight articles outlining individual human rights. Art 11; No one shall be subjected to arbitrary searches or seizures, or to unreasonable interference with his person, home, family relations, reputation, privacy, activities, or personal property. The secrecy of correspondence shall be respected. available at https://research.un.org/en/undhr/draftingcommittee/1

[60] US Constitution, 4th 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, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.' available at https://constitution.congress.gov/constitution/

contemplated at the time of the initial drafting of the Universal Declaration. Diggelmann has pointed out however that, in today's era of increased technology and social media, the guarantee of the right to privacy became a key right emphasizing how the development, in particular of privacy, is of increased importance in creating the foundations of the right to be forgotten.[61] In his view there are two competing claims for privacy, firstly, of being left alone, i.e. creating distance between oneself and society, and secondly, to protect the deep rooted norms of society, and being linked to what he calls 'intimate relationship' or public reputation, also referred to as public dignity.[62]

In understanding the limitations ultimately placed on the right of privacy and its relationship with dignity and reputation, the second session of the Commission of Human Rights provides vital further insight.[63] The process was divided into three activities.[64] The decision to proceed on agreeing each area separately through three working groups was intended to create an alignment of the principles, and to ensure agreement was reached more rapidly.[65] The original drafting Committee looked at the principles [66] proposing the wording for privacy. [67] This was then subject to several reviews before finally being submitted at the beginning of 1948 to the United Nations Economic and Social Council ("ECOSOC")[68] and its Member States for comments. A subsequent draft was then sent by the Commission on Human Rights to the

[61] Oliver Diggelmann, Maria Nicole Cleis, 'How the Right to Privacy became a Human Right', [2014] HRLR 442 'In our age of information technology and electronic media, the integral guarantee of a right to privacy became a key right. Secondly, the importance of the right contrasts with the uncertainties about its conceptual basis. '
[62] ibid Diggelmann, Cleis, p 442
[63] The Second Session took place between 3 May and 21 May 1948 in New York. Here various bodies were consulted in order for a final report to be made. This was then placed before the third session of the Commission on Human Rights, E/CN.4/95. available at https://research.un.org/en/undhr/draftingcommittee/2
[64] The first being the drafting of the general principles, the second the preparation for the legally binding guarantees and finally the plans for implementation.
[65] This was intended to be shorter in comparison to the time taken to reach agreement of detailed requirements of a convention.
[66] The core principles of the Universal Declaration were agreed to be based on universality, interdependence and indivisibility, equality and non-discrimination, and that human rights simultaneously entail both rights and obligations from duty bearers and rights owners, available at https://www.un.org/en/sections/universal-declaration/human-rights-law/index.html
[67] Article 12 - Everyone shall be entitled to protection under law from un-reasonable interference with his reputation, his privacy and his family. His home and correspondence' shall be inviolable. http://www.un.org/en/ga/search/view_doc.asp?symbol=E/CN.4/77/ANNEXA
[68] www.un.org/en/ecosoc the original member states included 51 countries

ECOSOC finally to the General Assembly for approval. An examination of the proposed wording shows the wording contained in the Secretariat Outline[69] as follows;

> 'No one should be subjected to arbitrary searches or seizures or to unreasonable interference with his person, home, family relations, reputation, privacy, activities or personal property. The secrecy of correspondence should be protected'.[70]

Compared to the US constitution, this wording included what would now be viewed as classic concepts of privacy,[71] however it also detailed a wider range where protection should apply not merely to the person, but to his home, family and, in an initial acknowledgement of its importance, his reputation. The idea of the sanctity of an individual's home and his family had emerged before as consistent with an individual's right to privacy, but the idea of reputation seemed new and one that also bought in earlier notions of dignity as a fundamental human right.[72] If privacy could be seen to include the idea of reputation, then such protection was being widened so as to include how an individual was portrayed through access to private aspects of their life.[73] Regrettably, as pointed out by Diggelmann and Cleis[74], the records of the discussions do not throw any real light on why the word 'privacy' was included in the list but not as an umbrella term. This would have made more sense in creating sub-divisions of privacy which could have been refined as changes in societies challenged preconceived ideas of privacy. This is illustrated by the development of accessible personal information through the Internet. Certainly, this would have clarified the value being placed on a right to be forgotten as part of a growing awareness that personal information could impact an individual's privacy and reputation.

---

[69] Drafting Commission Report on an International Bill of Rights on its First Session 1 July 1947 E/CN/.4/21 (Annex A)

[70] Drafting Commission Report (Secretariat Outline) http://research.un.org/en/undhr/draftingcommittee/1 last accessed 23 May 2017

[71] Jeremy Waldron**, '**Is Dignity the Foundation of Human Rights?' **in (**eds) Rowan Cruft, S. Matthew Liao, Massimo Renzo, Philosophical Foundations of Human Rights (OUP 2015)
'Dignity does not figure in the Constitution of the United States, but it is invoked sporadically in American constitutional doctrine.' p 120

[72] ibid Jeremy Waldron**,** He states that the claim for dignity as the foundation of rights 'instructs us to pay attention to questions about dignity.' p 122

[73] The inclusion of privacy as a standalone category almost appears as an afterthought coming fifth in the list.

[74] see n 61 Oliver Diggelmann, Maria Nicole Cleis, p 446

The influence of Professor René Cassin,[75] who had by then joined the Committee, was seen in the draft Declaration submitted to the Commission on Human Rights. Cassin prepared two draft addenda to the original proposal, the first of which (The Initial Draft), for the first time, proposed 'privacy' as an umbrella term with the following wording; 'Private life, the home, correspondence and reputation are inviolable and protected by law.'[76]

The umbrella term used here was 'private life' as opposed to 'privacy'. However, for the second draft the wording was completely changed with the re-introduction of 'privacy.' Again, this was not as an umbrella guarantee, as only certain aspects of privacy were to be protected.[77] This draft also retained recognition of reputation linked with privacy which would later be key to understanding the full application of the right to be forgotten with regard to informational self-determination. [78]

Without any full records of the various discussions and debates that took place, other than some annotations on the draft minutes, it is difficult to see the reasoning on how privacy could be interpreted behind the change of wording. The records that exist do not specify the debates that led to this change, in particular, the need to include 'correspondence.' This inclusion would provide support for wider aspects of privacy which came with the technological advancements, such as email. The introduction of new technology to provide new forms of correspondence by other means of communications opened up further potential loss of privacy with subsequent impact. The position was then complicated by the Working Group on the Declaration of Human Rights[79] further amending and incorporating comments made by various Member States, including reputation once again. There seemed to be little dispute on the idea of a loss or breach of privacy impacting how a person was

[75] Professor Rene Cassis, a leading campaigner and a known jurist, was a supporter of human rights theories and considered a major influence of the drafting of the declaration.
[76] Ist Addendum https://undocs.org/en/E/CN.4/AC.1/3/Add.1
[77] Art 8, Drafting Commission Report Annex 7 'The privacy of the home and of correspondence and respect for reputation shall be protected by the law'
[78] It should be noted that whereas reputation was included in the Universal Declaration this would not be the case in the European Convention of Human Rights despite it being based on Article 12 of the Declaration. It is only contained as an exemption to the right to freedom of expression.
[79] Working Group on the Declaration of Human Rights E/CN.4/53 available at https://research.un.org/en/undhr/chr/2

viewed in society or impacting an individual's position in society. This resulted in a new draft, with 'privacy', interestingly, being accorded a secondary position to reputation.[80]

However, the subsequent draft then removed the references to 'privacy' and 'private life'.[81] Research carried out by Diggelmann[82] does not offer an explanation for this as records do not show any debate as to the change of approach. Diggelmann does suggest that the influence of the United States may have prevailed, as they had previously put forward a similar provision. According to the records, it seemed that debates centered on whether family life should be included, and whether the provision should be considered as a guarantee offering either 'protection' or freedom from interference. However, the next draft re-positioned 'privacy' as an umbrella provision providing that: 'no one shall be subjected to unreasonable interference with his privacy, family, home, correspondence or reputation.'[83] This draft then went to the General Assembly[84] where it received further, but minor, amendments, ultimately becoming Article 12 of the UDHR. [85]

It is difficult to clearly understand not just the variations of the wording of this right, but the arguments around the changes. Here Diggelmann argues that the impact of translations, i.e. from the French viewpoint of Cassin to the Chinese comments and proposals, should not be underestimated.[86] Interestingly, the document 'Human Rights Commission Members Observations', submitted to the Drafting Committee at the same time as the Secretariat Outline, [87] did not refer to any state's constitution that contained an umbrella term of privacy

[80] This stated 'Everyone shall be entitled to protection under the law from unreasonable interference with his reputation, his privacy and his family. His home and correspondence shall be inviolable.'
[81] 'Everyone is entitled to protection under the law from unreasonable interferences with reputation, family, home or correspondence' Drafting Commission Report 95 Article 9
[82] see n 61 Oliver Diggelmann, Maria Nicole Cleis, 'The United States had suggested a provision with a very similar wording in their comment. It is likely that the participants thought that they made only minor editorial changes when they altered the wording. The Australian representative explicitly called the texts 'very similar'
[83] This appears to have been finally influenced by a proposal noted as being put forward by Chinese representatives although once again there are no detailed records recording the debate.
[84] Drafting Commission Documented Outline, available at http://research.un.org/en/undhr/draftingcommittee/1 E/CN.4/AC.1/3/ADD.3
[85] This stated "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."
[86] see n 61 Diggelmann, Maria Nicole Cleis, p 448
[87] see https://research.un.org/en/undhr/draftingcommittee/1

or private life. Neither the United States nor France had expressly provided for such recourse in their bill of rights. A closer look at other drafts presented, such as the Draft Declaration of the International Rights and Duties of Man' submitted by Chile[88] as drawn by the Inter American Juridical Committee[89], contained suggestions that allowed for the protection of 'the inviolability of the individual and his correspondence' under a provision for the right to personal liberty.' The linking of these aspects of privacy with one of the most fundamental human rights, namely liberty, provided more depth and scope to expand upon the more limited protection intended by mere privacy.

In 1968, as recognition of the perceived need to identify and separate the categories of human rights to provide the two sets of rights referred to earlier, proposals were made for civil and political rights, with separate economic, social and cultural rights to recognize rights more representative of the changes in societies. Two new protocols to the UDHR were subsequently drafted. The International Covenant on Civil and Political Rights[90] (ICCPR), which was primarily concerned with personal liberties and equality[91], and the International Covenant on Economic, Social and Cultural Rights (ICSECR) [92] for essentials for life, economic security and cultural identity.[93] Despite any reservations as to the how the value of privacy could be attributed, it was however widely accepted as a recognised civil and political human right.[94] Recognition of dignity underlying the UDHR[95] has been considered the main

[88] It can also be seen as noted by Diggelmann that such proposals by the South American states were also useful in the early stages of the creation of global treaties.
[89] available at http://www.oas.org/en/sla/iajc/ last accessed dec2020
[90] ICCPR (adopted 16 Dec 1966 entered into force 23 March 1976) 999 UNTS 171
[91] The ICCPR in particular has since been ratified by 168 states. However, with 193 Member States to the UN, it is clearly an area where agreement is still sought. In particular there are a number of states, being predominantly Muslim states, who have not ratified the Protocols such as Malaysia, Saudi Arabia, Qatar and UAE, where freedom of religion remains an issue.
[92] ICESCR (adopted 16 Dec 1966 entered into force 3 January 1976) 993 UNTS 3
[93] Substantial debates reflecting the problematic nature of distinguishing between such specific rights had resulted in the article-by-article negotiations taking over 18 years before conclusion between 1955-1966. with ratification over several years
[94] 'Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech.' Definition of Privacy as defined by Global Internet Liberty Campaign available at http://gilc.org/privacy/survey/intro.html last assessed 25 Feb 2020
[95] Article 22; Everyone, as a member of society, has the right to social security and is entitled to realization, through national effort and international cooperation and in accordance with the organization and resources of each State, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality.

component to privacy[96] whilst the idea of reputation as a concept despite also forming part of privacy and contributing to an individual's dignity has had less focus.[97] The length of the discussion and the amount of redrafts may have proved their worth in future developments. These culminated in the protection for privacy, as contained in the ICCPR, being almost identical[98] to those contained in the UDHR, with the breadth of the ICCPR having increased to provide for 'unlawful' attacks.'[99] Once again it was confirmed that the rights 'derive from the inherent dignity of the human person.'[100]

By 1966 it did seem as if any debate had been resolved, with a formal statement recognizing that as most, if not all, countries had constitutions that protected 'privacy, the sanctity of the home, the secrecy of correspondence and the honour and reputation of individuals.'[101] This approach as set out in the earlier report meant privacy would therefore be included. This seems an idealized approach with very few member states actually providing any such formal protection to it within their own constitutions. Concern remained that privacy might still become a uniform right presenting further challenges for human rights by then requiring universal application in all legal systems. A compromise was effectively reached with the decision that each state would be able to determine the applicability of the right within their own territory.

The UDHR and the ICCPR, together with the ICESCR followed through by other binding treaties in various jurisdictions, have advanced the position with regard to all individuals being

[96] See Jergen Habermas, 'The concept of Human Dignity and the Realistic Utopia of Human Right, The crisis of the European Union: A Response,' (2010) Wiley online, Metaphilospohy Vol 41 Iss 4, July 2010 pp 464-480

[97] In fact, it is only since 2003 that protection of reputation has been recognised by the Court since it was not included in the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") Despite being included in the Universal Declaration only being referred to as part of Article 10 (2) with the right of freedom of expression which provides expressly for an exemption to such right '…. for the protection of health or morals, ***for the protection of the reputation or the rights of others***, (emphasis added) for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

[98] Although there were close links between the drafting of these two declarations, the similarity of wording was not a short cut but represented earlier discussions and in particular what was referred to as the British draft Bill of International Rights initially part of intended discussions behind an International Bill of Rights.

[99] '1. No one shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence not to unlawful attacks on his honour and reputation 2. Everyone has the right to the protection of the law against such interference.'

[100] Preamble to the ICCPR available at https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

[101] Commission on Human Rights Report on its 9th Session 6 June 1953, 2447 para 67

entitled to ensure the state provides for more than basic human needs. Wider definitions of privacy and enhanced recognition of reputation would then be required to make way for the increasing need to protect personal information or data. This could be seen as early as 1988 from when the state was obligated to protect privacy with regard to data with particular provision being made in General Comment 16 by the UN Human Rights Committee:

'The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant.' [102]

The use of privacy, based on observing a right of dignity, was key to finding a right to be forgotten, but the ability to exercise autonomy also influenced the ability to control the use of personal information. It could be argued that the right to be forgotten is a manifestation of autonomy, for choosing the way in which the personal data is going to be used. This helps to support its function as a mechanism for the protection of reputation and dignity.

Ensuring that privacy could continue to be protected in the new world of potential intrusion with an individual striving to maintain privacy would increasingly be seen to be difficult. In addition, ensuring dignity and protection of reputation where personal information is made readily available would become more challenging and an issue that would be taken up primarily within Europe.

2.4.2 The further development of rights within Europe

Generally, it was considered that the western world, led by the US, initiated the formalization of human rights. However, such rights truly expanded with the establishment of the

[102] Office of the High Commissioner of Human Rights, UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, available http://www.refworld.org/docid/453883f922.html last accessed 30 June 2020

European approach seen in the European Convention on Human Rights (ECHR). [103] This was created by the Council of Europe then providing the first comprehensive treaty in the world. It uniquely contained an international complaints procedure prompted by a desire to involve all non-communist countries. A similar provision for privacy as set out in the ICCPR (Article 17) was included in the ECHR (Article 8). [104]

After the atrocities of the Second World War within Europe, there was a perceived need for measures to be taken to not only maintain, but to realize human rights with fundamental freedoms. Mowbray[105] considers that the first steps to this were through the Consultative Assembly proceeding as a Committee on Legal and Administrative Questions[106]. The work of this Committee was influenced significantly by the approach of the UDHR, and also by certain recommendations of the International Committee of the Movement for European Unit.[107] In addition there was input from the International Judicial Section of the Committee which drew up the draft ECHR. Here, Teitgen was an advocate, including various aspects of privacy, arguing for privacy to be covered by an umbrella term of 'private life' expanding the coverage provided. However, approval was difficult to obtain and was even challenged by the British representative, possibly reflecting the view taken of privacy by the British legal system.[108]

[103] European Convention on Human Rights 1950 as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13

[104] Art 8 - Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[105] Alistair Mowbray, *Cases Materials and Commentary on the European Convention on Human Rights* (PUP 3rd Ed 2012) ch 2

[106] Several non-governmental groups after the war came together to form this Committee and included two notable persons in Sir David Maxwell–Fyfe who had served as a law officer in Churchill's Government, before acting as the lead British prosecutor at the Nuremberg trials and Pierre–Henri Teitgen, a resistance hero and later Minister for Justice in post-occupation France. The Committee comprised of 24 lawyer-delegates, of which Fyfe became chair and Teitgen the rapporteur.

[107] This was set up in 1947 and intended to involve leading European politicians to promote European unity creating by 1948 the European Movement available at https://www.cvce.eu/en/unit-content/-/unit/04bfa990-86bc-402f-a633-11f39c9247c4/5e4d62cb-3849-434e-ac34-32b989d37059 last accessed 20 April 2020

[108] A common law approach in England meant that ideas of privacy were developed by judicial precedent not by statute, meaning there was no formal recognition of privacy nor formal acceptance as a right to privacy as such, although other remedies existed such as the tort of breach of confidence. It was not until the UK adopted the Human Rights Act 1998 (c42) which came into force on 2 Oct 2000 incorporating the provisions of C42 to implement the European Convention on Human Rights which was signed and enacted in 1953. Until this time privacy had not been enforceable within the UK's courts.

Underlying all of these discussions was the question of dignity and it may be argued that this reflected abuse, which had been a feature of the atrocities of the war with more emphasis placed on the importance of privacy due to the barbaric nature of the racism and genocide of the war. Similar to the experience of the UDHR, there seemed no clear intent behind the use of the words 'private life' and 'privacy' in the convention nor any building of a guarantee of such a right. It does not seem as if there were any logical steps to deciding the extent of the right nor the beliefs or understanding behind them. [109] However, what was clear was that it was considered essential to secure autonomy for the individual in private matters[110] leading to recognition of what can be referred to as three dimensions of the right i.e. the right for privacy, respect of communications in the form of correspondence, and respect of the home. [111] All of these would ultimately be incorporated within a wider interpretation of the right to be forgotten.[112]

With reference to protection of one's private life as opposed to a general 'privacy,' protection, Kalin and Kunzl[113] argue that this is a more comprehensive concept and one which could encompass the right to respect for privacy, the right to family as well as the right to marry and found a family. Generally, it could be seen to continue the promotion of autonomy as essential to a person's wellbeing, i.e., that each person has such right enabling them to make decisions relating to their personal matters which could include relationships, beliefs and lifestyle. This emphasis on autonomy would also extend to ideas of protecting reputation and ultimately how a person was perceived within their society. Neil argues that autonomy can

[109] Awareness of alternative fledgling movements such as communism was reflected in the detailed notes of the preparations of the work involved in activating the Convention. The detail of the debates appeared to have paid off as in contrast to the various debates for the UDHR, the draft was submitted to the Consultative Assembly in September 1949 without lengthy debate and was then incorporated into the recommendation to the Committee of Ministers. The next hurdle was greater as it passed to the Committee of Experts. The revised draft, which mirrored the UDHR alternatives, was proposed and in particular Alternative which detailed protection of privacy. Eventually the drafts were combined and without records of the discussions being available the end version reached

[110] The Committee of Ministers of the Council of Europe expressly authorized the Consultative Assembly to include such measures that would achieve the stated aim of the Council 'in regard to the maintenance and further realization of Human Rights and fundamental freedoms see Alistair Mowbray, *Cases, Materials and Commentary on the European Convention on Human Rights* (3rd ed OUP 2012)

[111] Article 8, Respect for private and family life; 1. Everyone has the right to respect for his private and family life, his home and his correspondence.

[112] This will be explored in later chapters when looking at the joined case of NT1 & NT 2 v Google LLC [2018] EWHC 799 (QB)

[113] Walter Kalin, Jorg Kunzl, *The Law of International Human Rights Protection* (OUP 2009) ch 12, 381

be reflected in the ability to control certain types of information about yourself.[114] Kalin and Kunzl also argue that a further component of privacy is the right to protection of a person's honour and reputation which can impact a person's social standing.[115] Here, the link to the ability under the right to be forgotten to keep control over a public digital portrayal of oneself which potentially impacts reputation and social status becomes more established.

What is then of significant interest in viewing this understanding of privacy in the context of a right to be forgotten is whether a potential additional component supporting the right to one's own identity and the ability to control personal information which may impact it exists. This was particularly pertinent within Europe due to its history of personality rights. This approach was confirmed in a decision where a state's refusal to allow an individual a change of name to reflect a change of religion was a violation of the right to privacy under Article 17 of the ICCPR [116]. In the judgment, it was made very clear that restrictions on names would constitute such a violation and it specifically extended its opinion to include a mandatory change of name.[117] In addition as provided by the ECHR, privacy could include a right to protection for a person's honour and potentially reputation as part of the requirements enabling individuals the freedom necessary to develop their own personality or identity and to maintain their sense of self.[118] Article 8 of the ECHR could be considered to guarantee this, as does the ICCPR, with similar provisions being contained in other conventions.[119] Cases

[114] Elizabeth Neil: *Rites of Privacy and the Privacy Trade: On the Limits of Protection for the Self,* 3 4 5 (McGill-Queen's University Press 2001) pp 25-26, see also Jaunius Gumbis, Jurgita Randakeviciute, Vytaute Bacianskaite, 'Do Human Rights Guarantee Autonomy?' 2008, Cuadernos constitucionales de la Cátedra Fadrique Furió Ceriol, ISSN 1135-0679, No 62-63, 2008, p 81 ' The conditions necessary for autonomy can be divided into two categories: internal and external. An autonomous individual must know what he/she wants to achieve, but he/she must also live in a favourable environment that provides means and resources to facilitate the realization of one's potential.'

[115] See n 113 Walter Kalin, Jorg Kunzl, p388 where the authors argue that a state should not undermine a person's honour and reutation and must also ensure that attacks on such are not made by other parties. See also Birindwa and Tshisekedi v Zaire, Human Rights Committee Com Nos 241/1987, 242/1987

[116] Coeriel & Aurik v The Netherlands, Com no 453/1991 1995 para 10.2-10.5

[117] The Committee is of the view that a person's surname constitutes an important component of one's identity and that the protection against arbitrary or unlawful interference with one's privacy includes the protection against arbitrary or unlawful interference with the right to choose and change one's own name. For instance, if a State were to compel all foreigners to change their surnames, this would constitute interference in contravention of article 17.

[118] This was summed up in the case of Denisov v Ukraine 25 Sept 2018 76639/11, [2018] ECHR 1061, where the court provided an up to date summary of the current Art 8 case law confirming a person's reputation forms part of their personal identity (para 96)

[119] African (Banjul) Charter on Human and Peoples' Rights

have interpreted this so that state must not only ensure that it does not undermine a person's honour and reputation[120], but that it also provides remedies against attacks by other entities. These would include such private enterprises as the Internet giants. It must be noted, however, that the right to privacy cannot be considered an absolute right and under the ECHR, proportional interference may be permitted where required for the protection of others. Regrettably, the ability to provide limitations on both privacy and reputation, as well as other rights such as freedom of expression, ultimately results in uncertainty as to the extent of protection and the provision of a platform for the right to be forgotten to gain validity.

2.5 Development of concepts of privacy, dignity and reputation within human right theories

Whilst states determine how to provide for accepted human rights, various theories have developed to establish why and how such rights have emerged. Although acknowledging the philosophies behind these rights which concerned the theory or theories of why such rights which potentially underlay the right to be forgotten (namely privacy but also dignity and reputation) came to be so accepted within human rights these may lead to how recognition of the right to be forgotten would ultimately take place. As a starting point, I will consider the words of Andrew Chapman;

'Unless we understand some of the driving forces behind human rights, we risk missing the currents that will determine its future direction.' [121]

The ability to provide for newer forms of rights, or interpret rights according to changes in society, must be essential to maintaining their continuous value. A more detailed examination of the various human right theories is helpful in analysing how a new right, such as the right to be forgotten, could arise, particularly where the existence of rights can be argued to be universal or provided through cultural interpretation of the need for such rights. Questions that need to be considered include; who has the ability to determine which so-called rights

(Adopted 27 June 1981,) OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entered into force 21 October 1986) Art 11.

[120] Birindwa & Tshisekedi v Zaire Com No 241/1987 and 242/1987 (1989) para 12.7

[121] Andrew Chapman, *Human Rights -A Very Short Introduction*, (OUP 2007) p 24

are worthy of protection and whether such rights really exist? Where there may be a moral understanding, as examined earlier, that no-one has the right to take another person's life, then how are rights such as privacy and freedom of expression justified within such claims? Within theories or accounts of human rights, the basis of such recognition can be considered and how such theory adapts to new categories of rights as required to deal the challenges of current times, such as the right to be forgotten.[122]

The ideology of human rights has developed into two main themes, the first being that of universalism and the second of (cultural) realism. These movements take differing approaches with initially the universalism approach, arguing that fundamental rights apply to all as being the basis of human rights. This can be compared to the approach of realists who believe that rights can only exist where the relevant culture has determined the depth or scope of such rights.

2.5.1 The Universal argument

Within the universal approach, human rights need to have three qualities; they are natural, i.e. inherent, they are equal, so applicable to everyone, and they are universal, so applicable everywhere.[123] However, even if these qualities are met, a human right only becomes meaningful, in the opinion of Hunt[124], if it gains political content, i.e. if it is accepted as having value. These are rights of citizens within society and therefore, their place in society can only be enforced or met should society recognize and demand that this is done.

Key to understanding the universal approach is the phrase 'inherent dignity' i.e. that it is natural for man to be provided with whatever protection necessary to secure this.[125] This requirement increases the difficulty of trying to meet the challenge of how human rights can

[122] Elsa Stamatopoulou*, '*Cultural Rights in International Law' (2007*)* EJIL Vol 21 Issue 4 1111-1115. However, in the view of Stamatopoulou's '*minimum core obligations* are particularly useful in the case of cultural rights, which are often viewed as a luxury that governments should pay attention to only after fulfilling other more basic needs of the population.' Although it is accepted that there is a need for expansion of rights to deal with fast moving societal or technological changes, the ability to do so rests on state actions which are often slow and unresponsive

[123] Lynn Hunt, *Inventing Human Rights*, (WW Norton & Co. 2007)

[124] ibid Lynn Hunt p 21

[125] ibid Lynn Hunt, p 21 She argues that this was seen in the acceptance of the American Declaration of Independence 1776 and the French Declaration of the Rights of Man and Citizens 1789

be universal if they are not universally recognized. This conundrum becomes increasingly important when categories of human rights were proposed in global treaties and conventions.

In contrast to ideas of universalism, other authors, such as Bentham[126] who, as the founder of utilitarianism, famously called human rights 'nonsense on sticks', focused on the argument that it is necessary to take a realistic view of the world and be aware that human rights cannot exist over and above the 'state,' that dependency on the 'state' is fundamental, and anything else is in 'the imagination of believers in Utopia'. However, the first ideas of privacy began to emerge from some of Bentham's discussions. In particular, he looked at the impact of surveillance in a prison and its effect on prisoners' behaviour.[127] In this study, he discovered that even the belief that they were being watched affected their behaviour to such an extent that independence was lost and the prisoners conformed.[128] This experiment was also explained in Foucault's social's control theory with lesser invasive means of control[129]. This theory on the impact of being observed acknowledged that individuals adjusted their behaviour under the psychological effect of knowing that there was constant observation. Therefore, power passed from an autonomous person to the observer, often seen as the state, prompting an "anxious awareness of being observed".[130] To protect the agency of an individual, a right to privacy could enable an individual to choose how to behave, perhaps introducing the first glimmers of the autonomy required.

However, Bentham's thoughts were that if the state was not obliged to treat all citizens equally, the use of punishment and reward could then be claimed to motivate individuals to moderate behaviours. John Locke, deemed to be the founder of the Age of Enlightenment, which was fundamental to the development of 'western' ideas in the United States and

[126] Jeremy Bentham, *Utilitarianism*, 1789 (re published by Broadview Press 2000)
[127] Michel Foucault, *Discipline & Punish* (1975) in *Panopticism III.: The Birth of the Prison* (NY: Vintage Books 1995) translated from the French by Alan Sheridan 1977
[128] This led Bentham to prepare an idealized version of a self-controlling prison called the "Panopticon" — a model prison where all prisoners would be observable by (unseen) guards at all times
[129] see n127 Michel Foucault.
[130] see n127 Foucault p 201 "Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should tend to render its actual exercise unnecessary"

France, saw a similar version of moral wellbeing essential to humanity as part of a universal theory of human rights. He was able to influence both the ideas expressed in the American Declaration of Independence and the French Declaration of the Rights of Man, which proclaimed 17 rights as "the natural, inalienable and sacred rights of man". His views on self and identity, believed to be the initiators of movements in philosophy led by Rousseau and Kant, argued that man is fundamentally good and that all men are equal and independent needing a civic society in order to resolve conflicts in a just way;[131]

> 'Men being as has been said by nature all free equal and independent no one can be put out of this estate and subjected to the political power of another without his own consent.'

He considered the only way whereby anyone could forego natural liberty and put on the 'bonds of civil society' is by agreeing with others to unite into a community for their comfortable, safe and peaceable living, with greater security against any potential outsiders. He viewed autonomy as being effectively waived in order that man could live in a society where a form of social order was preserved.

Similarly, Blackstone, writing on the rights of man[132], took the view that the individual should be considered a free agent endowed with the discernment to differentiate good from evil, and that key to this was the ability to empathize and to understand the impact of actions. His view involved the concept of moral autonomy providing the ability to reason, and independence to decide for oneself, but combined with the rule of law to regulate the absolute rights of individuals. His approach to the 'natural liberty of man' was an essential part of the thinking of the supporters of a natural law theory which should therefore be applied to all universally. From these writers, it is clear that autonomy was a key component of human rights and one that would underpin any concept of privacy.

---

[131] John Locke, *The Second Treatise of Government*, (1690, reprinted New York, MacMillan 1986) Ch 8, Second Treatise p 766

[132] Sir William Blackstone *Commentaries on the Laws of England,* (originally published by the Clarendon Press 1765–1770) available at https://avalon.law.yale.edu/subject_menus/blackstone.asp

2.5.2 Cultural Realism

The realist movement was often represented by Hobbes[133] who, in contrast to Blackstone,[134] took the view that mankind is formed as inherently bad. His view was that each man was out for the most he could get and, if some were more powerful than others, they would look to impose their will on the weaker. Despite the extremely gloomy picture he painted of humanity, he reluctantly conceded that, as man is possessed of reason, he can have insight into the conditions that nature may have evoked. Influences on the perception of rights or in the views of those set out below, the 'invention' or creation' of such rights involved the law in, not only regulating or attempting to do so, but with categorizing the forms of rights and looking at potential enforcement. This could be called the Realist view of human rights theory although such theory was soon to develop and broaden.

From this thinking, a second theory emerged which today is called cultural realism or cultural relativism. Cultural realism can be considered to be based on a premise that rights/ morals embedded in many different cultures, create a varying form of morality and therefore the theory of the universality of human rights cannot apply. It is therefore a question as to whether such cultural issues can or should form, and be included in, the category of human rights. One of the issues that highlight the difficulties in categorizing human rights is that of establishing reasonable and general grounds for making moral judgments about the actions of another's culture. A cultural relativist challenges the claim that human rights need to be universal and, even with belief of the inherent goodness in man as expressed by Lock and Bentham, argues that many cultures do not believe in those human rights as described by western societies, as their societies are based on fundamentally differing values and beliefs. This is an argument that could be used with regard to privacy which, as shown previously would be affected by cultural views.

[133] Thomas Hobbes "*Leviathan; or the Matter, Form, and Power of a Commonwealth, Ecclesiastical and Civil*" (first published 1651 reprinted Penguin 1985)

[134] see n132, Sir William Blackstone, Here Blackstone took the view that man's rights were not given politically but through God, i.e. were laws of nature although the state should protect such rights for the people

These views were subsequently developed by Rene Cassin[135], into an accepted view of human rights that autonomy of the individual provided acceptance of an individual's ability to separate out and have control over his being. Cassin was also able to build on the concept of an autonomous person being in the position of being a right holder and, in theory at least, being able to enforce such a right against the state. How one would be presented in society highlighted autonomy as the right to be able to exercise free will in such circumstances, and with dignity, so that one would be viewed without censor. The idea of reputation would also follow, as the need to maintain a role in society became of increasing importance. Without an opportunity to determine how one's life could be led, there would be little opportunity to exercise any right of privacy. Here, such concepts introduced ideas of the ability to exercise control over aspects of life which would ultimately be considered essential in the pursuit of protection for personal information and the ability to erase or forget information which directly impacted perception of oneself and how one is portrayed in society.

The next step to consider is how can one reconcile these this competing claim of cultural relativism with universal theory particularly regarding privacy, its development, and the path to the right to be forgotten. Jack Donnelly[136] argues that there are two extremes of cultural relativism, namely radical cultural relativism and radical universalism. The radical relativism says culture is the sole source of the validity of a right which is expressed to be moral. However, radical universalism argues that culture is irrelevant. Furthermore, in Donnelly's view, the position is controlled by concepts of strong and weak cultural relativism.

For strong cultural relativism, there is a claim that culture is the principal source of a moral right but that the universality of human nature and rights serve as a restriction on potential excesses. Here, some basic rights would be accepted with apparent universal applications but there would be a wide range of variation with notions of human nature and dignity that must influence such variation. However, Donnelly argues that weak cultural relativism permits limited deviations from universal human rights standards.[137] He looks at arguments that

[135] Cassin was previously the French delegate to the League of Nations from 1924 to 1938, then a draftsperson on the Universal Declaration and then also a member (1959–1965) and president (1965–1968) of the European Court of Human Rights.
[136] Jack Donnelly, 'Cultural Relativism and Universal Human Rights' (1984) HRQ vol 6 no 4, 400 -419
[137] ibid Jack Donnelly p 401

culture must be an important factor in the validity of a moral right with only a weak acceptance of universality, again, as a check on excesses. Therefore, cultural relativity can be used in the interpretation of rights based on culture. This is a 'logical contradiction'. If human rights are based on nature, and if the fact that a person is a human being then he has rights that are considered universal, how then can culture make them relative. He does not argue using cultural aspects to say that rights are not universal, but agrees that some rights cannot be universally accepted. This provides an understanding that the right to be forgotten can still exist even if not universally accepted or applied. Universal relativism can therefore be based on moral autonomy, as argued by many other theorists, and communal self-determination. However, his view that is the source of human rights is man's moral nature, linked loosely not just to life, but a life of dignity and social acceptance.[138] Again, the focus of human rights seems to be attached to the idea of the inherent dignity of a human being.

Donnelly further argues that as all human nature must, in some ways, be relative as everyone is subject to their own influences, so, he believes, can these 'significantly influence presence and expression of less easily quantifiable aspects of human nature.'[139] Thus, culture contributing to the shaping of individuals is systemic and can lead to the pre-dominance of specific social types in various cultures. If one can accept that one cannot force one's own beliefs/ codes on another person from another culture, then it is clear that human rights must be variable according to culture. However, the question is to what extent. Donnelly argues that a form of radical cultural relativism can mean that there are no actual 'human rights', i.e. the rights that one holds merely from being a human, but rights that benefit all of mankind. This is an opposing approach to that of universalism.

Although the history of early rights, as expanded upon by authors such as Ishay,[140] show arguments for fundamental rights, Donnelly believes that pre –modern societies did in fact define people by their social status or group membership, thus cultural influences were in place from early times. This argument can be seen to apply to various cultures, and even the western world, with differentiation in rights granted or, more importantly, not granted to

[138] n136 Jack Donnelly pp 414,415
[139] n136 Jack Donnelly p 403
[140] Micheline Ishay, *The History of Human Rights,* (University of California Press, 2nd ed 2008)

slaves and women. He questions whether the very nature of human nature means that it actually requires cross cultural variations in human rights. If it is accepted that certain behaviours are universally considered to be wrong, do these then set the standard for fundamental rights?[141] Thus it can be argued that there is an aspect of international law that provides a moral platform to 'condemn' forms of universal practice against human codes or rights. Donnelly believes it is possible for a radical form of cultural relativism to be argued in that human rights cannot exist as there is no universality and the process of natural law is really only intended to protect what is a most basic of rights, i.e. to protect human dignity.

However, dignity by its nature must be subject to interpretation according to the culture or society codes of behaviour. For an internal evaluation, there needs to be an examination of whether the action is acceptable within the codes of conduct of that particular society. If not, then there is no defence even on the basis of cultural evaluation and, certainly, universalism cannot apply. For an external evaluation, the examination needs to be conducted from an outsider's viewpoint (although Donnelly suggests this should be a moderated view).[142] There is emphasis on relativism being based on the idea of a moral autonomy and, for him, communal self-determination, which I understand to be that the individual makes decisions for themselves but based on acceptability of such decisions within their form of community. This potentially creates the idea of reputation as being the image that is portrayed and accepted within a society. There has to be some form of external evaluation away from such community to provide such a viewpoint. However, Donnelly considers that to choose between internal and external is itself a decision suggesting autonomy even in this decision making. However, once again, the rules of the particular society can be very strong and difficult to evaluate from an outsider's viewpoint, particularly when this is a westernized role. Very weak cultural relativism i.e. where there are not strong cultural or community based requirements to behave in a certain way can mirror arguments by relatively strong universalists that human rights are applicable to all. This reflects the same factors that make it difficult to draw distinctions with any precision between the form of right or its

[141] For example, this could include the right to life. Other rights such as the right not to be tortured if so does this then promote the arguments for universal human rights which have subsequently been reflected in international agreements and treaties.

[142] Jack Donnelly, Universal Human Rights in Theory and Practice 3rd ed (Cornell University Press 2013) Part 2 ch 6 pp 109-118

interpretation. These arguments help build up the requirements needed not merely for autonomy, dignity and potential privacy to benefit, but also ideas of reputation that also emerge with acknowledgment that there is an element involving acceptability from the community.

Cultural relativism can look at the indigenous societies' position and argue that certain principles of human rights cannot apply as other means are used to 'protect' and realize defensible mechanisms of human dignity.[143] Indeed, it can seem to be beyond intrusive to interfere and impose western ideas of 'universal' human rights onto such societies. Donnelly argues[144] further that such independent autonomous communities are, in fact, now rare as many of the people most in need of recognition of human rights are actually based in larger communities with growing deprived populations. Dual societies can accommodate both old and new practices, either incomplete westernization or take a too enthusiastic acceptance of western value and practices to the detriment of their own. He challenges whether the presence of strong cultural ties means that such communities should not be allowed the benefit of human rights, certainly not to the extent that the inappropriateness of western rights prevent any rights being given. Rights must be also be individualistic, thus held by persons even against state and society.

Clearly, similarities exist in what a human being is entitled to some rights by virtue of being a human in particular, liberty and protection from inhuman and degrading treatment which suggest a 'central core' of human nature usually based in dignity and autonomy. Human rights are needed more than ever to provide an individual who may have lost the form and protection of a smaller more traditional organized society or community[145], and to offset

[143] Jack Donnelly, 'Human Rights and Human Dignity: An Analytic Critique of Non-Western Conceptions of Human Rights' The American Political Science Review, Vol. 76, No. 2 (Jun 1982), pp. 303-316 Donnelly argues that particularly in non Western cultures there are 'elaborate systems of human duties which are designed for the protection of human dignity.' He also states that 'available regularized social protections of many of the values and interests which in the West are protected through individual human and legal rights. See also Fernando R. Tesón, 'International Human Rights and Cultural Relativism', 25 VA. J. INT'L L. (1985), pp 869- 898 who states that relativists claim substantive human rights standards vary among different cultures and necessarily reflect national idiosyncrasies. He explains that what may be regarded as a human rights violation in one society could be considered lawful in another, and that Western ideas of human rights should not be imposed upon such societies

[144] n 136 Jack Donnelly p 410, 411

[145] n 142 Jack Donnelly p 107

some of the increased vulnerabilities of this technological environment.[146]With the growth of both traditional and modern threats to human dignity, this is where the need for additional rights becomes more important with regard to a person's private life. Donnelly confirms that privacy, as seen in Article 12 of the Universal Declaration, is a modern right providing recourse to an individual to ensure his autonomy but debates as to how relevant is it to the traditional tribal community. Can it be argued that certain such communities are then not entitled to such rights, even from the prying documentary maker? Or can it be argued that such rights apply universally but are tempered by cultural relativism which Donnelly then refers to as weak cultural relativism. Rnegger argues that universal rights should not be fixed in their approach but must be compatible with cultural differences.[147] Another view held by Brown is that rights in general have no specific status being a product of a particular society and understood in a particular way so should not be claimed to be universal whilst this does not impact their desirability.[148] However, it is clear that at least two strands support the concept of human rights within such theories, with the idea of dignity being fundamental to the basis of human rights and autonomy therefore necessary for the exercise of rights.

Therefore, it could be argued that a right to privacy must be considered not only to be linked to the fundamental right of dignity, but also to those of liberty or freedom. Without liberty, there is no ability to conduct one's affairs privately with autonomy, whether of business (letters) or of family matters. Without this ability a human right whether considered to be a universal right or a culturally influence done, cannot be fully realized.

2.5.3 Towards a wider acceptance of rights

The work by Amartya Sen in Freedom and Development[149] also analyses the approaches to recognition of the basis of human rights. He puts forward the view that there are three areas

[146] The rise in social media and the taking part in an online environment has resulted in an active Global Social Media population reaching 4.2 billion users see https://www.statista.com/topics/1164/social-networks/ last accessed 16 Aug 2021. The usage of the Internet and in particular such sites has resulted in a growing awareness of online harms and the development of new crimes such as cyber stalking and revenge porn. The use of such sites as Twitter and the new attack by trolling also compounds these issues. This area of online harms is discussed further in ch 6.

[147] Nicholas Rengger, (2011), 'The World Turned Upside Down? Human Rights and International Relations after 25 Years', *International Affairs*, Vol. 87, No. 5, pp. 1159–1178

[148] Chris Brown, 'Universal human rights: a critique', 1997 Int Journal of Human Rights Vol 1 Iss 2 pp 41-65

[149] Amaryta Sen, *Development as Freedom*, (New York, Knopf 1999) pp 246 -248

of concern when accepting concepts of human rights, i.e., the legitimacy of such rights. It is clear to him that the idea of people coming into the world endowed with certain basic rights is as foreign as the idea of them arriving fully clothed. To have rights, these must be sanctioned by the state /legal authorities, who must have duties to uphold them. The third point he raises is that if human rights are viewed as being ethical then how can these be truly universal as cultures vary in how certain rights are valued, i.e., in turn, raising again the cultural argument. In the first area, which Sen calls the legitimacy argument, he examines views that rights cannot really exist by virtue of being human, considering Marx's view that rights cannot precede the state. [150] He also critiques the thoughts of Jeremy Bentham[151], so that it should be considered essential that instruments give rights not prior ethical grants. Sen further argues that this thinking goes against the idea of human rights being an entitlement, i.e., they are part of being a human. His view is that human rights may be wider in scope than actual enforceable rights. Thus, the existence of privacy together with rights of dignity and even reputation is accepted, whether formally recognized or enacted. Arguing for this, he sets out an example of the moral right of a wife to participate in family decisions. Such right could not and should not be enforced by the state but is a right that arguably should be recognized. A right to respect could also be considered within a set of ethical claims, but would not always be proclaimed as legal rights.

Sen's second argument, the coherence argument, is based around the premise that one can talk about rights without questioning who has the duty to 'guarantee' them. A person's right must be coupled with another's duty for the rights to be recognized or enforced. Immanual Kant calls this argument the 'perfect obligation' whereby a right is matched to a duty to provide for it. Sen argues against this by not accepting that rights can only exist with such duties. In his opinion, it is possible to see rights as things that people should have, irrespective of any obligations to provide them. Again, this supports ideas of concepts such as privacy, dignity, autonomy, as well as forming the basis around the right to be forgotten. As with reputation recognized as a right in the Universal Declaration, but where legal recourse such as defamation fails to support it then as a human right, it can still be valid even if not enforced.

[150] Karl Marx, *On the Jewish Question*, in *Deutsch-Französische Jahrbücher,* 1844
[151] John Bentham, *Utilitarianism* (1789, re published by Broadview Press 2000)

The result of 'imperfect obligations' can be that certain rights may end up potentially unfulfilled. Despite this, Sen regards such rights as still valid, just waiting for assistance to be fulfilled. It is this view that can explain the lack of enforceability often seen with privacy as, even where recognized as a right, there may be an inability to provide what is necessary for the right to be exercised. In many states, not only are concepts of dignity left unexplained and privacy not clearly defined, but remedies in respect of them are limited.

A third argument can be considered the cultural critique. This looks at the specific impact of cultural, primarily Asian, values on the question of universality of human rights. Here, Sen argues that to apply the term 'Asian' does not take into account the varying level of cultural differences. One description could not necessarily apply to all interpretations but in most cultures, importance is attached to specific concepts forming an essential part of human rights. This emphasizes however that cultural differences do not prevent wider acceptance, and this is particularly relevant where privacy and its broader principles are involved.

In looking at the key rights underlying the right to be forgotten, such as the impact on reputation, within such theories, there are also other challenges in considering why privacy should have been included as a human right. When examining where privacy could be positioned in the development of rights, it is clear from earlier in this chapter that despite numerous attempts to define and propose a clear definition of the concept of privacy and the needs for appropriate protection, no such definition exists. As one writer observed, 'in one sense, all human rights are aspects of the right to privacy.' [152]

2.5.4 Ideas of personhood leading to the right to be forgotten

A new theory on human rights, and potentially the most relevant in considering where a right to be forgotten may sit as a right, has been presented by Griffin, that of 'personhood'. Griffin[153] looks specifically at the basis of human rights being founded in the capacity to choose and act. He confirms the need for universal good for humans with three components parts. These are identified as autonomy, i.e., the ability to choose and make plans, liberty, i.e.

[152] Fernando Volio, *Legal personality, privacy and the family* in Louis Henkin (ed) *The International Bill of Rights, The Covenant on Civil and Political Rights*: (Columbia University Press, 1981.)
[153] James Griffin, *On Human Rights* (OUP 2008) ch 2 p 51

the ability to be able to make such choices, and also the ability to have sufficient resources to be able to provide for such choices. Key to his arguments are ideas of agency considering 'what we attach value to what we regard as giving dignity to human life is our capacity to choose'. [154] If one looks at the ideas of personhood as expressed by Griffin it is clear that without the ability to perform certain functions in a private manner not subject to the surveillance of others i.e. freedom from society as such, that autonomy for an individual is threatened along with the subsequent impact on dignity and reputation. He believes that society only functions as a group with man as a social being seeking generally to conform and be part of the group. If attempts are made to rebel against existing norms, then, in fear of censorship, the individual needs to be able to consider his deliberations/ actions in private. Griffin believes that 'autonomy is a feature of deliberation and decision' arguing that decisions need to be made alone and without interference.[155] For that certainty of privacy, he believes there is a need for strong well established principles of behaviour; 'deep dispositions and strong social conventions with an effective legal system'.

In his view, human rights are meant to protect the dignity of an ordinary human being and, for this, the usual human would require a background in which to function fully. He refers to this stance as being the 'narrow agency-focused right to privacy' deriving from his personhood viewpoint.[156] Bringing in concepts of 'informational privacy' where control of what he refers to as 'acts, thoughts and utterances should not be accessed by others' linking it to privacy. In looking at autonomy and separating it out from ideas of freedom and liberty, he refers to it as 'self-decision'.[157] This is where the right to be forgotten can be drawn in as providing not only an opportunity to protect and enable privacy but also to reduce the impact of a loss of standing in the community and a lack of reputation. It is clear that the formalization of human rights has resulted in protection for private life but it is equally clear that such protection can be widened. If a human being needs to be outside of society to determine their ability to function in the way they seek, then the easy accessibility or availability of information concerning him must therefore have an impact. The ability to

[154] n153 James Griffin Ch 2 p 44
[155] n153 James Griffin ch 13 p 226
[156] n153 James Griffin ch 13 p 226
[157] n153 James Griffin ch 8 p 156

achieve informational privacy although considered as part of the right could therefore affect many areas of their life. This clearly relates to any rights given in respect of not only privacy, but also reputation. Here might be where the right to be forgotten fits in, as it can be linked to both privacy and reputation with a right to have certain information 'hidden', or not made so easily accessible, thus potentially reducing the impact on the individual's position in society.

In the same vein, Griffin further argues that there was emphasis on the security of the person, his home and family but that not enough focus was placed on the issues of honour and reputation, which were often covered by other forms of legal remedy with unclear links to privacy.[158]

Griffin used the case of Roe and Wade[159] to show there was no need to follow the path to liberty when looking at privacy as being just within personal space. Later, in the case of Bowers and Hardwick[160], the judgment given by Justice Blackmun focused on the view of the right to be left alone as established by Roe and Wade, arguing that this introduced a new concept to liberty which emphasised the idea of 'personhood' and the ability to develop 'self-definition.' This is expanded through the need for independence to define such ability and considered to be 'central to the concept of liberty'. Griffin is keen to highlight that both narrow and wide interpretations of liberty can co-exist with the idea of personhood. Thus, this provides for the opportunity to follow what one might consider a worthwhile life for that individual. He believes that the right to liberty or freedom, so often used as the basis of human rights, does not provide all of the reasoning for a right to privacy. Therefore, autonomy is argued to play a key part in any ability to protect, in particular, informational privacy.[161]
He believes that arguments regarding privacy of space and life are doomed to fail for lack of any plausible reasoning to attach value to them. The value of reputation, which in effect places importance on loss of privacy and autonomy, is also considered. The importance of

[158] n153 James Griffin ch 13 p232
[159] Roe v Wade, US Supreme Court 1973 No 70-18 Here the Court held that laws criminalizing abortion in most instances was in breach of a woman's constitutional right of privacy. This was held to be founded in liberty within the Fourteenth Amendment.
[160] Bowers *v.* Hardwick*,* U.S. Supreme Court., 478 U.S. 186 (1986).
[161] n153 James Griffin ch 13 p 239

informational privacy is to provide for autonomy and liberty to be exercised by an individual (whether or not this results in questions of freedom of expression or other rights being impacted) in respect of personal information. He sees derived rights, i.e., those that result from a basic human right, as being rights that are 'culturally determined' from society to society and therefore very difficult to protect. Considering the impact of a loss of privacy on dignity or the ability to be autonomous, he recognises that this impacts on the loss of reputation. He argues that this is a measurable concept where value is through ensuring an individual is able to take part in his community. Yet he still sees merit in a more prosaic right to private space, so that, for example, an individual's home should not be capable of being violated by unauthorized entry by police.

Within his arguments, Griffin also raises the point that there is great potential for a clash between the right of privacy with freedom of expression. This is the elephant in the room which will be examined in more detail later in this thesis. Whilst accepting the value of the right to have a private life and the freedom to carry out certain aspects of life without the censor or control by other parts of, i.e., by virtue of reputation, the ability to do so must be balanced with the needs of society. For example, it must be balanced with freedom of expression, which, by its nature, is more in conflict with privacy of information. However, he states vehemently that the fact that a person has a public life should not restrict that person from arguing for a private life. This is despite how often the media may claim that this is against public interest by restricting freedom of expression, an argument which will be explored later in this thesis. It is within such arguments that the right to be forgotten should be considered to protect such a position through the balancing such interests determining how such a right could be considered excessive and prejudicial to public interest.

2.5.5 Privacy and society

It has been suggested that there are two core concepts of what constitutes privacy. Firstly, the creation of distance between oneself and another(s), i.e. the idea of being left alone. [162] This is viewed as a form of privacy providing freedom from society. The second core concept

[162] As set out in Alan Westin, *Privacy and Freedom*, (New York: Atheneum, 1967) and discussed later on in this chapter

is more concerned with meeting the requirements of society, namely enforcing its standards whilst at the same time looking for protection of reputation or 'privacy as dignity'.[163] Within such theories, there is recognition of a need to find a useful way to protect other values, and not only the potential foundation right of dignity. Even democracy can be achieved through the protection of human rights and by ensuring the freedom for people to be autonomous beings. the ability to challenge laws considered unjust is vital. Human rights are important as tools to change the world, not only for individual entitlements.

Therefore, human rights must be considered as an intrinsic part of the process of an evolving state led society. Human rights need to change and develop to provide protection as the needs of societies and individuals vary and the need for acceptance of different or varied rights increases. Griffin concludes that;

'[t]he runaway growth of the extension of the term in our time makes having some grasp of its intension the more urgent, and its intension is what is so especially thin.' [164]

Viewing this in the context of Donnelly's viewpoint, that human rights are rights, 'not benefits, duties or privileges or some other perhaps related practice'[165], then these can be considered special entitlements for those entitled to such protection. It is clear that, to ensure autonomy and dignity, such protection must include not only privacy, but also the ability to control information as well as access to information about oneself. Often, in addition, within such societies, reputation must be maintained so that one's position within one's community can be recognized.

A practical view of issues with human rights may well look at the difficulty in making them enforceable, thereby ensuring that those who should be benefiting from such rights actually do so. This can be expanded to declare that the ability to find recourse is thwarted by the fact

[163] See Jeremy Waldron, *Is Dignity the Foundation of Human Rights*? in Rowan Croft, S Matthew Liao Massimo Renzo (eds) *Philosophical Foundations of Human Rights* (OUP 2015)
[164] n153 Griffin, ch 13 p 239
[165] Jack Donnelly, 'Human Rights and Human Dignity: An Analytic Critique of Non-Western Conceptions of Human Rights', (1982) The American Political Science Review Vol 76 No 2 p 304

that such rights, despite acceptance of the need for individuals to be autonomous in their decisions unless there is some form of delegation to the state, rests in the hands of the large non state actors. This may be the position to some extent with what has happened with Google. It is compounded by political and economic issues which can fetter acknowledgment of rights where such issues as security are perceived to be more important. This is exemplified by issues around terrorism and the appropriate response, for example Guantanamo Bay where various human rights have been suspended in a reaction to such security issues. There is a need for human rights to work better to fill the 'gap' between the rights and the ability to exercise them successfully and to expand their scope where the needs of society change in a world of online posting and social media.

In looking at privacy through Griffin's lens of personhood, not only is it made clear that a right of privacy forms an integral part of human dignity and autonomy, but also that it leads the way into the acceptance of rights which would ultimately include those relating to information where its availability or access could impact portrayal of self and reputation and the potential to have informational self-determination.

2.6 Developments leading to current ideas and recognition of the wider scope of privacy

The challenges faced after initial recognition of specific rights and the theories of how these have come about, were how to give this right of privacy some definition. Here clarity would help to ascertain how it could meet the increasing challenges to it. Such challenges were largely in response to changing interactions within society bought about by increased technology. Many would argue that protection of privacy as a limited right would be difficult to legislate for, no matter how necessary. However, specific regulation is required to deal with the growth of technological changes that could potentially impact an individual's private life.

Despite privacy having been debated in earlier works which had led to recognition of it as a human right, based in theories of underlying dignity and autonomy, understandings of modern concepts of 'privacy' and its application within society did not begin until around 1964. Westin's influence, as set out below, was widely accepted in the US and persuasive in

the UK and across Europe. Other debates and discussions took place separately, culminating with the development of various paths recognizing wider aspects of privacy and ultimately concepts of data protection. These approaches to privacy were intensified by the divergence of the views held by continental Europe and the approach taken by the US.

Initial proposals on the definition of privacy came from the writings of Brandeis and Warren[166], and largely focused on remedies that might be available under a law of tort for breach of privacy rather than considering the concept of privacy itself and how to protect it. Progressing Brandeis and Warren's proposal of a 'right to be let alone,' in the US ideas and acceptance of privacy revolved around the views put forward by Alan Westin. In 'Privacy and Freedom', [167]Westin investigated both the meaning and importance of privacy, particularly following the invention of electronic surveillance. This led to wider discussions on the early developments of formal protection. It was at this point that debate became more focused on the need to protect the individual from the intervention of the state. This echoed concerns as to state involvement in the ability to record and watch interventions between individuals. The beliefs underlying privacy, whilst still evoking the ability to be autonomous, had become overtaken by more practical considerations

In Westin's view, the US's attitudes represented an 'egalitarian democratic balance'. Thus, although there were ideals of individualism and civil liberties, these were often opposed in the name of 'social egalitarianism, personal activism and political fundamentalism'.[168] Part of this thinking involved the overreaching belief that in a society free from class divisions, there must be the freedom to pursue 'the American Dream'[169] , without the baggage of the English legal system. This had the intent of forming a flexible status and mobile society, and above all else, a belief in freedom of expression and protection from interference by governments. Westin argues that US society is based upon its citizens being open and involved so that 'outsiders', even those who might seek to enjoy a private space for their own

[166] Samuel D Warren & Louis D Brandeis, 'The Right to Privacy' [1890] 4 HARV.L. REV. 193
[167] Alan Westin, *Privacy and Freedom*, (Atheneum 1967)
[168] ibid Westin ch 2 p 29 s
[169] James Truslow Adams, *The Epic of America* (Little, Brown and Co. 1931) Adams put forward a definition of the American Dream Adams, "life should be better and richer and fuller for everyone, with opportunity for each according to ability or achievement" regardless of social class or circumstances of birth.

interests, are viewed with suspicion. This view, at variance to that of its European counterparts, opened the door to the US pursuit of having not only freedom of speech, but also accessibility to information, particularly if it is already in the public domain and irrespective of its impact on a person's dignity or reputation. By way of comparison with the English position where status is reflected in a class system, Westin believed that there is a 'classic' American demand for equality and democracy, which could be used to deny what he calls 'status rights' or the old view of a class system. Thus, to maintain social mobility, the openness of American culture is focused on activities which the many can aspire to with the more solitary or reclusive activities belonging to the outsiders. For true American democracy. it would appear there must be an openness, whether in politics or in social activities, leading to acceptance that more disclosure is anticipated and accepted by the majority of its nationals.

Westin accepted that different cultures held and continued to hold very differing views of privacy. For comparison, he identified the German law that restricted the photographing of strangers in public without consent and viewed this against the open door policy of the Americans and the informality of US society. Westin further believed this informality was characterized by the lack of a need for US citizens to 'hide' themselves away in order to exercise autonomy, or in Griffin's view 'self-definition'[170] to obtain privacy, as might be evidenced with the introduction of open plan offices, unfenced gardens, and so on. Differing views of privacy with the growth in technology would largely be driven by the needs of the particular culture or society with constant challenges to determine where and how privacy could be universally defined. In current time this must appear obvious, but writing in 1964, these views were very thought provoking and built on the recent development of privacy as a right.[171] There was also acknowledgment that technical means could lead to a more invasive approach to accessing personal details, particularly by locating information which could be considered by many to be essentially 'private'.

[170] n153 James Griffin Ch 8 p 150

[171] This had been accepted in the Universal Declaration of Human Rights as well as in the European Convention of Human Rights only a few years before

Despite Westin's opinion that there would be substantial difficulty in a 'one size fits all' approach to defining privacy, his view, based on beliefs that certainly applied for the Western world, was that privacy comprised of certain elements. The first of these elements was solitude, or the ability 'to be freed from the observation of other people.' This initiated the idea of privacy as being a 'right to be left alone', which underlays much of his view of privacy. This mirrors some of the earlier religious thoughts around privacy and the need to be able to contemplate in solitude as seen in early philosophies. The second element he believed was universal was to enjoy the ability to be intimate with another person or a small group, although he recognized that different cultures had differing ways of obtaining 'intimacy'.[172] The third element related to anonymity, or what he referred to as freedom from identification or surveillance, even when in a public place. This, again, links to ideas around dignity and position in society, i.e., 'reputation'. This highlighted the level of concern that was emerging in the early 1960s with the development of 'bugs' and recording devices but could also be of particular importance today with the ubiquity of social media and the growth of constant access. Today, the ability of such companies as Facebook to ensure that connections are made to individuals, whether sought or not, means the ability to be anonymous has been rapidly reduced. With the concern to make access to individuals safer in an era of internet trolls and such like, this is surely an aspect unlikely to change in the forthcoming years. The final element of privacy as outlined by Westin was that of 'reserve', namely the ability to limit communications being created around a person. To act or speak with reserve is to give little away and to heighten the privacy around oneself and one's way of living, thus enhancing both dignity and, potentially, reputation. This again is in accordance with the cultural aspects reviewed by Westin, particularly with regard to such nations as the UK where it is habitual for reserve to be used to afford privacy. This illustrates the cultural variations seen in the development of human rights. When considering these principles in the context of retention or permanent accessibility of personal information or data, it is clear that additional protection could be necessary to meet at least these requirements of privacy.

[172] n167 Alan Westin, Ch 1 p 13, Here Westin gave examples of cultures such as that explored by Robert Murphy in 'Social Distance and the Veil', 66 American Anthropologist 1257-74 1964 & the symbolism of the veil in the Tuareg tribe of north Africa where the veil is adjusted according to the relationship between the individuals and depending on the level of exposure or privacy needed in the circumstances so ensuring the required level of intimacy.

Contrasting the US approach with that of the UK, Westin viewed it as having a 'deferential democratic balance', with the basis of privacy being fundamentally cultural. In that in his opinion the classic 'Englishman' had as an individual great personal reserve whilst accepting however that acts considered as deviant beliefs or behaviour i.e., acts outside the widely accepted norm of society would be tolerated as 'permissible private action.'[173] The disclosure of such behaviours could potentially impact the reputation of such an individual to the extent that they were no longer accepted within society. The accepted view of privacy seemed, at that stage within the UK, to be based on the personal rights of the nobility, certainly lords and ladies to stop the public becoming aware of their indiscretions and to protect their status.[174]

Influenced by Westin's work, the case of Katz v United States[175] helped to further define the stance on privacy. Justice Harlan proposed a two-part test that introduced the concept of a 'reasonable expectation of privacy', and this test has been widely followed. [176] However, it became increasingly clear that such struggles, which attempted to define privacy despite its acceptance as a human right and provide effective legal remedies, would become only more complex. Certainly, with the advancement of technology forward thinking privacy advocates could immediately see the impact on privacy of not only of physical surveillance being potentially increased by the deliverance of 'gadgets' but also by the retention and use of personal information heightening impact not only on privacy but on reputation. The early days of these initial concerns could not have forecast the commercial value which would be placed on such data and the growth of the Internet giants and limitless possibilities of 'Big Data'. In the early 1960s and 70s, the need for some ownership of control was beginning to emerge. This may have marked a change from the need for privacy as a right to be enforced against state actions to rights of ownership and control over personal information or the accessibility to it as linked to the individual and their life. It also bought into conflict those promoting the free flow of information for cross border activities, which required acceptance

[173] n168 Alan Westin, Ch 1 p 29, Here he proposed that in the UK unlike the US there is a pattern of trust and even deference towards those in position of authority.
[174] Prince Albert v Strange (1849) 1 Mac & G 25, Duke of Argyll v Duchess of Argyll HL,1962 SC (HL) 88)
[175] Katz v United States 389 U.S. 347 (1967) Harlan J. proposed a two-part test introducing the concept of the 'reasonable expectation of privacy'
[176] see the case of Campbell v MGN [2004] UK HL 22 p 50

that the divergences between not only mere views of privacy, but also of embryonic data protection, which would hinder this impacting the internal market in the EU.

2.7 The influence of privacy, dignity and reputation as human rights on data protection

To consolidate these views, by the 1970s, the origins of formal right to data protection were emerging, specifically by developments within Europe. This acceptance showed that although protection of data was concerned with privacy, it was also linked with many other interests, such as limiting the use of data, and identifying the purpose for which the information was held and accessed, thereby potentially expanding more traditional views of privacy. Within the early 1970s, the Council of Europe passed resolutions on data-processing, focusing on providing protection around the newly invented electronic/automated processing and recognizing in part that Article 8 of the European Convention on Human Rights (ECHR) was potentially too narrow in scope to help.[177] The European Union then took up the challenge as it became aware of issues around the non-standardization of laws relating to the free flow of data across the national states.

Initial recognition of the concept of data protection came from the German state of Hesse in 1970.[178] Here limited rights for individuals were documented based on the concerns that the state, through its various organizations, could use information obtained or accessed theoretically against an individual. Such concerns potentially arose from state activities relating to the Second World War, but also echoed concerns arising from the era of the McCarthy investigations in the US.[179] The German Federal Data Protection Act[180] followed in

[177] In April 1967 the Consultative Assembly of the Council of Europe discussed their concerns with regard to the increase in technical devices with the Council of Europe then debating the question of Article 8 of the European Convention of Human Rights as to whether its right to privacy gave a form of protection sufficient to meet the needs growing with regard to this new technology. The Council of Europe was not able to pass binding laws but in theory it could enforce laws ie under Conventions entered into through the European Court of Human Rights.

[178] Hessische Datenschutzgesetz vom, 7 October 1970, GVBI II 300-10 published at Wiesbaden. This law was primarily concerned with the information accessed by Government departments following the emergence of initial data processing by automatic means by government departments. Other German federal states had also looked to provide similar protection for personal information by Hesse was the first state to provide for it is a separate dedicated law, even if only in recognition of the rights that public bodies owed to citizens as the days of private entities being included were still some way off.

[179] https://millercenter.org/the-presidency/educational-resources/age-of-eisenhower/mcarthyism-red-scare

[180] (*Bundesdatenschutzgesetz* 1977 Section 35 – *lonitle Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung* nb this act makes ref in s. 16 to limiting the powers of the Federal

1977 and was translated to form the law on protection against the misuse of personal data in data processing.[181] Awareness grew that the holding of such personal information and the permitting of access to it indefinitely could present increased privacy concerns. Orla Lynskey[182] argues that human dignity provided the 'conceptual foundation' for a right to data protection subsequently found in the 1983 Population Census Decision case (unreported in English), where the German Constitutional Court held that individuals should have the right to determine how their data is disclosed and how it is put to use.[183] On this basis, a right to not only withdraw consent to the use of such data but also to remove personal information limiting its accessibility also evoked the right to dignity. The German Court called such a right 'informational self-determination', a concept considered more fully in this thesis, and in particular the extent it forms part of the scope of the right to be forgotten. The case is also considered authority for the introduction of the separation of data protection and privacy, although this as been argued by Lynskey to be the case as the two concepts protect different objectives.[184] These were then regarded as two rights, both providing support to individual self-development and the ability to exercise autonomous controls. [185] However, the separate form of data protection was not recognised widely nor so quickly, despite acceptance that it presented a new aspect of the need for privacy. The decision in Google Spain[186] confirming the right to be forgotten subsequently evoked both data protection and the loss of privacy.

Argued to be representing the evolution of privacy required due to increasing technology, data protection, as such, had no independent objectives. This created debate that all it would

Commissioner to the fundamental right of privacy of correspondence, post and telecommunications under art 10 basic law to permit access to premises/property and information so they can do their role. As a federal act this covered the whole of Germany, https://germanlawarchive.iuscomp.org/?p=712 last accessed 17 Nov 2020

[181] In early recognition as to consequences of holding data, this law contained provision for every data subject to have the right of erasure in defined and specific circumstances

[182] Orla Lynskey, *The Foundations of EU Data Protection*, (OUP 2015) ch 4, 94

[183] 1983 Population Census Decision, 15 Dec 1983 BvR 209/83, BVerfG 65 1

[184] Orla Lynskey, 'Deconstructing data protection: the added value of a right to data protection in the EU legal order', Int & Comp Law Quarterly 2014, 63 (30) pp569-597

[185] Antoniette Rouvroy, Yves Poullet '*The Right to Informational Self-determination and the Value of Self Development. Reassuring the Importance of Privacy for Democracy* in (eds) Serge Gutwirth, Yves Poullet, Paul de Hert, Sjaak Nouwt and Cecile de Terwangne, *Reinventing Data Protection* (Springer 2009)

[186] Case C- 131/12 Google Spain Sl Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González Case, [2014] ECLI: EU:C:2014:317 (Google Spain)

ultimately protect were other aspects of privacy.[187] It was too early for the world of 'Big Data' and the machinations of social media to provide the new arena where not just protection of a private life, but also informational privacy, was required. It was also too early for any subsequent arguments that data protection would, in itself, provide for more rights other than just privacy.

In the UK, this was clearly illustrated when the Younger Report[188] published a survey directly relating to new form of interferences which might be considered to intrude into an individual's privacy. However, the report was limited in its early attempt to establish a definition of privacy. In this survey, the biggest response by the public was to a question on the holding of personal data, which would have had relevance to the situation on information technology today.[189] Subsequently, a White Paper headed 'Computers and Privacy'[190] identified key issues, and there grew awareness of conflicts with privacy as a result of the development of information technology. The outlined recommendations and substantial thoughts on future data protection legislation were followed by a proposed bill. [191] New ideas of additional protection were beginning to emerge on a wider scale, with proposed new rights appearing in various jurisdictions.[192].

[187] n 184 Orla Lynskey, Here the question of whether data protection could be considered a subset of privacy or did it provide a 'self-standing right,' one that attempted to balance the power asymmetries between individuals and data processors.

[188] The Younger Report, HL Deb 06 June 1973 vol 343 cc 104-78

[189] The question put to the public was: 'in a few years' time from now, it may be technically possible for details of your life such as family circumstances, financial situation, political views and so on to be recorded on a big central computer, with any of the information being available to anyone who asks for it; would you regard this as an invasion of privacy etc.?" The questionnaire and the report on the survey by Research Bureau Limited are reproduced as Appendix E of the Committee's report (Cmnd. 5012, HMO, 1972).

[190] The Lindop Report was subsequently published in December 1978

[191] There followed Parliamentary questions over the following years where privacy was raised but what was also considered even in these early stages the ability to protect privacy by the removal of information which impacted a person's life. 'That increasing encroachment on the individual is a matter of concern and something to which we should be alerted'. https://api.parliament.uk/historic-hansard/commons/1980/dec/19/privacy last accessed 12 April 2020 Subsequently in April 1982 a new White Paper was published which contained a proposed bill leading to the first UK Data Protection Act.

[192] In Sweden the first form of data protection authority was formed in 1973 initiating the concept of not only licencing automated data processing but also authorisation before data could be transferred out of Sweden. Both progressing no only the concepts of data protection but increasing awareness of the potential for abuse of access to data.

At a similar time, the Minitel system issue in France in the 1980s provided the first example of a mass online system, being the nearest predecessor to the Internet. The scope of its offering moved from effectively being an online telephone directory to having the ability to host forums with opinions being expressed. Subsequently, this led to false accusations of defamation as a result of adverse impact to reputation and even identity fraud. The scandal of the Minitel sex lines[193] began the end of freedom for Minitel users and introduced concepts such as the need to obtain consent by owners for telephone numbers to be published. There was ultimately criminal responsibility for the disclosure of data which might adversely affect reputation or reveal details of a person's private life. The link between privacy, reputation and the ability of accessibility of data was becoming clearer.

However, other countries looked differently at controlling personal data, regarding it as not separate but part of the scope of privacy. This was the approach taken by the Dutch authorities with the main legislation being put in place in 1989 whilst clearly basing the rights on privacy used differing terms to other systems within the EU.[194] Particular provision was contained in Article 10 of the Dutch Constitution[195], which contained a right to respect for one's 'personal sphere'.[196] In this jurisdiction, the notion of privacy in practice is most strongly associated with protection against unwanted publication of personal facts and how a person was regarded by their peers however, linking it closely to ideas of reputation.[197]

---

[193] The Independent, 'How France fell out of love with Mintel ' article about the Minitel Rose sex line scandal http://www.independent.co.uk/news/world/europe/how-france-fell-out-of-love-with-minitel-7831816.html last accessed 15 June 2019

[194] Dutch Data Protection 1989 (*Wet Persoonsregistraties privé-levenssfeer, persoonlijkleven,privé-sfeer, persoonlijke levenssfeer, persoonlijke vrijheid, privé-leven7*) Terms are used to refer to privacy.
Ref http://uir.unisa.ac.za/bitstream/handle/10500/1463/09chapter5.pdf last accessed 5 May 2019

[195] Article 10 of the Dutch Constitution goes further as it seems to distinguish between relational privacy and informational privacy see Schuijt, G. A. I. *Groene Serie Onrechtmatige daad, aant*. 10.5
Deventer: Kluwer.2010.as referred in A.J. Verheij 'The right to be forgotten – a Dutch perspective', (2016) International Review of Law, Computers & Technology, 30:1-2, 32-41,

[196] Section 1 states that everyone is entitled to respect for his 'personal sphere' (translated from 'persoonlijke levenssfeer') and that exceptions should be provided by law. ss 2 and 3 provided reference to the need to create laws with regard to data and its processing This latter has been done first by the Act on the registration of personal data (*Wet Persoonsregistraties*) of 1988, which in 2001 was replaced by the Act on the protection of personal data (*Wet bescherming persoonsgegevens*; hereinafter Wbp) that implemented Directive 95/46/EC on the processing of personal data.

[197] It was no surprise with this stance that the Dutch Supreme Court protects reputation within privacy protection see A.J. Verheij (2016) 'The right to be forgotten – a Dutch perspective', International Review of Law, Computers & Technology, 30:1-2, 32-41,

2.7.1 The introduction of data protection

The European Court of Human Rights (ECtHR) also seemed to be taking steps to find remedies for issues raised by the new technologies. De Hert and Gutwirth[198], analyzing the cases interpreting the scope of Article 8 of the ECHR, saw the Court as increasingly finding ways to include data protection within it. Since the mid-1980s, the Court has broadly interpreted the term 'private life' to include personal data, as shown in the case of *Rotaru v Romania*.[199] This held that the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[200] was 'to secure' respect for an individual's rights and fundamental freedoms and, in particular, their 'right to privacy with regard to automatic processing of personal data.' The authors believe the ECtHR was instrumental in finding that there was a right for individuals to have control of the use and registration of their personal information, i.e. an early stance of informational self-determination. The decision in this case was based on the data held which contained certain information about the individual's life, in particular their studies, political activities and criminal record, although some of the information had been collected more than 50 years previously. The Court determined that this data, where systematically collected and retained by a state or other organization, fell within the perimeters of a 'private life' under Article 8(1) of the Convention. Additional cases had similar outcomes ranging from claims for the deletion of personal data from public files[201] and claims from transsexuals to have their official sexual data corrected.[202]

Subsequently, considerations as to how privacy and reputation relating to personal information could be protected led to calls for specific protection as a separate right. Despite the challenge of technology chasing at the heels of privacy, [203] recognition of data protection

[198] Serge Gutwirth, Yves Poullet, Paul De Hert , *Data Protection in the Case Law of Strasbourg and Luxembourg* in (eds) Serge Gutwirth , Yves Poullet, Paul De Hert, Cecile de Terwangne, Sjaak Nouwt, *Reinventing Data Protection* (Springer 2009)

[199] Rotaru v Romania, 28341/95, [2000] ECHR 192, (2000) 8 BHRC 449

[200] Council of Europe, 1981 ETS 108

[201] Leander v Sweden, ECHR ([1987] 9 EHRR 433, 9248/81

[202] Rees v UK, ECHR [1986] Appl. 9532/81

[203] J Lee Riccardi, 'The German Federal Data Protection Act of 1977: Protecting the Right to Privacy, B.C.Int'l & Comp. L. Rev. 243 (1983), http://lawdigitalcommons.bc.edu/iclr/v ol6/iss1/8 last accessed 13 Sept 2017 Computers involve 'machine aided manipulation of information.' see J. Adams & D. Haden, Social Effects of Computer Use and Misuse 23 (1976) p 35; The first business use of an electronic computer was in 1964. Since then, both technological progress and growth in numbers have been steady. In 1966, 15,000 computers existed; by 1970, 80,000 were in use, of these, 70,000 were in use in the US alone.

only became fully accepted with the EU finalizing the Data Protection Directive in 1995, (the DPD).[204] This was also the first true indication of awareness for the need to exercise autonomy over the use of personal information. This included stages such as the need for consent to ensure data would be held under the DPD's principles, and for also providing initial steps for the removal, erasure or rectification of information.

The EU data protection regime will be examined in more detail in the next chapter, however its contribution to the importance of protecting and providing a form of autonomy, or control, over personal information ultimately reflected in the Charter of Fundamental Rights of the European Union (the Charter)[205] was key. This was in line with the EU's intention to achieve an internal digital market combined with the protection of what were seen as individual freedoms and rights[206], enabling the development of the right to be forgotten.

2.7.2 The differing US approach

With the growth of data collection and usage emerging due to the increased power of the internet giants, the so called 'FAANGs', the need for more uniformity of approach between the US and the EU has increased. As EU data protection was developing so comprehensively, and largely within the human right of privacy, the divergence of approach towards privacy in the US became more apparent. This was despite the consensus within the Universal Declaration. Then, as now, US citizens do not have, nor indeed do not seem to require, a high level of control over their personal information not regarding this as conflicting with idea of privacy.[207] Where the information is used for accepted purposes, then no individual control over such data is seen as necessary. With the US being the homeplace of many of the entities

[204] The first reading of the DPA Bill took place in the House of Lords on December 21, 1982. Passage of the Bill was stopped when Parliament was dissolved on May 13, 1983. An amended version was discussed in the House of Lords on June 23, 1983. It passed to the House of Commons on November 3, of that year, returning to the House of Lords on June 29, 1984. The DPA received the Royal Assent on July 12, 1984. ref https://pdpecho.com/2012/08/14/it-took-15-years-for-uk-to-pass-its-data-protection-act/

[205] The Charter of Fundamental Rights of the European Union, Dec 2000 was the first embodiment of rights agreed by the three key EU constitutions progressed from the 1950 Convention for the Protection of Human Rights and Fundamental freedoms recognizing 'changes in society social progress and scientific and technological developments making those more visible'

[206] In 2009 the European Union and the Treaty on the Functioning of the European Union 2012/C 326/01 gave this instrument a legal status akin to that of the EU treaties.

[207] Other than in a few specific areas where ultimately specific legislation was passed such example medical records

now involved in the information technology environment, it is easy to see how the development of products collecting what appears to be endless information, ranging from private or public sources and from smart phones to Fitbits and other devices, can have happened in this environment without the necessity to validate such collections or have to obtain detailed consent. The creation of information or data to create a form of digital memory has been largely based in the US due to the growth of the technology companies based there. As was seen with the decision in Google Spain, the ability to exercise European beliefs of privacy and of data protection has proved difficult. Recognition of the importance of the right to be forgotten and its scope has therefore been limited within the US to date, as will be shown in later chapters.[208]

To try to understand this is to realize that the priority over any rights of privacy for the US has always been freedom of speech or expression. This is considered by many to be linked to the ability to pursue a free market. Privacy is accepted as a human right, but it is only seen as a more limited one. Freedom of the press and media has generally been considered key to protecting people from the onslaught of technology and its misuse, not just by any government agencies but also by other people. In the opinion of James Whitman, the media is there 'to cover and report it-not merely the truth about government and public affairs but the truth about people.'[209]

The constant debate on the clash between the right to free speech and the right of privacy has shaped the approach taken by the US to the protection of personal information. With the US stance largely in favour of free speech, there is the use of what has been termed a free governance theory, a theory that protects ideas of self-governance where the public determines how much access there should be to relevant information, potentially at the detriment of the rights of the individual. For privacy to be enacted or for any ideas to be expanded upon, the retention and access to information, known as 'the secrecy paradigm' [210], is applied. This has been argued specifically by Daniel Solove, who puts forward the notion

[208] Chapters 3 & 4 will show the response of the US to the initial ideas of the right to be forgotten and in particular to the decision in the Google Spain case.

[209] James Q Whitman, 'The Two Western cultures of Privacy; Dignity versus Liberty' [2004] 113 Yale, 1151-1197

[210] Daniel J. Solove, *Understanding Privacy*, (Harvard University Press 2008) Ch 5, 111, 150

that once information has been leaked into the public arena, it can never be held to be private.

Despite signing up to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980[211], the US has largely ignored the drive towards data protection. Some of the issues on the interpretation of privacy failed to encompass data protection, and were aggravated by the lack of uniformity within the states of the US. A look at the Uniform Law Commission in the US [212] reveals little or no information about existing or new laws relating to privacy or data protection. Although, for example, the Employee and Student Online Privacy Protection Act[213] does deal directly with the issues of access to social media platforms, it has only been enacted or considered for enactment in states as diverse as Hawaii, Minnesota and New York.[214] Individual states considered to be more technologically savvy had already created specific legislation prior to the uniform bill's proposals. The location of the internet based companies has also been a factor in state-led legislation, therefore, as would be expected, the state of California is often in the forefront of developing legislation and, through exposure to other countries, has more awareness of the need for data privacy and protection. This is reflected in California's Online Privacy Protection Act 2003.[215] Such provision provides safeguards where an entity, whether a person or a corporate, who collects information that is sufficient to identify an individual in California through a website or other online service, must post a conspicuous privacy policy on its website or online service. It is worth noting that this could include even mobile phone apps.[216]

---

[211] Adopted and became applicable on the 23rd Sept 1980 and revised in 2013

[212] Uniform Law Commission also known as the National Conference of Commissioners on Uniform State available at https://www.uniformlaws.org/committees/community-home?CommunityKey=c3a46a62-51bd-4098-ac70-61c20a959ff2 , last accessed 17 Nov 2020

[213] The Uniform Employee and Student Online Privacy Protection Act addresses both employers' access to employees or prospective employees' social media and other online accounts accessed via username and password or other credentials of authentication as well as post-secondary educational institutions' access to students' or prospective students' similar online accounts.

[214] This act however was a specific response to a leading case that detailed an occasion where a job candidate was asked for access through passwords to his social media accounts to allow the prospective employer to use this in the assessment of the job application

[215] Calif. Bus. & Prof. Code ss 22575-22578 (CalOPPA) California's Online Privacy Protection Act, Conn. Gen. Stat. ss 42-471. This has been supplemented by the California Privacy Rights Act 2020 which modifies and expands on the California Consumer Privacy Act of 2018. These provisions allow consumers to take control and make informed choices with regard to use of their personal data as well as request data be deleted.

[216] ibid see Ch 22. Internet Privacy Requirements [22575 - 22579] (added by Stats. 2003, Ch. 829, Sec. 3)

The policy must also identify categories of information that can produce identification collected about individual consumers using or visiting the website/online services and any third parties with whom the operator may share the information.

Outside of California, US state laws are prolific but more targeted to specific circumstances, such as designed for privacy statements or social security numbers. Thus, although there are examples showing that specific legislation exists, these do not cover the misuse of personal data specifically and the practice is that certain legislation is put in place to cover situations as they arise.[217] The areas of concern are more related to practices concerning consumers' personal information. An example of how there was limited acceptance of protection of informational privacy was seen in the case of Nixon v Administrator of General Services, [218] although this case expanded the concept of constitutional privacy protection. Here, privacy was held to include the avoidance of disclosing personal information. However, without a comprehensive acceptance of the need for data protection, there is an inability to create an enforceable data protection authority. This has triggered other issues which will be discussed later in this thesis, and includes data transfers between the US and other jurisdictions, and the non-acceptance of a right to be forgotten. The view of Whitman emphasized the difference of approach, i.e., one of 'dignity' as observed by Europe and other nations following suit, and one of 'liberty' highlighting the emphasis on freedom of expression in the US. [219]

Despite this, it can be seen that there is a change to the norm and, along with acceptance of a diminished right of privacy, the need for a form of data protection is increasing. This includes

'(a) An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site, or in the case of an operator of an online service, make that policy available in accordance with paragraph (5) of subdivision (b) of Section 22577. An operator shall be in violation of this subdivision only if the operator fails to post its policy within 30 days after being notified of noncompliance.'

[217] The Federal Trade Commission Act (15 U.S.C. ss 41-58) (FTC Act) is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies. The FTC has brought many enforcement actions against companies failing to comply with posted privacy policies and for the unauthorised disclosure of personal data. The FTC is also the primary enforcer of the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. ss 6501-6506), which applies to the online collection of information from children, and the Self-Regulatory Principles for Behavioural Advertising

[218] Nixon v Administrator of General Services 433 US 425 (1977)

[219] n209 James Q Whitman p 1197

more recognition of the need to limit the accessibility of data within the US, where greater awareness of this need began to emerge with the efforts of such individuals as Edward Snowden, highlighting the accessibility of personal data. Also, more recent data breaches (Facebook)[220] have shown that not only is an individual's privacy at risk but also the impact of the misuse of personal data. This also concerns security of data, which is outside the scope of this research, but can also dramatically affect an individual's autonomy or control over information which potentially shapes them. The question of trust is not only a factor in the attitude an individual takes to the holding of his data, but can impact a company commercially, for example the trust placed in a company can increase its reputation and therefore its value. This is evidenced by the use of the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity [221](NIST) not only by Government agencies, but now also by a minimum of 30% of US organizations. The success of schemes promoted to protect privacy focuses on trust placed in the company, which is now seen as a valuable selling point.

More widely, the involvement of the OECD[222] on a global approach focused recognition of the need to meet a uniform level of protection in states, particularly with the contrast of responses between the EU and the US. The fact that Guidelines produced by the OECD formed the basis of the original DPD and largely led to the subsequent development of the EU's General Data Protection Regulation, as well as ancillary protection[223], could be seen as the initiator of wider recognition of acceptance of its terms. Recent years have indeed bought more focus onto the need for adequate data protection controls on a global basis, as has been highlighted in the Schrems case. [224]

[220] see v Snowden revelations; https://www.bbc.co.uk/news/world-us-canada-23123964 last accessed 10 Nov 2020, https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

[221] https://www.nist.gov/publications/framework-improving-critical-infrastructure

[222] OECD, The Guidelines on the protection of Privacy and Trans border flows of Personal Data. 1980

[223] Directive 2002/58/EC of The European Parliament and of the Council12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37)

[224] Case 362/14 Maximillian Schrems v Data Protection Commissioner Joined Party, Digital Rights Ireland Ltd [2015] ECU C 2015 650, paras 74-75. Here Max Schrems raised the issue that the data being held in the US was not subject to the same standards of protection as provided for by the EU member states and on this basis the CJEU held that the Safe Harbour agreement entered into between the US and the EU was not sufficient to offer such necessary safeguards

2.8 Conclusion

The development and formalisation of privacy as a human right and its relationship with dignity and reputation can be seen through the lens of the various theories that relate to how it is viewed and utilized.[225] This is of greater importance where the law does not always provide a clear definition of privacy, and where it is subject to influence from cultural and other potentially more limiting attitudes, such as prioritising freedom of expression. Both data protection and privacy can be argued to have the same roots, potentially providing for personhood through the acknowledgment of the need of dignity and the protection of reputation. Despite such rights not being considered essential or universal, they are critical to the formation of the right to be forgotten and the ability to provide for a form of control of personal information.

Where there is a deeper belief in a right of privacy, the path to data protection, whether as a subset of privacy or as a fundamental right in itself as contained in the EU's Charter, has been steadily progressive. As the demands of society not only increase but are shaped by the new developments in technology, with new challenges often under-estimated, this brings more urgency to the ability to redefine human rights with a view to opening the gate for additional rights. The existence of information with the potential to be retained permanently, and with the ability to impact privacy, to also affect one's dignity and reputation and ultimately remove autonomy specifically in respect of such data, underlies the foundation of the right to be forgotten. This highlights the need to consider the status, and ultimately the extent and scope, of the right to be forgotten. The right to be forgotten must therefore be considered to be primarily evolving from not only rights of privacy and dignity and ultimately reputation, but also through the quest for autonomy and personhood, linking these with the ability to define oneself. This provides the potential to include the ability to protect one's own reputation through the choice of what information should remain accessible and what should be erased or forgotten. Solove argues that 'Protecting individual privacy need not be at society's expense, in fact the value of safe guarding people's privacy should be justified by its

[225] This is particularly seen in the work by Sen as discussed previously

social benefits.'[226] In such an era of accessible information, this can enable one to present oneself publicly whilst retaining privacy around information that one does not believe should define oneself for eternity. The question when examining the right to be forgotten in more detail is where such a right can fit within the challenges of universalism or cultural realism, which may restrict an expansion of rights. Where the concept of freedom, as expressed by Sen, or of personhood, not only proposed by Griffin but accepted within many jurisdictions where the idea of identity or persona is more accepted, are applied, then understanding of the right to be forgotten becomes clearer. Here its benefit can be seen to not only protect an individual's privacy but to meet the expectation of maintaining reputation within society and providing rehabilitation. This promotes the idea of a right to be forgotten as delivering rights in respect autonomy and the ability to choose how to define oneself through the availability or not of such information. In later chapters, the question of reputation with the ability to be integrated or even rehabilitated into society will be examined in the context of how the right can be more widely interpreted and how can any social contract be made between state and citizens to enforce this protection.

A wider interpretation of this new right can offer individuals greater scope in ensuring they remain in control not only of personal and even private information, but also of how it is utilised, as well as controlling the impact on one's portrayal, particularly online. However, this can only be done if balanced with the right to freedom of expression.

In the next chapters the development and subsequent use of the right to be forgotten through the implementation of European data protection, together with the impact and influence of the Google Spain case, will be examined to determine where such right fits within existing laws and regulations. In addition, the challenges of the interpretation of the scope of the right to be forgotten, as well as its application through the use of internet service providers, will be reviewed.

[226] Daniel J.Solove, *Understanding Privacy*, (Harvard University Press 2008) ch 4 91

Chapter 3 -The right to be forgotten: From pre Google Spain to the GDPR

3.1 Introduction

To fully consider the impact of the decision reached in the ground-breaking Google Spain case,[1] which found in favour of a right to be forgotten, or perhaps more specifically a right to request de-linking from a search engine, we need to consider how this builds on a platform of the recognition of privacy whilst incorporating further aspects of human rights. As seen in Europe, the development of acceptance and recognition of a right of privacy into a separate concept of data protection, at least within European Union, expanded towards a realization that the erasure, or 'forgetting', of personal information in certain circumstances would be essential to protect such rights, but also to protect human dignity as well as ultimately impacting a person's reputation. Ideas of privacy as 'a right to be left alone',[2] as put forward by Warren and Brandeis, initially focused attention on the need to manage your public portrayal through accessible information. However, thoughts of a right to be forgotten had emerged through early data protection where the dual needs of privacy and data protection focused on how access to data could potentially indefinitely affect individuals in a much wider context in the new digitalization era. An examination of the preliminary discussions around this challenge, and the growing realization as to the effect of a 'digital memory,' highlighted an intention for formalization of a right to be forgotten. This was seen not only in early discussions of such rights among various national states, but clearly in announcements made by the EU in acknowledgement of the need to protect individuals at risk of the impact of a digital memory.[3] Consequently, initial steps taken led to the Google Spain case reaching the Court of Justice of the European Union (CJEU) arising from Spain but supported by other member states. This decision then impacted the progression of this right to its finalization and implementation as Article 17 of the General Data Protection Regulation (GDPR) incorporating the new right of erasure, discussion of which occurs later in this chapter. It could be considered that the CJEU actually pre-empted the GDPR by interpreting an out of

[1] Case C- 131/12 Google Spain Sl Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González Case, [2014] ECLI: EU:C:2014:317 (Google Spain)

[2] Samuel Warren & Louis D Brandeis, 'The Right to Privacy', [1890] .4 HARV.L. REV. 193

[3] Viviane Reding Vice-President of the European Commission, EU Justice Commissioner, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age Innovation Conference Digital, Life, Design, Munich, 22 January 2012 available https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_26 last accessed 10 Feb 2021

date directive, the Data Protection Directive (DPD), which was no longer 'fit for purpose' nearly twenty years after its implementation. Despite acknowledgement of the need to implement the right to be forgotten within formal and up to date data protection, this was not the end of the story with regard to how the scope and extent of the right would be formulated through differing approaches.

The GDPR was itself subject to much debate, despite recognition generally within the EU as to the need to 'modernize' and harmonize the data protection laws.[4] Some of the ideas that would be incorporated into the new regulation were not initially universally approved by the member states.[5] The approach towards internet service providers (ISPs), such as search engines, had previously been based on limited liability enabling the free flow of information on the Internet, largely to facilitate business being carried out online.[6] Any change to this was considered controversial. The draft regulation faced criticism with much debate focusing around Article 17.

One critic of the proposal, Christopher Kuner,[7] saw its draft wording as merely an extension of existing rights to have data erased, or indeed rectified, under Article 12 of the DPD,[8] arguing that no new right was being created. He expressed concern that there would be considerable difficulty applying such a right with regard to balancing it with the freedom of expression. Additionally, he argued that exemptions in Article 17 lacked clear definitions, resulting in the

[4] Edwards & Veale argue that the additional layer of regulation would create a 'formalistic overkill alongside a lack of substantive change', see Lilian Edwards & Micheal Veale, 'Slave to the Algorithm? Why a 'Right to Explanation is Probably not the Remedy You Are Looking for,' [2017] 16 Duke L & Tech Rev 80, 18-81

[5] In particular, the idea of a 'one stop shop' mechanism was to ensure each member state had in place a competent authority to enforce the provisions of the GDPR; it was considered burdensome, particularly where its decisions could be overridden by the European Commission. There was also a range of implementing acts required by member states which might impact the key objective of harmonization, see Orla Lynskey *The Foundations of EU Data Protection Law*, (OUP 2015) p 69-71

[6] This question of responsibility was partially addressed in the E-Commerce Directive 2000/31/EC which determined that internet service providers would not be held responsible for hosting where there is no actual knowledge of illegal activity or information (Art 14)[6] or for monitoring (Art 15).

[7] Christopher Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernian Revolution in European Data Law', [2012] Bloomberg BNA Privacy & Security Law Report 6 Feb 2012 1-15, 11

[8] The Data Protection Directive, 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31

likelihood of inconsistent application by member states. However, to others[9] it was clear that Article 17 could potentially be considered a different right to the that determined by Google Spain; even the name of the right was changed to become the 'right of erasure'.[10] This potentially made the provision more complex, although it was argued that the new name aimed to avoid the emotive content of the right to be forgotten and allow the new Article 17 to reflect its data driven function.[11] This chapter investigates how, from initial discussions, the right to be forgotten developed through Google Spain to the finalization and implementation of Article 17 and examines the issues that arose in establishing its scope.

3.2 Towards a new data protection regime

The early focus on the right to be forgotten, in respect of the retention of information, reflected awareness that use of the Internet emphasized the availability of information online. This was particularly exposed through social media sites with realization of the comprehensive digital memory now being created. It was also noted that exposure of such information continues long after it may have been relevant, or even appropriate, for it to be available. As early discussions were taking place on the need for greater protection in 2010, Mayer–Schonberger [12] argued that the possibility existed for actions, whether described in words or displayed in pictures in postings on the Internet, to be judged not only by contemporaries but to an unlimited extent by future viewers. These concerns were subsequently acknowledged by the EU with its intention to bring forward more appropriate data protection in a form that would meet the obligations of a fundamental right under the Charter whilst also protecting privacy and ultimately facilitating the free flow of information.[13]

---

[9] Alessandro Mantelero, 'The EU Proposal for a General Data Protection Regulation and the roots of the right to be forgotten,' [2013] Computer Law & Security Review 29 no 3, paras 1-3. He states that the provisions of Article 17 do not bring about a 'revolutionary change 'to existing rules since the recognition of the right to erase information is very similar to the existing right under Article 12 of the DPD.

[10] Art 17 'Right to erasure' ('right to be forgotten') 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: '

[11] Gabriela Zanfir, 'Tracing the Right to be Forgotten in the Short History of Data Protection Law: The 'New Clothes' of an Old Right' [2013] presented at the Computers, Privacy and *Data Protection* Conference, Brussels, 22-34 January 2014. available at SSRN: https://ssrn.com/abstract=2501312 last accessed 20 April 2019

[12] Viktor Mayer Schonberger, '*delete' The Virtue of Forgetting in the Digital Age,* (Princeton University Press 2009)

[13] see n 3 Viviane Reding, acknowledging that there was concern about the growth in technological developments she asked continuing 'Legal uncertainty and legal fragmentation are a burden for those companies – both small and large – that want to do business in Europe's Single Market. This fragmentation of

The intention to bring new safeguards in the form of a regulation with direct effect was also made clear. That the impact of the retention of personal information could, in effect, be timeless, was of increasing concern. This ability will only be increased with the imminent arrival of new 'Quantum' computers which will harness the activities of the world's super computers into even faster and ever quicker dynamic tools for the ever-flowing, potentially invasive data. [14] The result of such technological progression intertwined with the creation of artificial intelligence (AI) can potentially hinder control and accessibility to a greater extent. It therefore becomes increasingly urgent that additional controls be put in place, with clearer understanding of the impact, as argued by Solove. [15] There was an increased need for tighter controls.

However, the recognition for such a need has not always been sufficient for it to be translated into any form of statute or regulatory code. This was to change with the development of formal data protection regimes largely pioneered in Europe, but also gradually introduced on a wider global basis as awareness grew of the new data era where the necessity of provisions that could impact the correction of inaccuracies and retention of data were being explored.

3.2.1. First steps regarding recognition of the need for deletion or removal of personal data within data protection

By the 1970s, early legislation, primarily within Europe, was already focusing on data protection and had begun to introduce embryonic provisions to provide for deletion of information held or, as a minimum, to provide for rectification of such data. Within such early examples of data protection,[16] it became apparent that wherever data was held an individual needed the ability to ask for correction of inaccurate information and for it to be removed if

data protection laws in Europe is not only an extra cost for business, but it also holds back economic growth and innovation.'

[14] see press release available at https://www.newstatesman.com/science-tech/technology/2017/12/how-quantum-computing-will-change-world last accessed 9 Feb 2018; It has been said that we are 'on the cusp of a new era of computing, with Google, IBM and other tech companies using a theory launched by Einstein to build machines capable of solving seemingly impossible tasks.'

[15] Daniel J.Solove, *Understanding Privacy*, (Harvard University Press 2008)

[16] For example, in France the law put in place Law 78-17 January 1978 on Information Technologies Data Files and Civil Liberties Act n°78, In Germany German Federal Data Protection Act (*Bundesdatenschutzgesetz* [BDSG] 1977, Section 35 – *lonitle Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung*

no longer required or no longer relevant. The full extent of the invasive nature of retained information aligned with more deep-rooted ideas of shaping identity or reputation had not yet begun to emerge, but unease, particularly where state activity was involved in processing data, was growing.

For those countries that favoured personality rights, such as France, but also Germany and Italy where human rights were prominent, particularly dignity, honour, and privacy, ideas of a remedy seen as a right to be forgotten were becoming well established. In particular, the approach in Europe, specifically in the French and German legal systems, was beginning to put into effect provisions to provide an ability to lose or forget information through early steps. An example was apparent in France through early recognition of *le droit a l'oubli*. Although the early data protection law, or rather information law, put into place in 1978[17] had no explicit right to be forgotten as such, there was provision for a right of correction in legislative amendments in 2004.[18] The provisions contained in this,[19] which included the destruction of data, pre-empted the EU provisions relating to the rectification of inaccurate or old information. This provided for data that is inaccurate, incomplete, ambiguous or out of date, or by its use was prohibited, could be basically amended, rectified, or destroyed. By 2010, with its acceptance of *le droit a l'oubli*, France was prominent in calling for formal recognition of a right to be forgotten, again led through a campaign headed by Nathalie Kosciusko-Morizet, the French Secretary of State.[20] The intended law was seen to be providing for individuals to be able to request deletion of personal data as "part of a broader French government campaign to create a citizen's 'right to be forgotten' on digital

[17] Law 78-17 January 1978 on Information Technologies Data Files and Civil Liberties Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties
(Amended by the Act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data) available at: www.cnil.fr/fileadmin/documents/en/act78-17VA

[18] Under this campaign, headed by Kosciusko-Morizet, certain codes of conduct, e.g., relating to advertising for social networks and specifically for search engines, were prepared and signed by industry members, although notably not by Google and Facebook.

[19] Law 78 Art 6 para 4 contained provision that 'Appropriate steps shall be taken in order to delete and rectify data that are inaccurate and incomplete with regard to the purposes for which they are obtained and processed'.

[20] The campaign was to provide more education to French users of the Internet about the concerns over privacy, to ensure good practices were adhered to by all, and to provide not only data protection to all, but also the beginnings of a right to be forgotten in France. This was contained in two codes: Code of Good Practice on Targeted Advertising and the Protection of Internet Users ('*Charte sur la publicité ciblée et la protection des internautes*'); Code of Good Practice on the Right to Be Forgotten on Social Networks and Search Engines ('*Charte du Droit à l'oubli dans les sites collaboratifs et les moteurs de recherche*')

networks."[21] As explained by Bruno Rasle, executive director of the French Association of Data Protection Correspondents, (AFCDP) the "right to be forgotten" could be interpreted in two ways which potentially made its function unclear:

> "In the first sense, the 'right to be forgotten' is a prohibition, made in France, against the indefinite retention of personal data. The French Data Protection Act (translated from the *Informatique et Libertés* Law) requires the data controller to define a retention period compatible with the intended purpose" [22]

Working with Neelie Kroes, European Commission Vice-President for the Digital Agenda, focus on a potential right to be forgotten was indicated, but in the words of Kroes:

> "…the issue is not merely about deleting all data. Just like in real life, when you present yourself on the net, you cannot assume no records exist of your past actions. What matters is that in those cases any data records are made irreversibly anonymous before further use is made of them."[23]

This did not recognize the erasure of information as such, but focused on the ability to make it anonymous, recognizing the importance that it could no longer be attached to how one individual was portrayed. In line with privacy, the ability to reveal as little or as much of yourself or your activities as you chose was clearly regarded as important. More commentators were building on the development of ideas based on this premise and seeking a new form of recourse.[24]

---

[21] Winston Maxwell, 'Chronicle of Data Protection, Report on the French proposal'. Hogan Lovells, Nov 18 2009 available at https://www.hldataprotection.com/tags/french-privacy/ last accessed 26 Feb 2021

[22] Jennifer Saunders, 'Understanding the Right to be Forgotten in a digital world,' presented at IAPP 15 Oct 2010, https://iapp.org/news/a/2010-10-20-understanding-the-right-to-be-forgotten-in-a-digital-world/

[23] Press Release, Neelie Kroes European Commission Vice-President for the Digital Agenda Les Assises du Numérique conference, Université Paris-Dauphine, 25 November 2010 available at *europa.eu/rapid/press-release_SPEECH-10-686_en.pdf*

[24] See Alessandro Mantelero, 'The EU Proposal for a General Data Protection Regulation and the roots of the right to be forgotten', [2013] Computer Law & Security Review 29 no 3 2013 paras 1-3. Here he argues that an individual has a need to determine the development of his life in an autonomous way 'without being perpetually or periodically stigmatised as a consequence of a specific action performed in the past…'

This ability to control information had already been accepted in Germany where early ideas within the German Constitution,[25] namely Article 1, relate to the right to human dignity.[26] In Article 2 this right is increased with the free development of one's personality, demonstrating the importance of such entitlements.[27].

As early as 1983, revolt against a national census, seen by German citizens as invasive, led to the spelling out of what was seen as crucial protection. The German Constitutional Court, in the absence of a specific right protecting against the collection and use of such data, looked at the impact of this census, interpreting these constitutional rights in light of technological advancements. It summed up that 'the worth and dignity of individuals through free self-determination function as members of a free society lie at the core of the constitutional order'.[28] The influence of Westin,[29] as was seen in Chapter 2, contributed to the approach. His views had been widely accepted in Europe, particularly by the Council of Europe in 1968,[30] and have been gradually followed in the development of data rights, including the right to be forgotten. This was in part recognition that his view involves the right of anybody to control how others use their personal information as part of privacy.[31]

In addition to specific guarantees of freedom, the general right of personality guaranteed by Article 2.1 in conjunction with Article 1 of the German Basic Law was also important in modern developments with concurrent new threats to the rights of personality and, accordingly, 'serves to protect that worth and dignity.'[32] The ruling in this case also included specific

[25] Basic Law for the Federal Republic of Germany 1949 as amended Available https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0026 last accessed 7 June 2018
[26] Basic Law for the Federal Republic of Germany Article 1. (1) Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority. (2) The German people therefore acknowledge inviolable and inalienable human rights as the basis of every community, of peace and of justice in the world. (3) The following basic rights shall bind the legislature, the executive and the judiciary as directly applicable law.
[27] Basic Law for the Federal Republic of Germany (Grundgesetz -GG) Article 2. (1) Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law. (2) Every person shall have the right to life and physical integrity. Freedom of the person shall be inviolable. These rights may be interfered with only pursuant to a law.
[28] ibid Basic Law, Art 1.1
[29] Alan Westin, *Freedom and Privacy* (Atheneum, 1967 New York)
[30] Council of Europe's views on privacy were contained in Recommendation 509, 1968 and expanded through other recommendations of 1973 and 1981
[31] Alan Westin, *Freedom and Privacy* (Atheneum, 1967 New York) 7
[32] BVerfGE 65 (translated to be the Census), (1983)1 at para 154 of 15

reference to the obligations to protect data collected, including the right for such data to be deleted.[33] It also looked at the idea that any form of state action could affect individuals in a negative way by reducing their freedom or autonomy with regard to their personal information. This seemed to confirm that the concept of informational self-determination[34] could form part of the foundation to a right to be forgotten and was key to the approach taken by Germany. The Court argued that the increase in technological data collection and its use had very different and serious aspects. These could be used to influence an individual's behaviour, even without them knowing what data was being collected and how it was being used. Therefore, the ability to request deletion was of increasing importance. The value attached to the freedom of individuals to make choices within their ability to have such self-determination would, in the opinion of the German Court, be seriously restricted if they could not know what information about them was being collected, how it was being used and in what manner. [35] It could also be argued that a society that allows this lack of freedom would not provide any substantive rights of data protection nor individual informational self-determination.

Variations of ideas of personality rights also existed under Italian laws with a right to personal identity being inclusive of a right to be represented in society (which certainly included the media, and would later include social media). This must be in a manner that does not prejudice or distort that individual. This entitlement was based on the rights conferred under the Italian Civil Code, but also as developed by the courts who interpreted the less than explicit rights under the Code to provide for this specific right to personal identity. An early example of this was the case of Pangrazi and Silvetti v Comitato Referendum[36] where an image taken of the claimants was held to have violated their rights to have their identities protected from being misrepresented through the media. Some of the rights referred to in this case were then expanded upon in the case of a convicted, but subsequently pardoned, murderer who was referred to in a newspaper quiz some 30 years later. In Pangrazi, it was

[33] n32 BVerfGE 65,

[34] Antoniette Rouvroy, Yves Poulellet. '*The Right to Informational Self-determination and the Value of Self Development. Reassuring the Importance of Privacy for Democracy* in Serge Gutwirth, Yves Poullet, Paul de Hert, Sjaak Nouwt, Cecile de Terwangne, (eds) *Reinventing Data Protection*, (Springer 2009)

[35] 1983 Population Census Decision, Germany, 15 Dec 1983 BvR 209/83, BVerf G 65 1

[36] Pangrazi & Silvetti v Comitato Referendum, Pretura Roma 6-5-1964

held that the newspaper had shed 'false light' on the personalities of the claimants without there being justifiable public interest. Pino[37] regarded this interpretation of the case as showing a marked change in attitude as the claimants resisted the use of their photos as a means of propaganda with the use of them to represent a traditional view of a married woman and man opposing divorce.[38] This finding could be compared to cases based on similar facts following the Google Spain decision to determine if there had been any change in the way such matters were approached, following the advancements in technology and with the increasing use of social media. On this basis the ability to create some form of outline of who you are as an individual has always been considered important. This is also linked to the importance of reputation which is explored below when examining the scope of the right to be forgotten.

However, the common law system in the UK took a different approach, challenging the view of privacy held by its civil law based European neighbours. By having no express recognition for privacy under English law, there was accordingly no civil action available for any purported breach of such privacy. This lack of formal protection might be the result of the focus on the protection of property rights, which were considered to be of primary importance, as opposed to personality rights. However, it could also be argued that privacy safeguards only really developed where an element of proprietorial interest existed, demonstrated by the use of the law of confidentiality being applied to protect private information in specific circumstances[39]. As an example, in the UK early cases could be seen to largely involve members of the English aristocracy who had greater concern with reputational risk rather than the protection of disclosure of information.[40]

Gradually however, ideas of privacy and data protection were becoming linked within the UK as the growth of machines accessing data became known.[41] This combined the necessity to

[37] Georgio Pino, *The Right to Personal Identity*, in (eds) Mark Van Hoeke and Francois Ost *Italian Private Law, Constitutional Interpretation and Judge Made Laws, The Harmonization of Private Law in Europe* (Hart 2000) pp 225, 235 -23

[38] Here the subjects in the photo were pro the principles of divorce and not married to each other.

[39] OBG Ltd v Allen [2007] UKHL 21 [2008] 1AC1

[40] Duchess of Argyll v Duke of Argyll [1967] ch 302

[41] The Younger Report, Hansard 6th June 1973, Baroness Gaitskell; 'The balance between freedom of speech and privacy is a very fine one, though I think there is a difference between eliciting information and soliciting

protect personal information with elements of human life potentially protected by privacy through the legal devices used by the UK. As part of the pre-cursor to the European data protection regime's formal recognition of the need at least to remedy inaccurate data, the UK, with its initial Data Protection Act 1984, produced a right of rectification and erasure under Article 24,[42] but once again this related purely to inaccurate information. A court needed to find such a request justified the recognition of protection, so at this stage the law had limited impact. Gradually this was expanded to a more formal acceptance which only took shape as data protection progressively developed within Europe.[43]

Once the implications of continuous availability of personal information were becoming known to the millions of internet users, recognition of the need for rectification and even erasure of incorrect information became more widely accepted. Information that was becoming more easily accessed and transmitted through the Internet also contained a degree of permanency unimaginable in the pre-digital era. This new ability to transmit information was a change for which many were ill prepared. Not only had the sharing of information became so widespread, but retrieval of information was fast becoming a 'norm'. There was new focus on the ability to be able to use this information at will, for both informative and social purposes. With greater recognition of the initial steps required at least in obtaining the rectification or removal of incorrect or no longer relevant information there was a leaning towards an ability to 'forget' or even 'erase' such information. The limited provisions set out in original data protection legislation needed to be built upon in order to recognize these new requirements and the necessity of their application to a wider field to protect, as a minimum, a person's privacy. Despite there being no clear policy yet developed towards this requirement, a potential new remedy and recognition of it within the concept of data protection was beginning to grow.

---

information. We have come to a point where technology will continue to threaten our social conventions, which, after all, so often pass for our morals'. Available at: https://api.parliament.uk/historic-hansard/lords/1973/jun/06/privacy-younger-committees-report

[42] Data Protection Act 1984, Section 24. Rectification and Erasure - (l) If a court is satisfied on the application of a data and erasure, subject that personal data held by a data user of which the applicant is the subject are inaccurate 'within the meaning of section 22 above, the court may order the rectification or erasure of the data and of any data held by the data user and containing an expression of opinion which appears to the court to be based on the inaccurate data. Available at http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf last accessed 22nd May 2018

[43] Specifically through Arts 12 (b) and 14(a) of the Data Protection Directive 1995

3.3 The approach by the European Commission to recognize the right to be forgotten within data protection

3.3.1 The stages leading to acceptance of the need for modernisation of data protection

In Europe steps leading towards the implementation of the GDPR had begun with the Data Protection Directive (DPD).[44] Recognized also as providing a distinct separation from rights of privacy,[45] this had aimed to provide consistent data protection laws throughout the EU, thereby contributing to the free flow of data between member states. The policy behind the drafting of this directive was based on the need for individuals to control their personal data, whilst balanced with the accessibility of data now required commercially. In the DPD Article 12, [46] the ability to request rectification, erasure, or blocking of information was included as necessary. This provision could also cover situations where data was being processed unfairly or unlawfully. The implementation of the DPD was, however, left to be addressed by the member states. In addition, the interpretation of this specific right was for national data protection authorities and the national courts to apply, ultimately creating a diverse stance towards how such action, if indeed any, would be taken or carried out. Within the DPD, Article 12, with its limited form of recourse, provided that once a data subject had indeed identified data that was being held it would then be possible to ask for 'the rectification, erasure or blocking of data where the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data'.

[44] The Data Protection Directive, 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31

[45] Maria Tzanou, The Fundamental Right to Data Protection (Hart 2017), 21 Here she explains that the time seemed 'ripe' for the independence of data protection from privacy and also recognized some of the varying European constitutional values such as liberty (France) and dignity and personality (Germany)

[46] DPD Art 12. Right of access. Member States shall guarantee every data subject the right to obtain from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense: confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; communication to him in an intelligible form of the data undergoing processing and of any available information as to their source; knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1); (b) as appropriate the rectification, erasure, or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; (c) notification to third parties to whom the data have been disclosed of any rectification, erasure, or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

Zanfir[47] argues that as Article 12 b)[48] linked the right to object to processing of data under Article 14, this could be considered to have produced, in effect, a right to be forgotten. Significantly this right of deletion was the first step towards a right to remove personal information and represented the first attempt to provide a form of consistency in national provisions.

Building on national understandings of the ability to forget or erase information, certain states gradually expanded these limited ideas. For example, in Germany under earlier German data protection legislation[49]each citizen had the right to the 'erasure of stored data concerning him where such storage was inadmissible or an as option to the blocking of data, where the original requirements for storage no longer apply'. Acceptance of additional rights under the DPD was therefore welcomed.[50]

In Italy there were further developments in 2004 when the Italian Data Authority, the *Garante per la protezione dei dati personali*, reviewed Article 11 of its data protection legislation. Following the provisions of the DPD through Legislative Decree No. 196/2003, the Italian Data Protection Code, then in force was to progress the view that the necessary quality of data could not be met if such data no longer met the objectives for which it had been obtained. Again, this acceptance of such principle was in line with ideas of personality rights inherent in the Italian laws.[51]

Other states struggled with such ideas whilst accepting the need to protect data control. and even privacy, in the changing landscape. During the reading of the Data Protection Bill leading

---

47 Gabriela Zanfir, 'Tracing the Right to be Forgotten in the Short History of Data Protection Law: The 'New Clothes' of an Old Right' [2013] presented at the Computers, Privacy and Data Protection Conference, Brussels, 22-34 January 2014, available at SSRN: https://ssrn.com/abstract=2501312 accessed 20 April 2019

48 DPD, Article 12

49 Bundesdatenschutzgesetz 1977 Section 4

50 The DPD however not having direct effect was required to be implemented into each member state's legal system, this highlighted the different approaches to the removal of information leading to lack of consistency in applying such recourse.

51 The Italian Constitution under Article 2 provides that "The Republic recognises and guarantees the inviolable rights of the person, both as an individual and in the social groups where human personality is expressed. The Republic expects that the fundamental duties of political, economic and social solidarity be fulfilled'. http://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf

to the Data Protection Act 1998 (DPA) which implemented the directive in the UK,[52] Lord Williams of Mostyn in the House of Lords[53] acknowledged the need for data protection even for necessary electronic processing.[54] With limited recognition of the relationship between privacy and data protection, the UK was taking early steps towards recognizing that loss of data protection would impact an individual's right of privacy as a minimum. However, this was still a long way from the ideas of personality expressed within Europe and beliefs seen as vital to dignity within privacy, such as the ability for past information to no longer impact an individual.

This approach was shown again in the UK case of Johnson v Medical Defence Union Limited (No. 2)[55] which looked at how data processing could be considered unfair, as well as its impact on reputation. Although the court ultimately held that the processing was fair and lawful under the DPA and that consent to the processing had been given, it also considered data protection and the impact on privacy through loss of reputation which would result in financial loss. In this case, even if a breach of the DPA had been shown, there was nothing within the act that gave the right to compensation for general loss of reputation. Although this was a form of recognition of the need to protect human rights, such as dignity, through privacy in the form of data protection, the UK did not appear to see the need to restrict availability of information as a specific formal right. It would later be seen to oppose recognition of any right to be forgotten within the early discussions of the proposed GDPR.[56] Although announced by the EC in 2012,[57] this regulation took until 2016 to finalize. The

[52] Data Protection Act 1998 c 29 This act has now been superseded by the Data Protection Act 2018.

[53] Hansard, House of Lords 5th series, vol 585, col 436, Jan 1998. Lord Williams stated 'the proposed act would affect our wellbeing in a much more general way. It shares common ground with the Human Rights Bill. These rights include the right to respect for private and family life.'

[54] n 52 Hansard, House of Lords, With recognition of the impact on privacy of the availability of personal information Lord Williams' opinion also stated that, 'The Data Protection Bill also governs privacy albeit a specific form of privacy, personal information privacy.'

[55] Johnson v Medical Defence Union Limited (No. 2) [2007] EWCA Civ 262 Bus LR 503

[56] The House of Lords European Union Committee's Sub Committee on Home Affairs, Health and Education acknowledged that where there is information about an individual which they would prefer not to be known publicly they disagreed with the incorporation of a right to remove such information. The ICO also stated vehemently that they did not want the right included largely due to the 'wrongness of the principle' i.e., that it impacted on freedom of information and its transmission. European Union Comm., EU Data Protection Law; A 'Right to be Forgotten' 2014 HL Paper 40 p54-56 available at https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf last accessed 10 April 2018

[57] See n3, in the Press Release, Viviane Reding announced 'To address all these challenges, I will propose this week a comprehensive reform of the data protection rules. There will be two legislative texts to accomplish

impact of the Google Spain decision raised further debates, however, there were also long drawn out arguments by member states on the form the GDPR would take. The inclusion of the right to be forgotten to be renamed as the 'Right of erasure' was one of the more hotly debated topics with issues around protection for freedom of expression and the idea of history being rewritten. Many believed it was not necessary, that there were existing rights and only means of identifying and removing inaccurate information was necessary.

Despite the recognition of the commercial advantages of a free flow of data, the more emphasis that was placed on such flow, the more the EU examined the unforeseen consequences of the information being so readily available. It commissioned numerous reports to be made within its organization on the impact. In particular, specific Working Parties carried out investigations into specific aspects of the retention of data, albeit with limited success in updating how such issues could be tackled.[58] Various reports included the Working Document of the Processing of Personal Data on the Internet, the Working Document on privacy on the Internet, and the Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites.[59] This movement reflected increasing concern and the movement towards updating data protection regulation in this new environment.[60]

Reflecting the intention to become the leader in providing control over data, the innovative stance of the EU moved forward by enhancing the status of data protection not only as a legal right, but also as part of a series of human rights as set out in the Charter of Fundamental

---

these goals: First, a Regulation to enhance opportunities for companies that want to do business in the EU's internal market, while ensuring a high level of data protection for individuals. Second, a Directive to ensure a smoother exchange of information between Member States' police and judicial authorities in the fight against serious crime while at the same time protecting people's fundamental right to data protection.'

[58] see Art 29 Data Protection Working Party no 654/06/EN WP 119, Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC 25 March 2006

[59] The Working Party on the protection of individuals with regard to the processing of personal data, Opinion 4/2007; Working Document Privacy on the Internet - An integrated EU Approach to On-line Data Protection-5063/00/EN/FINAL WP 37, 21 Nov 2000

Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 5035/01/EN/Final WP 56, 30 May 2000,

[60] Other research included Opinion 1/2008 on data protection issues related to search engines, and Opinion 8/2010 on applicable law.

Rights of the European Union 2000 (the Charter).[61] In fact the Charter could be seen to be a new step in dividing data protection from privacy by adding, within Article 8, a specific provision for the right to the protection of personal data concerning an individual together with a right to have certain data rectified. The EU referred to natural rights and human rights using a new term, 'fundamental rights,' which was then applied to data protection.[62] The nearest analogy to a 'fundamental right' seems to be from the EU's use of the term 'fundamental freedoms' which form the pillars of the EU providing for the EU's acclaimed priorities; freedom of the common market and the free movement of goods as well as persons, services, and capital. However Rodata argues that this term could be considered to be used to distinguish between two concepts the first being the prevention of one's family and private life as a form of negative protection whereas data protection is concerned with the use and processing of data resulting in empowering the individual providing what he calls protecting the 'electronic body.' [63] Both concepts relate to the sanctity of maintenance of dignity. It was representative of the foresight within the EU that there was not just an awareness of the commercial impact of data being used in various forms with the need for a free flow of data, but of the paradox between such acceptance and the need to protect its citizens from misuse of such data.[64]

The wording of Article 8 of the Charter[65] specifically provided for 'protection' of 'personal data'. Earlier discussions saw the proposed article as aligning with privacy, but not identifying

[61] Charter of Fundamental Human Rights of the European Union [2000] OJ C 364/1

[62] Regrettably the reasoning behind this was unclear. The Explanatory Memorandum, Charte 11 Oct 2000 only referred to existing protections such as the DPD, Article 8 of the ECHR and the Council of Europe's Convention no 108 and did not add reasoning for why this was being added. See discussion by Orla Lynskey, 'Deconstructing data protection: the 'added value' of a right to data protection in the EU Legal order' (2014) Int & Com Law Quarterly, 63 (3) p570

[63] Stefano Rodotà, *Data Protection as a Fundamental Right* in (eds) Serge Gutwirth, Yves Poullet, Paul de Hert, Cecile de Terwangne, Sjaak Nouwt, *Reinventing Data Protection* (Springer 2009) pp 77-82

[64] This is highlighted in Orla Lynskey, *The Foundations of EU Data Protection Law*, (OUP 2015) ch3, pp 47-51 where she examines the conflict between objectives and the ultimate decision to introduce an integrated approach to protect citizens' data, noting in pp 55 to 62 the resulting tension between such objectives.

[65] Charter of Fundamental Rights of the European Union, Art 8 - Protection of personal data.
1.Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected. concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.

the issues around the need to control personal data.[66] Protection implied the need to safeguard data which links back to the original ideas of such data being held, especially by government bodies or state organisations potentially against the rights of the citizens (possibly as a result of the recollections of the traumas of the second world war). However, in the author's opinion this did not represent movement towards what appeared necessary specifically the 'controlling' of access or use or, more controversially, the now public availability of such data which was just being recognized. [67]

To understand the intention behind the drafting of the Charter, authors De Hert and Gutwirth [68] argue that the Charter's recognition of a fundamental right of data protection was needed to support the EU's programme of data protection and perhaps highlight its importance as it attempted to balance the 'economic' right to have a free flow of data with individual rights and freedoms. As early as the 1970s it had been noted by the Council of Europe that the European Convention on Human Rights and Fundamental Freedoms[69] was limited in its scope and therefore could not be said to be meeting new developments in information technology. There was additional need for protection against invasions of privacy by public bodies and generally an insufficient response to the challenges of a digital memory.[70] These steps were, however, constructing the new European regime in which the GDPR would be the defining foundation.

---

[66] See n61, also Explanations relating to the Charter of Fundamental Rights OJ C 303, 14.12.2007, p. 17–35 In this to the proposal for the charter it was recognized that 'The scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life'. However, this did not specifically pinpoint the reasoning behind such protection.

[67] This highlighted the loss of autonomy in determining how much personal data should be available and questioned the effectiveness of concepts such as consent particularly in tracking secondary tranfers see Antoinette Rouvroy, Yves Poullet *The Right to informational Self Determination and the Value of Self-development: Reassessing the importance of privacy for Democracy* ch 2 ; Stefano Rodotà, *Data Protection as a Fundamental Right* both in (eds) Serge Gutwirth, Yves Poullet, Paul de Hert, Cecile de Terwangne, Sjaak Nouwt, *Reinventing Data Protection* (Springer 2009) ch 3 p 81 which introduces the idea of 'networked people' being those constantly on the net.

[68] Paul De Hert, Serge Gutwirth, '*Data Protection in the case law of Strasbourg and Luxembourg; Constitutionalism in practice*' in (eds) Serge Gutwirth, Yves Poullet, Paul de Hert, Cecile de Terwangne, Sjaak Nouwt, *Reinventing Data Protection* (Springer 2009) pp 3 -44

[69] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 134 November 1950, ETS 5

[70] n 68 Paul De Hert, Serge Gutwirth p 5

It was also becoming clearer in early discussions from 2009 onwards, that rationales behind the developing data protection regimes were beginning to focus on the ability for individuals to express some form of self-determination in respect of data, particularly in the light of increased electronic communications. Early arguments by Helen Nissenbaum were concerned that at this time:

> 'a) there is virtually no limits to the amount of information that could be recorded and b) there is virtually no limit to the scope of analysis that can be done - bounded only by human ingenuity and c) the information may be stored virtually forever.'[71]

This situation also preceded the increasing ability to distribute and copy personal information available through social media. [72] This new arena and its impact had yet to be fully understood and explored. It was clear that these developments, as outlined by Nissenbaum, would adversely impact an individual's ability to exercise autonomy, to be able to make decisions as to the usage or storage of the data, and for other organizations to make decisions about such persons based on this information, whether the individual was aware of it or not. The control was not just exercised by government agencies, as seen before as an historic concern. As the new era developed, control was being taken up by commercial entities through flourishing technology and, ultimately, the Internet. In addition, despite the retaining, passing, and sharing of data, there was a lack of awareness of the consequences that could result in how a person would then be viewed in the light of such accumulated data.

The need then not just of protection in respect of data but more specifically of control, was concurrent with the new expression 'data controllers', as defined within the DPD.[73] This

[71] Helen Nissenbaum, 'Protecting Privacy in an Information Age: the Problem of Privacy in Public', (1998) 17 Law & Phil, p 576

[72] The volume of information posted online through sites such as Facebook, Instagram and similar is reported as almost 300 million new social media users each year. That is 550 new social media users each minute. Since 2013, the number of Tweets each minute has increased 58% to more than 474,000 Tweets per minute in 2019. Since 2013, the number of Facebook Posts shared each minute has increased 22%, from 2.5 million to 3 million posts per minute in 2016. This number has increased more than 300 percent, from around 650,000 posts per minute in 2011. Source Jeff Schulz, Micro Focus 'How Much Data is Created on the Internet Each Day?' available at https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/ last accessed 18 June 2019

[73] Directive 95 /46 of the European Parliament and of the Council of 24th October, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ 1995 L

referred to an entity that processed data through its 'controls.' The term potentially began recognition of the need for individuals to have the opportunity to control, rather than merely ask for protection for, their data. As a consequence, the ability to control the use, storage, and access to personal data by a request for it to be erased or 'forgotten' is clearly in line with such concepts, but also linked to the ability to exercise autonomously, or indeed to ensure dignity.

More generally, as part of the concern with the control of data, questions arose as to the extent of liability of such data controllers, where data was placed, and how such information was being used, in addition to who could access the data and for how long.[74] Increased focus combining concerns as to the volume of data being accessed and processed, together with the developing availability of data or through the Internet, now concentrated on who was controlling such data.[75] The development of the Internet was increasing the complexity of such questions as a direct result of the search engines having the ability to collate and create previously unimaginable amounts of information, the consequences of which were only just being considered. Although a by-product of the invention of the Internet, the concept itself was not new, i.e., the ability to piece together information to present a picture of an individual whether factually correct or not. Reference to a piecemeal technique, i.e., 'through use of the "mosaic" technique, a complete picture can be assembled of the life-style of even the "model" citizen', was made incidentally by Judge Petteti as early as 1984 in the ECtHR case of Malone

281/31 Article 2 provides in (d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law; Lynskey talks also about the idea 'of individual control over personal data is central to emerging information society ecosystems' see n 64. Ausloos also refers to the control component also constituting 'a predominant narrative ' in the lead up to the adoption of Article 8 in the Charter, Jef Ausloos, *The right to Erasure in the EU Data Protection Law* (OUP 2020)

[74] See in re Southern Pacific Personal Loans Ltd; Oakley Smith and another v Information Commissioner [2013] EWHC 2485 (Ch); [2013] WLR (D) 336, which looked at the liabilities of a data controller at that time

[75] Andrew Murray, *Information Technology Law* (2nd Ed. OUP 2013) Ch 19, p. 518 In this earlier version of Murray's work, soon after the announcements by the EC, Murray noted the driving force for the need for a new data protection regime could be two-fold; firstly, to ensure non-EU companies became subject to EU data protection when targeting EU citizens, and secondly, to ensure that companies based in the EU (as could be seen with Google and Facebook also established in Ireland) would be subject to one form of data regulation and one primary supervisory authority.

v the UK[76] concerning a breach of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.[77] A portrayal of an individual through such process not only increased the potential for invasion of privacy, but could also provide a form of perpetual stigmatization.

To understand the consequences of these data processes, part of the issue was then to consider who was potentially in control of them, thereby leading to questions of the responsibility of ISPs. This was partially addressed in the E-Commerce Directive.[78] However, at this stage it was determined that ISPs would not be held responsible for merely hosting services where there is no actual knowledge of illegal activity or information,[79] or for monitoring.[80] The collection of data in this new activity was generally seen to be provided by automatic processing or by algorithms collecting information, usually with limited independent inspection, intervention, or indeed verification. It became clear that even with legally obtained correct information, this information could be located and linked to false information, malicious stories, and even rumours if published or made available, however innocently, on the Internet. Through what is termed an autocomplete function,[81] word suggestions could be automatically associated with other words forming part of a complex algorithm making searches wider and quicker. However, the law around such functions was not clear and the ability to dis-associate the linking of words, unless the process resulted in an accepted breach of the law, was being hampered by lack of recourse.[82] This would be a

[76] Malone v. The United Kingdom - 8691/79 [1984] ECHR 10 (2 August 1984) URL: http://www.bailii.org/eu/cases/ECHR/1984/10.html last accessed 3rd June 2018

[77] Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14 Rome, 4.XI.1950 Art 8 '1. Everyone has the right to respect for his private and family life, his home and his correspondence.'

[78] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

[79] Directive on electronic commerce 2000/31/EC Art 14

[80] Directive on electronic commerce 2000/31/EC Art 15

[81] E.g., Google Instant, Google Suggest, Related Searches

[82] Stavroula Karapapa, Maurizio Borghi, 'Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm' [2015] Int J Law Info Tech 23 (3): pp 261-289. Here the issue of the difficulty in determining whether the search engine is a publisher, or an innocent intermediary becomes crucial. T authors report that over 25 cases in respect of search engine liability had been bought before courts in more than 10 jurisdictions with only four reaching Supreme Court level. Claims included both common law torts and statutory rights such as defamation, damage to business reputation, negligence, inducement to copyright infringement (particularly through streaming) trademark infringement as well as breach of privacy and data protection. Despite the search engine not having complete control over each suggestion and linking of wording

situation where the exercise of a right to be forgotten would provide a remedy exercisable in such circumstances. In addition, the position becomes more complex where information omitted from search results may be accessed through alternative searches suggested by autocomplete generated calculation. Other concerns from this collation of data has resulted in specific claims of defamation which result from the automatic linking of words to identifiable individuals[83]. This presented a minefield where control of data becomes a greater issue and the consequences potentially more harmful, not just to privacy, as was often claimed, but particularly to dignity and reputation.

3.3.2 Initial cases and debates on the right to be forgotten achieving legal recognition within the EU prior to the GDPR

Running parallel with thoughts of 'forgetting' information was recognition of the immediate need for rectification of incorrect or obsolete data. Many commentators tried to reconcile the need for any right to forget or erase information as a part of a series of legal steps towards the concept of redemption with the present not being over-shadowed by events of the past.[84] An example is the UK's Rehabilitation of Offences Act 1974, which provided that even information relating to criminal offences may become 'spent', i.e., no longer accurate in the present time. Many jurisdictions had put in place laws relating to the forgetting of 'spent convictions', recognizing such past activity should be prevented from impacting an individual's life.[85] The availability of information through the Internet hinders the redemption

---

it is argued that they have the capacity to exclude certain word associations through the use of filters. Certain cases supported elements of this eg Bunt v Tilley 2007 1WLR 1242 where a mental element of control was required.

[83] This has resulted in various cases, including that of Bettina Wulff who sued Google for the linking of her name with the word 'prostituierte' in search results. This caused her to be infamous for being linked to prostitution. In response Google argued that it had no responsibility as the auto generated text results only reflected what others were searching online (i.e., linking the words). The case ultimately settled out of court, see https://www.bbc.co.uk/news/technology-19542938. There were, in addition, several other reported cases throughout Europe on similar grounds, see AB v Google, Tribunale Ordinario di Milano, 24 March 2011.

[84] Mayer-Schonberger also links the ability to forget information to the human mind being able to fade memories over time which causes the prevention of being able to move on and start afresh. see also Meg Leta Jones *Ctrl + Z: the right to be Forgotten*, (New York University Press 2016) Here the author refers to this as 'Digital memory in short prevents society from moving beyond the past because it cannot forget the past.'

[85] E.g., in the US, the Second Chance Act (HR 1593) intention is to reauthorize the grant program for re-entry into the community (part of the Omnibus Crime Control and Safe Streets Act, 1968). See also Sonja Meijer, 'Rehabilitation as a Positive Obligation', European Journal of Crime, Criminal Law and Criminal Justice, 2017, Vol 25, Issue 2, here reference is made to the German right of re-socialism which is recognized as part of rights guaranteed by the Constitution. The principle is derived from respect of human dignity and a right to develop their personality freely (Articles 1 and 2 of the Basic Law)

of the individual and their ability to effectively 're-invent' themselves. Even where the initial release of such information is justified, it can clearly be argued that such justification becomes less relevant over time, or indeed as recognition of privacy rights gain in credence.[86]

In a similar fashion, by 1998 the Dutch Data Protection Act[87] widened the scope of the DPD to include the right to request correction, supplementation, or erasure of data if inaccurate, incomplete for purpose, not relevant, or in contravention of a legal requirement.[88] No jurisdiction had yet looked at the position where it was to provide not only remedies along these lines, but also solutions to meet other options to hide or remove information where it had an adverse impact of the privacy rights of an individual, despite increasing recognition of the potential need to be able to do this.

However, although the greatest impetus was within the EU, a case occurred in 2009 in Argentina which pre-empted the EU approach. This reflects the growth of awareness of the impact of the availability and longevity of free-flowing information, identifying and, to some extent, clarifying such concerns. Here the claimant, Virginia da Cunha, took action against internet giants Google and Yahoo to remove links to postings using her unauthorized name and image on pornographic sites.[89] Despite more than 200 unreported cases for removal of links made by Google, this was the case that made the headlines. To make such a claim, the claimant relied on her right of privacy, dignity, and honour as contained in the Argentinian Constitution and the American Convention of Human Rights.[90] Although she won in 2015, she was not successful in an appeal by Google. However, the case raised the profile of this new 'right' and was loudly debated, particularly in the US, as having a potentially adverse impact

[86] Meg Leta Jones, *Ctrl +Z The Right to be Forgotten* (New York University Press 2016) p 29, '…overtime the justifications for continuing to make available or to disclose old data wane as privacy rights gain legitimacy'. She also makes reference to the countries with strong systems of personality rights already evolving rights to allow information to be forgotten over many decades.

[87] *Wet persoonsregistratries* 1989

[88] This was also seen in the UK's Data Protection Act of 1998 which gave data subjects the right to have incorrect data corrected or destroyed.

[89] http://law.emory.edu/eilr/content/volume-27/issue-1/recent-developments/argentinas-right-to-be-forgotten.html

[90] American Convention on Human Rights art. 11, Nov. 22, 1969, No.17955.

on freedom of expression. With other claims[91] Argentina was leading the way through expansion of the ability to not only control personal information, but to look at how to protect reputation. Although unsuccessful, Da Cunha had claimed damages of 200,000 Argentine pesos (about $42,000) for material and moral harms, specifically for damage to her rights of personality, reputation, and privacy. The Judge, Virginia Simari, here representing the levels of concern now publicly being aired, voiced her concern[92] that the key conflict was the issues between freedom of expression and primarily the right to control one's own image whilst concentrating on the rights of reputation and privacy contained in human rights declarations and conventions.[93] As part of the discussions reference was also made to the opinions of Julio César Rivera,[94] a Brazilian lawyer who had introduced the idea that personal data should include not only the right to control one's own image, but the right for a person to correct any information, or to ask for information to be updated or deleted if out of date, and not used for the purposes for which it was obtained.

On appeal, however, the main question in this case appeared to have been the extent to which a search engine could be held liable. The details of the case, however, reflected considerable debate on a global basis as to where a 'right to be forgotten' could occur with Judge Brilla de Seret making reference specifically to the ideas propounded by Schonberger's published view that remembering had become a new 'norm'.[95]

---

[91] Julieta Andea Grinffiel, 'Don't Shoot the Messenger: Civil Liability for ISPs after Virginia da Cunha v Yahoo, Argentina & Google,' (2011) Inc 17 Law & Business Review Am 111 available at: https://cpb-us-w2.wpmucdn.com/people.smu.edu/dist/c/520/files/2016/08/17-1.pdf last accessed 20 Feb 2021
Uki Goni, 'Can a soccer star block Google's searches?', (Nov 14 2008) Time, available at http://content.time.com/time/world/article/0,8599,1859329,00.html last accessed 2 March 2020. The soccer star Diego Maradona is just one of 110 major public figures in Argentina to have secured a court order restraining the Argentine versions of Google and Yahoo from serving up search results on their names.

[92] Da Cunha, Virginia v Yahoo de Argentina s/ Daños y Perjuicos, Juzgado de Primera Instancia [Court of First Instance], 29/7/2009, (Resulta, I, para. 3) (Arg.) Opinion Simari J available at http://www.diariojudicial.com/documentos/adjuntos/DJArchadjunto17173.pdf last accessed 24 Feb 2021

[93] American Declaration of the Rights and Duties of Man, 1948, Art 2, the Universal Declaration of Human Rights, 1948, Art 12, the American Convention on Human Rights (also known as the Pact of San José de Costa Rica) 1969, Art 11, The International Covenant on Civil and Political Rights 1966, Art 17.

[94] n82 Opinion of Judge Simari, (Y Considerando, II.a, para. 6) (citing Julio César Rivera 21 Nstituticiones Del Derecho)

[95] ibid, s III, para. 3

To illustrate the depth of interest then being shown in the removal of information no longer considered relevant and the momentum being accelerated, a significantly similar case also took place in 2009 when a German citizen sought to have references removed from Wikipedia, an online resource, which recounted facts about a murder of which he and another were convicted of many years earlier.[96] The case had commenced several years previously, but only reached the Federal Court that year. In what would become a theme for future requests, the criminal conviction had been spent in line with attempts to bring about rehabilitation and in line with other jurisdictions,[97] Germany permitted erasure of such information once the conviction was spent.[98] Despite this, Wikipedia was able to defend successfully such a claim with the German Constitutional Court which overruled on the basis that such erasure was an unwarranted restriction on free speech.[99] Thus, neither of these cases confirmed a right equivalent to the right to be forgotten, but both emphasized the need for an individual — particularly where privacy rights were compromised — to be able to do more than merely correct inaccurate information.

Emphasis continued to be placed on the activities of the Internet giants as the development of the Internet continued and the influence of such companies increased, thus accelerating the availability of information. By 2010 acceptance of the requirement for a form of right to be forgotten was being examined in various actions promoted by the work of such commentators as Rouvroy[100] and Meyer Schönberger.[101] As well as concerns over posting which could affect job prospects and relationships, there was increasing concerns as to the use of posts online to mock and harass individuals. This was shown in the criminal convictions for three Google executives, sentenced for six months, for allowing the posting of a video of

[96] see https://www.theguardian.com/technology/2009/nov/13/wikipedia-sued-privacy-claim

[97] The European Court of Human Rights has determined that there is a positive obligation on states to ensure rehabilitation as was shown in *Khoroshenko v. Russia*, 30 June 2015, para. 121.

[98] This was shown in the German Federal Constitutional Court (*Bundesverfassungsgericht*) in 1973, where it recognized the right to resocialization or rehabilitation as part of rights guaranteed by the constitution. 5 June 1973, BVerfGE 35, 202 (Lebach decision)

[99] The subsequent actions by the claimants in the ECtHR are considered in Chapter 5

[100] A Rouvroy, *Reinventer L'art d'oublier et de se Faire Oublier dans la Societe de l'information Version Augmentee* (ed) Stéphanie Lacour. (Paris: L'Harmattan, 2008) pp 249-278. Available at: http://works.bepress.com/antoinette_rouvroy/5

[101] see ibid Rouvroy, also Viktor Mayer-Schönberger, '*delete' The Virtue of Forgetting in the Digital Age,* (Princeton University Press 2009)

a disabled boy.[102] This breached his privacy continuously by the non-removal of the same, despite requests to do so. This decision was then overturned by the Italian Supreme Court. Even this failed to discourage those arguing for the ability to control access to what was considered personal data which not only could be considered to invade privacy, but to impact an individual's dignity. With no clear right to request removal of postings or links to such, and with the ability for such links to be shared and shared again, the wider implications were being felt directly by individuals. Specific cases were becoming part of the Internet's folklore with growing awareness of such concerns.[103]

The availability of information seemingly without boundaries had, therefore, begun to place pressure on individuals seeking to enforce not only their right to privacy, but also their ability to maintain dignity, and even to defend their reputation through the Internet, potentially globally. As the information was primarily personal data, the need to control this exposure of data through data protection laws was now steadily increasing in profile. [104] This is despite arguments referred to by Lynskey[105] that the right of data protection relating to the control of data specifically is distinct from privacy rooted in dignity.[106]

Daniel Solove's earlier work on issues around reputation[107] also drew attention to a new world where every fragment of information could be pieced together and published on the Internet to form a permanent profile, however inaccurate, constantly available at the press

[102] *See* Trib. Milan, 24 February 2010, n. 1972; App. Milan, 21 December 2012 n. 8611; Cass., Criminal S III, 3 Feb 2014, n. 3672; *see also* Ernesto Apa & Oreste Pollicino, Modelling the Liability of Internet Service Providers: Google v Vivi Down (Egea 2013) see also Stacy Meichtry, 'Italy says Google Trio violated Boy's privacy', Wall ST J Feb 25 2010, https://www.wsj.com/articles/SB10001424052748704240004575084851798366446

[103] See Stacey Synder v Millersville University, et al. United States District Court for the Eastern District of Pennsylvania, 2008, case 2:07-cv-01660-pd

[104] Even Google were aware of the discussions; see Peter Fleischer, 'Foggy thinking about the right to Oblivion March 2011 http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html

[105] OECD 1980. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Marc Rotenberg Privacy Law Sourcebook, 2002. See also Orla Lynskey, *The Foundations of Data Protection Law*, (OUP, 1st Ed, 2015)

[106] See also Roger Brownsword. *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality* in (eds) Serge Gutwirth, Yves Poullet, Paul De Hert, Cecile de Terwangne, Sjaak Nouwt. *Reinventing Data Protection?* (Springer, 2009)

[107] Daniel J Solove, *The Future of Reputation: gossip, rumor, and privacy on the Internet* (Yale University Press 2007) Daniel J Solove, *Speech, Privacy and Reputation on the Internet*, In (eds) Saul Levmore & Martha C. Nussbaum, *The Offensive Internet* (Cambridge / Harvard University Press 2010) 15–30.

of a search button. This ability created a new aspect to the impact of information being publicly accessed, even theoretically, on an individual's ability for informational self-determination.

An increase in vocalisation around the need for further data protection expressed progressive concern as to what was significantly involved with the ease of access and availability of data through mechanical means. The European Commission subsequently announced in 2012[108] that it would be reviewing the DPD and updating the level of protection offered following on from its work in implementing the previous directives that dealt with electronic services and privacy in electronic communications.[109]

As a result, it was identified and noted that whilst the key principles of the DPD remained valid, there were new challenges facing society with increased technology creating unprecedented access to all forms of information. Whilst this related predominantly to individuals in their private capacity, there were many other concerns, including the security of such data. Such issues as the impact of globalization and the transferring and accessing of data caused further apprehension, together with relevant areas still not addressed by other regulation, such as the e-Privacy Directive. [110] Opinions from commentators such as Murray,[111] voiced concerns relating to 'automation of data gathering risks our privacy' where systems collated information "without an ability to assess or evaluate data or the sensitivity of private information".[112] Lee Bygrave also concentrated on the new techniques impacting

[108] Proposal for a Regulation of The European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 final -

[109] Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services,

[110] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) 2002/58/EC

[111] Andrew Murray, *Information Technology Law; The Law and Society* (3rd Ed OUP 2016) Ch 20 para 1 p 542

[112] ibid Andrew Murray, Ch 20 para 1 pp 542/543

> ‘certain interests and rights of individuals in their role as data subjects — that is, when data about them is processed by others. These interests and rights are usually expressed in terms of privacy, and sometimes in terms of autonomy or integrity.’[113]

The full realization of the challenges and impact of this new world on individual rights not just privacy now needed a solution.

3.3.3 The EC’s approach to providing a right to be forgotten

In 2012, a statement in a press release issued by the EC[114] made reference to this acknowledged change in technology and the resultant impact. EU Justice Commissioner Viviane Reding, the Commission’s Vice-President who became a vital champion in the progressing of protection for the individuals in a data driven society, expanded on the premise by explaining that;

> "17 years ago less than 1% of Europeans used the internet. Today, vast amounts of personal data are transferred and exchanged, across continents and around the globe in fractions of seconds."

Focusing on the new needs, she put forward the EU’s proposals indicating that

> "[t]he protection of personal data is a fundamental right for all Europeans, but citizens do not always feel in full control of their personal data. My proposals will help build trust in online services because people will be better informed about their rights and in more control of their information. The reform will accomplish this while making life easier and less costly for businesses. A strong, clear and uniform legal framework at EU level will help to unleash the potential of the Digital Single Market and foster economic growth, innovation and job creation."

This was an occasion where the need to fit commercial requirements was matched with what now seemed an overwhelming desire to safeguard EU citizens whose data was being used as

[113] Lee Andrew Bygrave, *Data Privacy Law; An International Perspective*, (OUP, 2014) Ch 1, 1

[114] Press release ‘Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses’ http://europa.eu/rapid/press-release_IP-12-46_en.htm

collateral, resulting in a loss of privacy and with more impact to yet be realised. It could also be considered that this review of the legislation was visionary in addressing the unprecedented growth of US owned corporates[115] to ensure their activities, targeted at EU Citizens, were subject to EU based data protection regulation. In addition, where such companies had based themselves within the member states, e.g., in Ireland, to take advantage of tax efficiencies, a supervisory authority bound by similar rules would provide consistent compliance within the EU.

Within this new approach, by 2012 there was finally formal recognition within the European member states that a right to forget as such should exist, or at least an ability to delete information should exist. This would include information which individuals no longer wanted to share with banks, websites, and social media, with the potential to have an expiry date on how long data could be held.[116] This was placed firmly within the data protection review, highlighting the drive towards the requirement not just to reform the existing data protection regime in the light of the individual's increased need to control their data, but to enshrine this concept within the EU's first draft of the proposed GDPR. [117]

After many discussions, EU Justice Commissioner Viviane Redding announced the EC's proposal to create such a new right within the new regulation, calling it a new privacy right - 'a right to be forgotten'. She claimed this would be a new form of control, stating that '[i]f an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system'.[118] In the words of Meg Leta Jones, this proposal was "an explicit, legislative right to

[115] The growth of these entities and the subsequent impact will be considered in more detail in Chapter 6
[116] https://www.euractiv.com/section/justice-home-affairs/news/reding-unveils-new-eu-data-protection-rules/
[117] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM 2012/11 final, Council Document 5853/12), and Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM 2012/10 final, Council Document 5833/12)
[118] n3 Viviane Reding, stating generally 'The Internet has an almost unlimited search and memory capacity. So even tiny scraps of personal information can have a huge impact, even years after they were shared or made public. The right to be forgotten will build on already existing rules to better cope with privacy risks online. It is the individual who should be in the best position to protect the privacy of their data by choosing whether or

be forgotten and to erasure"[119] which recognizes that the Digital Age, a phrase coined by Mayer Schonberger, has shifted the balance between forgetting and remembering. In the proposed regulation there was a 'formalized and mechanical right to erase personal information held by another party'. [120]

Despite reassurances that such a right did not mean that history could be re-written by the erasure of information, potentially trying to offset a clash with advocates for the freedom of expression, there was still great opposition for two reasons. Firstly, such a right already existed and did not need to be 're-invented'.[121] Secondly, the US took a very different stance to data protection. In fact, the proposal was narrower than initial suggestions as, in effect, it only looked at controlling the personal data provided by an individual as opposed to reported or collated information. Unsurprisingly, Google itself was also involved at this early stage expressing not only that the results were 'disappointing' amongst its initial concerns, but that a request to delete could place pressure on an ISP to respond promptly with no limitation as to how much information would need to be deleted. [122]

3.3.4 Final drafting of Article 17 of the GDPR; the creation of the right of erasure

The decision in the Google Spain case bought focus to the right to be forgotten debate with its decision to find in favour of Senor Gonzales' claim that the revelation of personal information relating to a former bankruptcy impacted his privacy and ultimately his reputation. This was considered by many to have bought about a new right in respect of data protection and privacy.[123] However, this assumption overlooked the on-going and lengthy

not to provide it. It is therefore important to empower EU citizens, particularly teenagers, to be in control of their own identity online.'

[119] Meg Leta Jones, *Ctrl + Z The Right To Be Forgotten*, (New York University Press 2016) p 10

[120] ibid Meg Leta Jones, p 41

[121] See n47 Gabriela Zanfir

[122] see https://www.bbc.co.uk/news/world-europe-27388289

[123] Anna Bunn, 'The curious case of the right to be forgotten', (2015) Computer Law and Security Review Vol 31, Iss 3, pp 336-350 She argues that the case provided a new right for an individual to have information relating to him no longer be linked to his name and that such right arose in light of the fundamental rights under Articles 7 & 8 of the Charter of Fundamental Rights of the EU. However, she believes that the decision of the court confirmed that the right existed within the scope of the Directive. This is confirmed by Julia Powles, 'The case that won't be forgotten' (2015) 47 Loyola University of Chicago Law Journal, p 583 available at; http://luc.edu/media/lucedu/law/students/publications/llj/pdfs/vol47/issue2/Powles.pdf
See also Simon Breheny, 'Comment: the Right to be Forgotten Online sets a dangerous precedent', The Age (online) July 16 2014 referring to and commenting on a 'right' invented by the CJEU.

negotiations taking place to bring about the required right within new data protection to be provided in the proposed regulation. The initial proposed right to be forgotten, as contained in the draft of Article 17,[124] was based on earlier provisions in the DPD, arguably strengthening these. This evoked considerable interest from both legal commentators and government bodies. Leading the legal comments on the initial draft, Andy Murray[125] viewed this proposal as a specific solution to provide help for individuals to better manage online data protection risks with an appropriate remedy. That is, should they no longer wish to have their data retained, or if there was no real reason for it to be retained, then an application for removal could be made, although he also argued that the decision in Google Spain had provided a wider remedy. This was additionally consistent with what could be considered one of the main themes of the proposed regulation that clear, informed, and explicit, rather than implied, consent was to be given to data processing so a data subject could fully understand the purpose for which their data was being supplied or retained. What was apparent was that the amount of personal data that individuals were providing to organizations, or that organizations were retaining, often without any knowledge or informed consent of data subjects, was of very real concern to the EC and was intended to be addressed specifically in the regulation. [126] Part of the much debated discussions at EU level included concerns over how consent to such data being held could be obtained without impacting the ability to have a free flow of data, particularly to enable commercial objectives. Subsequently, it was recognized that, in accordance with the majority of member states' views, obtaining 'explicit' consent would be unrealistic. Although there was a desire to ensure the deletion of information or the links making such information available, the idea of an individual providing consent to such collation of the information was considered to be immensely complicated.

By the time the Snowden revelations[127] were made public in 2013, the European Parliament had voted by a large majority to approve the initial legislation. In addition, the European

[124] In the draft General Data Protection Regulation, Art 17 was headed, 'Right to be forgotten and to erasure'
[125] Andrew Murray *Information Technology Law* (2nd Ed OUP) Ch20 Para 7 p 587
[126] Conclusions of European Council Brussels re new EU data protection and cyber security framework to be adopted by 2015, 24/25 Oct 2013
https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf
[127] This was where information was leaked to reveal the extent that access was being granted to personal data, largely the co-operation between the tech companies and the US agency NSA see
https://www.bbc.co.uk/news/world-us-canada-23123964 last accessed 10 Nov 2020 see also

Council[128] was starting to call for the adoption of a strong data protection framework within Europe. Following the decision in the Google Spain case, there was a call from 16 national parliaments to speed up such process.[129] The length of time the drafting of the regulation was taking had really begun to be noticed with further cases only adding to the level of concern about varying approaches being taken. It did not appear that there was any uniformity in the approach nor analysis as to why there had been such a delay. Issues seemed to range from differing views of data protection and privacy and how fundamental rights key to this would be evaluated, to the more mundane aspects of finding time to debate the process. The position was affected by external factors, such as elections, which complicated the running of the organization despite repeated requests for progress. Peter Hustinx, the European Data Protection Supervisor, looked at the 'attempts serving political and economic interests to restrict the fundamental right to privacy and data protection', [130] in particular looking at rising issues with regard to the disconnect between the EU and the US. Despite concerns being raised, specifically in Germany, that the proposal for a new regime was at risk of not materializing, it could be argued that this delay may have been a factor in the findings in the Google Spain case, not only in pre-empting the proposed regulation in an attempt to find a compromise, but particularly between the stances of France and Germany. By 2015 there was significant pressure to find a solution.

There was also considerable concern as to how to control fundamental issues of data protection and privacy whilst still maintaining business confidence within the EU. Opponents argued there would be a loss in revenue and reduction in competition as a result of deterrence of new entrants into the market, where the use of data was prevalent. This could

https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 last accessed 15 January 2019

[128] The European Council https://www.consilium.europa.eu/en/european-council/

[129] Cecile Barbiere, 'In a joint declaration, adopted with an overwhelming majority, the representatives of the 16 parliaments (Germany, Austria, Belgium, Croatia, France, Greece, Hungary, Lithuania, Luxembourg, the Netherlands, Portugal, the Czech Republic, Romania, the United Kingdom, Slovakia and Sweden) called on European legislators to adopt the legislative package on the reform personal data protection "by 2015".' https://www.euractiv.com/section/digital/news/national-parliaments-raise-the-pressure-on-data-protection/ last accessed 20/12/2018

[130] Press Release EDPS: Enforcing EU data protection law essential for rebuilding trust between EU 21 Feb 2014 available at https://ec.europa.eu/commission/presscorner/detail/en/EDPS_14_4

however be challenged by the growth of the internet giants.[131] The decision in Google Spain was said to be adding complexity with the determined right to be forgotten. This argument also raised the spectre of competing rights with arguments that freedom to conduct a business was also being compromised. The position was then further agitated by the CJEU ruling on the safe harbour agreement with the US.[132]

The numerous discussions that took place at EU level concerning the draft GDPR included initially labelling the new provision as a 'right to be forgotten', but later replacing it with the less controversial label 'a right of erasure.' This increased concerns that it seemed to be a rewriting of existing rights, but with the complexity of imposing it onto data controllers to determine the balancing of rights necessary for the exercise of such right.[133] Original drafting of the regulation had included nine paragraphs of the proposed Article 17, making this provision notoriously more intricate. In addition, ancillary provisions, such as the ability to request removal of data made available whilst the data subject was a child, increased its complexity. This draft even failed to mention the word 'forget', relying on provisions for erasure and 'abstention from further dissemination' in the revised versions. It was noted by the European Parliament that the words 'right to be forgotten' produced an 'emotive and misleading label', thus the words 'right of erasure' replaced the original wording and were finalized in the subsequent final draft to minimize this effect. [134]

In the final version, the draft Article contained four conditions to be met for the right to be forgotten, or more accurately the right of erasure, to apply. Compared to some of the historic ideas on the right to be forgotten, these could be considered to be more limited in scope. For example, these conditions were that: the information was no longer necessary for the

[131] Orla Lynskey, 'Delivering Data Protection: The Next Chapter', (2020) German Law Journal 21 pp 80-84. Here, Lynskey points out that between 2008 and 2018 the acquisition and mergers regime enabled Google to acquire 168 companies, Facebook to acquire 71, and Amazon 60. This dominancy may have been a greater factor in the lack of alternative providers. See also, Kieron O' Hara, 'The right to be forgotten: The good, the bad, and the ugly,' (2015) IEEE Internet Computing 19(4) 73-79

[132] Case 362/14 Schrems v Data Protection Commissioner, [2015] ECLI:EU:C:2015:650

[133] Christopher Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', (2012) Bloomsberg BNA Privacy and Security Law Report, p 11. Available http://ssrn.com/abstract +2162781

[134] The words 'abstention for further dissemination' were also removed due to input by the Working Party on Information Exchange and Data protection of the European Council in 2013

purpose for which it had been provided; consent had been revoked; the data subject had exercised their right to object to the information being held; and lastly, that a violation of the regulation itself had occurred. If such condition(s) were met, a controller would be required to erase the information without delay.[135] Arguing for the benefit of such provision, promising greater control to an individual over both personal data and potentially their reputation,[136] Commissioner Vivian Redding's statement protested that: 'it is the individual who should be in the best position to protect the privacy of their data by choosing whether or not to provide it'. The draft GDPR was considered to be putting forward a provision which was, to many,[137] a highly technical provision not truly in accordance with the nature of a fundamental right and only illustrative of the approach taken in the Google Spain case.[138]
Key to this right, however, was the deletion of data within a specific time scale, potentially with the opportunity to create a 'clean slate' and a right for unrestrained individual expression 'here and now'. Although of good intent and an indication of recognition of the needs arising, the draft regulation was not met with universal approval and faced much criticism, as is discussed further in this chapter.

Data controllers were seemingly panicked by the final version of the draft regulation as the extent of the proposals and the impact of the increased ability for data subjects to access and retain data were realized.[139] The evolution of the ever-increasing economic reliance on such

[135] GDPR Art 17(3)

[136] n 3 Press release: Vivian Reding

[137] see Bert Jaap Koops. 'The trouble with European data Protection Law', [2015] Tilburg Law School Legal Studies Research Paper Series no 04/2015 available at http://ssrn.com/abstract=2505692, see also
Winifred Veil, 'The GDPR, The Emperor's new clothes. On the structural shortcomings of both the old and the new Data Protection Law' [2018] IAPP Resource Center available at http://ssrn.com.abstract=3305056

[138] Emily Shoor, 'Narrowing the Rights to be Forgotten: Why the European Union needs to amend the proposed Data Protection Legislation', [2014] 39 Brook Journal of International Law, Shoor argues that could be seen to be more a right of erasure of information relying on specified incidents and not available where one of the exceptions applied when providers would not be required to honour requests. This is compared to the right to be forgotten seen as a right evoking privacy providing autonomy over an online identity and reputation. Ausloos talks of 'The functional approach and granular interpretation of the GDPR's scope of application' as being critical to the effective application of the right of erasure, he further concludes that whether personal data is actually erased or not depends on the controller and runs the risk of a loss of freedom and autonomy which is essential to the application of a right to be forgotten. Ausloos J, *The Right to Erasure in EU Data Protection Law*, (OUP 2020)

[139] See Winfried Veil, 'The GDPR, The Emperor's new clothes. On the structural shortcomings of both the old and the new Data Protection Law' [2018] IAPP Resource Center available at http;//ssrn.com abstract =3305056, p 11 here Veil reports that there was concern that every controller which was construed so widely as to cover many activities online would be having to fulfil many obligations to inform, to notify, to communicate, to ensure activities, to demonstrate, to verify, to document and finally to be accountable. In

data was now being recognized for example by by Viktor Mayer Schonberger in his work 'Big Data,[140] as well as the weight of this strong regulation.[141] Although the intent was clearly good, with formal recognition of the need around the permanency and accessibility of data, the draft regulation now faced strong objections. This was not merely in the EU where the UK in particular had voiced such objections, but also increasingly in the US where further concerns were being raised as to the status of the ISPs, largely US corporates.

Media coverage included debates as to the impact on the transfer and retention of data, as well as access with a focus on the US. The view expressed in the US clearly saw Europe regulation as being overly protective as to recognition of rights such as privacy and data protection to the detriment of freedom of expression. Concern as to the involvement of non-EU jurisdictions with regard to the potential extra-territorial impact[142] and the ability for the final regulation to impact the activities, particularly of the US based entities, was loudly voiced.[143]

The concluding version of Article 17, prior to the GDPR being accepted by the member states, contained the final four pre-conditions for a right of erasure. In addition, a further obligation

addition, the new provisions in the form of placed increased burdens such as Art 15 Right of access, Art 20 right to data portability.

[140] Viktor Meyer-Schönberger, Kenneth Cukier, *Big Data*, (John Murray Publishers, 2013)

[141] This was shown in the EC's release of a report 'A comprehensive approach on personal data protection in the European Union', COM (2010) 609 final, which declared that despite the DPD still being considered valid it could no longer meet the challenges posed by the increase in technology development and the globalisation of 'Big Data' and needed to be revised to be more relevant. This was subsequently confirmed by Viviane Reding when announcing the proposal for the GDPR see Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age' Innovation Conference Digital, Life, Design Munich, 22 January 2012

[142] The extension of the GDPR provisions to non-EU companies was part of the main objectives of the regulation and this formed part of the reasoning behind its implementation, to protect data belonging to EU citizens and residents. The law, therefore, applies to organizations that handle such data whether they are EU-based organizations or not, known as "extra-territorial effect". See https://gdpr.eu/companies-outside-of-europe/

[143] Omer Tene & Christopher Wolf, 'Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation'(2013) presented at The Future of Privacy Forum, White Paper, p5 Concerns raised over the extraterritorial jurisdiction included, '[M]oreover, unilateral application of extraterritorial jurisdiction undermines the emerging concept of interoperability, which recognizes that although global privacy frameworks will continue to diverge due to cultural and historical reasons, transborder data flows must be maintained and individual rights protected. https://fpf.org/wpcontent/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf last accessed 22 May 2018

to ensure the erasure was carried out within a short time frame was included.[144] Under the GDPR, it was fully intended that the proposed right to be forgotten would provide individuals with greater control over their private information with recognition that this could also the impact their representation on the Internet.[145] In what was perhaps an indication of the concern being expressed by the European Commission as to the power of the Internet entities such as Google and Facebook, but also YouTube and others, Commissioner Vivian Reding also voiced concern the role the businesses operating through the Internet would need to take; 'If we want to give a real meaning to the fundamental right to the protection of personal data, if we want individuals to be in control of their information, then business responsibility has to come in.'

However, as discussed further in Chapter 6, as the ISPs grew in strength the provision of personal data became the price that would be paid for 'free' services, potentially removing the argument that individuals were in a position to determine the provision of data. The power of many such entities in a quasi -monopolistic position meant there might be no alternative suppliers of the required services, so the opportunity to choose was not available as desired.

Despite the recognized need and apparent agreement on the final version, implementation of the GDPR floundered and the time taken by the Commission to address the issue of the differing national systems[146] was criticized. As a leading technology lawyer Murray,[147] voiced his concern that finalization of the regulation was becoming long overdue, placing pressure on jurisdictions to find resolutions to the difficulties now apparent. In his opinion, the proposed regulation was beginning to look as if it would never become law in its current form. Murray expressed his view that the proposed right to be forgotten would still be regarded with concern by US authorities considering the impact of possible additional costs that might be incurred by US companies in setting up systems to deal with applications under the

[144] GDPR, Art 17(3)
[145] Press release: Vivian Reding, Vice President, EC, 'The EU Data Protection Reform, 2012. Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age,' 22 Jan, 2012 available at https://europa.eu/rapid/press-release_SPEECH-12-26_en.htm
[146] 28 in total by 2013
[147] Andrew Murray, *Information Technology Law* (2nd Ed OUP) p 519- 520,

proposed Article 17. These also increased with the demands of trans-border data protection. It was also claimed that such entities as ISPs would potentially no longer be able or willing to provide their services free due to such costs and restraints.[148] In fact the ISPs were already facing a change in approach to their services with recognition that they were potentially taking, for their own commercial advantage, the ability to access information whether protected by copyright or other remedy.[149] As a new approach was being developed in order to provide some form of resolution to an individual's need to control their personal data through a right to be forgotten and by way of informational self-determination, it was beginning to look as if the price of doing this was a reduction in the provision of 'free' internet services, such as social media platforms.

This concern relating to the implementation and cost of providing resources to deal with the obligations imposed was also seen in the UK's Information Commissioner's reaction which was highly critical of the extent of the GDPR, he took the view that this should only address the absolute risks and abuses.[150] The UK published its formal commentary in the Government's response to the Justice Select Committee's opinion on the European Union Data Protection framework proposals, not only expressing general concerns,[151] but also concentrating on the proposed Article 17 referring to the UK's Information Commissioner's view that a "right to be forgotten" was superfluous. It argued that the use of such terminology could give rise to unrealistic expectations of ISPs for users of social media. It could also be considered that the government was concerned about the ability of commercial organisations to carry out their profitable (and potentially tax providing businesses) rather

[148] see Wired, 1 Feb 2013

[149] This was supported with the implementation of the Copyright Directive in April 2018

[150] Christopher Graham 'Data Protection Reforms must target crooks not business', The Register, 6 Feb 2013

[151] Government response to the Justice Select Committee's opinion on the European Union Data Protection framework proposals, January, 2013 Cm 8530 stated 'The Government agrees with the ICO's assertion that the system set out in the draft Regulation 'cannot work' and is 'a regime which no-one will pay for'. Under the risk-based model that the UK is advocating, it would be for data controllers to put measures in place in order to comply with the outcomes prescribed in the legislation. The ICO has estimated that the additional requirements outlined in the proposed Regulation could cost it between £8–£28 million per annum, not accounting for the loss of the notification fee income'. P 7 of the Report Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/217296/response-eu-data-protection-framework-proposals.pdf

than providing citizens with additional privacy rights.[152] Indeed it seemed almost to be condemning the new concept as being detrimental to the rights of citizens:

> 'We therefore consider that this article raises unrealistic expectations for consumers that their data can be deleted when it has been passed on to third parties. This may encourage data subjects to be more reckless with their personal data, thus undermining the intention of enhancing their protection and rights.'[153]

This was a seemingly negative response to what was generally viewed as a vital protection with the growth of the Internet. With such ongoing issues, various commentators, including Murray, prophesized that the proposed regulation would not be finalized largely due to the difficulties faced with the member states in reaching agreement.[154] He concurred, however, that it was equally clear that the existing regime based on the DPD could no longer continue in its insubstantial form. He also anticipated that many changes, particularly those focusing on the right to be forgotten, would need to be made in 2014 or 2015 to ensure agreement and sufficient progress before the GDPR could be implemented. Included within this recognition was the increased awareness that vast amounts of data would be stored, perhaps indefinitely, with further consequences linking individuals to data not merely inaccurate or misleading, but potentially portraying someone in a negative light. It may seem odd that with the protection of individuals clearly at the core of the increased regulation there should be such an outcry against the proposed right to be forgotten proposed in Article 17 of the GDPR. If unpicked and viewed with the stated aim of the EC to not only update the data protection legislation, but to harmonize it throughout the EU, it should not have been considered controversial if its intent was only to build on existing rights already contained in the Directive and often recognized by member states' own legal systems.[155] However, before the full

---

[152] see n151 referring to the Justice Select Committee's comments 'The right of citizens to secure the erasure of data about them which is wrongly or inappropriately held is very important, but it is misleading to refer to this as **a** "right to be forgotten", and the use of such terminology could create unrealistic expectations, for example in relation to search engines and social media.' (Para 63) The Government agreed with the principles of deletion but argued as to the practicality particularly of information posted online.

[153] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/217296/response-eu-data-protection-framework-proposals.pdf

[154] Andrew Murray, *Information Technology Law* (2nd Ed OUP) p 519- 520

[155] Art 12 b) combined with the right to object to processing of data under Art 14 of the Data Protection Act 1998 implementing the Data Protection Directive, 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31

examination of the GDPR could be considered and agreed, the decision in the Google Spain case[156] was announced and the next stage of the debate on the nature of the right to be forgotten commenced.

The case featured the first EU acceptance of the right to be forgotten, but did it really take the world by surprise? This view is unlikely when considering the work done in progressing the ability to control personal data through rectification of inaccurate data, removal of out of date or irrelevant information, etc. Mayer Schönberger's work[157] had led the focus away from the acceptance of the commercial value of such data to the need to exercise some form of property rights over it, recognizing that loss of control over data may not really compensate for the availability of other information and its subsequent impact on privacy, dignity, and reputation, or the loss of any ability to provide for informational self -determination. Some form of action had been required and this finally came with the decision of the Google Spain case. This took the opportunity to not only reject existing ideas of who could be considered a data controller, but even to pre-empt the finalization of the GDPR to provide the elusive right to be forgotten.

3.4 The immediate response to the finalisation of the right to be forgotten

There was certainly a varied response to the Google Spain decision. This is discussed in more detail in Chapter 4 in order to assess the importance and influence of the case on the development and final creation of the right to be forgotten. It was clear, however, that the CJEU could be seen to have pre-empted the proposed regulation with its own interpretation of the DPD using the balancing of human rights[158] to determine a right to be forgotten. Equally the decision could be considered a catalyst to the finalisation of the GDPR's provision in Article 17. However, this did not mean that the various discussions concerning the purported right had gone away.

---

[156] Case C- 131/12 Google Spain Sl Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González Case, [2014] ECLI: EU:C:2014:317 (Google Spain)

[157] Viktor Mayer-Schönberger, '*delete' The Virtue of Forgetting in the Digital Age,* (Princeton University Press 2009)

[158] Specifically here rights of privacy and freedom of expression

The final form of the GDPR was clearly intended to try to defuse the debate then exaggerated by the Google Spain decision by providing not only the ability to remove links to information building upon the DPD, but the information itself. The final wording in Article 17, headed 'The Right of Erasure (the Right to be forgotten)' and provided concisely in para 1, states that the data subject could obtain 'without undue delay' the erasure of personal data on specific grounds.[159] It was equally clear in paragraph 2 that the conditions of the right would not apply where the processing was necessary for the exercise of the freedom of expression and information, or indeed for public interest. It included instances where the removal of the information[160] would render it impossible or seriously impair the achievement of the objectives of that processing.[161] To add to the complexity, part of the criticisms made regarding Article 17 were based on the structure of the actual wording of the provisions. In Article 17 (1) there is a duty to achieve a specific response, i.e., a deletion of links to information accessible by third parties (this is usually inferred to be the Internet but can be applicable to other media). By contrast, in Article 17 (2) there is only an obligation to take 'all reasonable steps', a much lesser obligation. These provisions add to the misunderstanding of the obligations and ability to meet the terms of the article which can also increase where national legal systems differ in approach.

In the foreword to the GDPR, the intent of the regulation was set out in considerable detail and it was expressly stated that the processing of personal data would not be declared an absolute right, rather as one that must be 'considered in relation to its function in society and be balanced against other fundamental rights in accordance with the principle of

[159] During what is termed the Travaux Preparatoires, the wording was different and Art 17 was headed the 'Right to be forgotten or right to erase', but MEPs and US commentators expressed their concern that this was intended to create one right and this heading might imply two versions of it.

[160] GDPR Art 17 para 1 provides that personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

'a) the data subject withdraws consent on which the processing is based according to point: (a) of Article 6 (1), or point (a) of Article 9 (2), and where there is no other legal ground for the processing;

b) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

c) the personal data have been unlawfully processed;

d) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

e) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).'

[161] GDPR Art 17 para 3

proportionality', [162] echoing the balancing of interests exercise carried out within the Google Spain decision. The fact that this could potentially impact the right for freedom of expression created wider controversy, particularly with states which were more opposed to protecting privacy at the cost of reduced freedom of expression. However, the wording within the provision shows that it was not limited to privacy but could include other allied rights, such as dignity and reputation.

Despite the initial lack of unity around the debate on the final wording of Article 17 containing the right to be forgotten, or right of erasure as it became, it failed to meet all the views held by differing jurisdictions. To many it was unsuccessful in meeting the existing provisions under previous legislation, for example in France.[163] There were claims that an obligation already existed whereby the data user should inform third parties who had access to the personal information and that it must be corrected or destroyed, narrowing the provisions of the soon to be implemented Article 17 (3) of the GDPR. Even the UK as an opponent of the new right under Article 17 had similar provisions already in its Data Protection Act 1984.[164] That is, there was a right of rectification and erasure, although the court would be required to determine if such right could be exercised. Despite the challenges presented at the time of constructing the right, it appeared that its acceptance would ultimately take place within those states affected. Reflecting on the wider decision to formulate the right to be forgotten, in the words of Gabriela Zanfir[165] it was an 'old right in new clothes'. However the main focus of the exceptions to the ability to exercise the right to be forgotten is the protection of freedom of expression as well as different approaches to the concept of free speech. This potential conflict illustrated the fundamentally and specific differences of approach opening up between the US and the EU.

As was seen by the stance taken by Google, the US's position, not only on data protection, but specifically on any acceptance of a right for publicly accessible information to be 'forgotten', was inherently different to that of the EU and the UK. The diverse approach was

[162] GDPR Foreword para 4
[163] France*, Loi relative a l'informatique aux fichiers et aux libertes* , 1978 Art 38
[164] UK, Data Protection Act 1984 Art 24
[165] see n 47 Gabriela Zanfir,

referred to by James Whitman[166] as 'Liberty' versus 'Dignity.' The US did not consider that there was any need for such a right and indeed the ability to refer to it as a right was hotly contested. Initially reaction to the right had been muted, but became more vocal as the implications of the claim of such a right became more understood. An aggressive response by Rosen[167] brought media attention to what was then being argued as the biggest threat to American values and 'to free speech on the internet in the coming decade.' In his view the right could transform Google, for example, into becoming censorship in chief for the European Union rather than a 'neutral platform'.[168] As had been seen previously, the approach to privacy, where the importance of freedom of expression and the ability of the general public to be informed was paramount, had taken a different perspective to that expressed by Europe. The introduction of concepts such as a reasonable expectation of privacy were not feasible in a regime where privacy was lost as soon as there was any public awareness of the individual. The US based courts would struggle with the ability to erase information which, however private, had already been made public.[169]

This contrast to the European approach allows for publication of someone's criminal history under the First Amendment, with its focus on freedom of expression. The widely reported case where Wikipedia, to the expressed approval of US media and commentators, resisted the efforts of two Germans convicted of murdering a famous actor to remove their criminal history from the actor's Wikipedia page.[170] The fate of these two men was to have considerable legal impact within a short time as they pursued their claim to have their past forgotten through other channels.

---

[166] James Q Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty', [2004] Faculty Scholarship Series Paper 649 available at http://digitalcommons.law.yale.edu/fsspapers/649

[167] Jeffrey Rosen 'Symposium Issue; The Right To Be Forgotten', (2012) Stanford Law Review Online Vol. 64 p 88 https://review.law.stanford.edu/wp-content/uploads/sites/3/2012/02/64-SLRO-88.pdf last accessed 13 Nov 2020

[168] ibid. 'This could transform Google, for example, into a censor-in-chief for the European Union, rather than a neutral platform'

[169] Jasmine E MacNealy, 'The emerging conflict between newsworthiness and the right to be forgotten' (2012) Northern Kentucky Review vol 39.2 119-135 available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2027018 last accessed 22 Jan 2019

[170] available at see https://www.theguardian.com/technology/2009/nov/13/wikipedia-sued-privacy-claim

Fundamental to the approach taken by the US to fight any suggestions of a viable right to be forgotten, it is essential to understand more broadly how the US view of data protection, and indeed privacy, is crucially different from that of the EU. The Fourth Amendment to the US Constitution does not provide for privacy but for a reduced right, specifically for the people to be 'secure in their persons, houses, papers and effects against unreasonable searches and seizures'.[171]

The hostile relationship created by the differing viewpoints of Europe and the US over the requirement for data protection, notwithstanding the subsequent acceptance by Europe of data protection as a fundamental right, caused severe friction in the 1990s which was only subdued by the creation of the Safe Harbour agreement in 2000[172]. This in itself then became a more contentious issue with concerns around the access to personal data particularly in the US which will be explored later on in this thesis[173]. Generally, the US regard the European approach towards privacy as too protective, meanwhile the Europeans argue that the American way of permitting access to information is intrusive and a violation of citizens' rights.. Not only the right to privacy, but the right to dignity is challenged as well as ideas of personhood which looks at privacy through a lens based on 'rights to respect and personal dignity.' The German offering of informational self-determination, i.e., the right to control information disclosed about oneself, is also a key component to such European views, but hotly disputed by US commentators. Whitman speaks of the 'transatlantic clash' with the idea of privacy differing from society to society. [174] However, the idea that liberty is at the forefront of any US rights when looked at through the intrusion by the state, as shown in the

[171] 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, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized' https://www.law.cornell.edu/constitution/fourth_amendment

[172]2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.)https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520

[173] see Ch 5 p 211 onwards

[174] James Q Whitman, The Two Western Cultures of Privacy: Dignity versus Liberty, (2004) Faculty Scholarship Series Paper 649 p1153 available at http://digitalcommons.law.yale.edu/fsspapers/649

revelations through Snowden and WikiLeaks, [175] argued by Whitman seems a contradiction. Not only can it be argued that standards for protection of privacy reveal two different attitudes to privacy but as Tzanou points out this view does not acknowledge the vertical and horizontal application of data protection and privacy providing application against not only the state but also against private individuals.[176]

The occupation with intrusion by the media, as highlighted in the UK, France, and Germany, has little however in common with the concern as to State violation, particularly in the American home. Moreover, the depth of differing approaches cannot be explained so simply.[177] Even Weston could have been considered to have been of the opinion that privacy evoked control of the public image presented. Erving Goffman[178] argued, very much earlier, for the 'presentation of self' which could be a breach of privacy if we were unable to control this, i.e., the image of ourselves in the eyes of others. Is this privacy or a right to a public face?

Notwithstanding that targeted collection of data, particularly of non-US persons, is now recognised to be considerable, as seen in the Snowden revelations, the indiscriminate collection of detailed and very accurate data without knowledge or consent had become of worldwide concern. Within the Fourth Amendment, information could be collected and shared where individuals had no 'reasonable expectation of privacy', presenting an issue for a data subject who had no control over how his personal data was being collected, by whom, or for what purpose. This had led to the establishment of the third-party doctrine in the US

[175] Press Coverage of the Snowden revelations, available at;
https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 Last accessed Nov, 2018

[176] Maria Tzanou, 'The war against terror and transatlantic information sharing: Spillovers of privacy or Spillovers of security?' (2015) 31 (80) Utrecht Journal of Int. & European Law 87

[177] Although the US is regarded as being the more intrusive state, studies have shown that the tapping of telephones is greater in France and Germany and even more in Italy and the Netherlands, see Hans Jorg Albrecht et al., *Rechtswirklichkeit und Effizienz der Uberwachung der telekommunikenation nach den 100A 100B stop und Anderer verdeckter ermittlungsmabnaahmen* translated to 'Legal reality and efficiency of the surveillance of telecommunications according to ss 100a, 100b StPO and other covert investigative measures A factual legal investigation on behalf of the Federal Ministry of Justice', available at the Max Plank Institute: https://csl.mpg.de/en/publications/rechtswirklichkeit-und-effizienz-der-uberwachung-der-telekommunikation-nach-den-100a-100b-stpo-und-anderer-verdeckter-2/

[178] Erving Goffman 'The presentation of self in everyday Life' (1959) Edinburgh University Social Sciences Research Centre accessed at;
https://monoskop.org/images/1/19/Goffman_Erving_The_Presentation_of_Self_in_Everyday_Life.pdf

which provides that any information shared with a third party is no longer considered 'private' other than certain exceptions for legally recognised confidential relationship e.g. lawyer/client. Any information so shared is no longer considered private and is therefore not protected. Established in Smith v Maryland,[179] the court found that a person had no such reasonable expectation of privacy in information voluntarily provided to another party. This had also been raised in the case of United States v Miller some years earlier where Miller argued unsuccessfully for protection against a government search of his bank accounts.[180] In Smith V Maryland, the argument was that phone numbers dialled were capable of 4th Amendment protection and would therefore be protected against intrusions into the privacy of individuals. [181] However as the third party phone company had passed on information to the Government, the 4th Amendment was held to no longer apply as the relevant information had been shared. Whilst the doctrine is widely accepted, in more recent years with new technology providing increasingly invasive tools, Justice Sotomajor in the case of United States v Jones which involved the use of GPS a tracking device, took the opportunity to declare that the doctrine was no longer appropriate and that all information disclosed would or should be worthy of protection under the 4th Amendment. [182]

The impact of this doctrine however could be very relevant to how personal information could be made readily available through the use of the Internet to other parties where the individual concerned had little or no control over how access was given and to whom. Potentially, any affected individual would be anxious to not only obtain details of the data, but to ask for removal of any links to information considered no longer relevant as a minimum. Disputing an individual's ability to exercise the right to be forgotten outside of the EU, despite the knowledge of personal data being held and accessed, the US decision makers made it clear that they did not regard this right as being material and would not accept any of the constraints imposed by it. It has been argued[183] that the revelations of Snowden[184] and

[179] Smith v Maryland (1979) 442 US 735
[180] United States v Miller (1976) 425 US 435
[181] Katz v United States (1967) 389 US 347
[182] United States v Jones (2012) 565 US 400
[183] Melissa de Zwart, *Privacy for the weak transparency for the powerful*, in Andrew T Kenyon, (ed) *Comparative Defamation and Privacy Law* (CUP 2016)
[184] Snowden revelations; see https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 last accessed 10 Nov 2018

Assange[185] were created in an attempt to highlight the lack of privacy, particularly in light of the US approach. There would be no easy route to applying any right to be forgotten in whatever form. In addition, reviews following the decision not only in Google Spain, but in the creation of the right of erasure under Article 17 of the Regulation, despite being based on the existing rights under the Directive and other national remedies,[186] has been seen as a contradiction to the First Amendment relating to freedom of speech and the ability to restrict information to a right of censorship. Under the European approach, the passage of time can alter how the information should be viewed and made available, whereas for the US there is no time restriction on freedom of expression and there is little appetite for information to just fade over time.[187]

3.5 Conclusion

The emergence of the right to be forgotten, initially through concepts contained in Chapter 2 by establishment of rights of privacy and dignity as well as the development of the fundamental right of data protection, has been finalized by the implementation of the GDPR. This recognition has formed part of a wider acceptance of the need for modernisation of data protection to provide the necessary tools for an individual to control the information that is accessible and which potentially impact how they are portrayed. Whether or not it can be considered that the decision in Google Spain pre-empted such finalization, the position is clear that the right to be forgotten is now accepted as valid recourse, or a right for those who wish to maintain their privacy through the control of the availability of personal information, particularly on the Internet. To do so not only requires fitting data protection but the ability to include wider rights of recourse, e.g., the protection of dignity in the form of personhood and reputation by determining how a person can be portrayed. The right to be forgotten in the form of Article 17 of the GDPR must be viewed as being built on the more limited grounds of existing legislation but can also be considered to stand for more individual rights in the

[185] This involved the exposure by Wikileaks of certain activities in the US through the action of Julian A series of leaks provided by U.S. Army intelligence analyst Chelsea Manning included the Baghdad airstrike, the Afghanistan war logs, the Iraq war logs and Cablegate.

[186] *Bundesdatenschutzgesetz* , the German Federal Law 1977, *Loi relative a l'informatique aux fichiers et aux libertes* 1978 France, the Data Protection Act UK 1984 *Wet Persoonregistraties* 1989

[187] 'Ordering Google to Forget', The New York Times, May 2014, available at https://www.nytimes.com/2014/05/14/opinion/ordering-google-to-forget.html?r=0 last accessed 10 April 2019

guise of autonomy and the ability to present one's identity in a digitalized world. It affords a wider protection than as offered under data protection i.e., providing the ability to control the use of data, to request removal of inaccurate information as well as the restricting of the retention of no longer required data or rectifying inaccurate or potentially misleading data. The right therefore allows the ability to 'pick and choose' which data and which aspects of personal information can be accessed to portray the individual as they so determine. It also offers more than privacy as it is not just about forgetting specific information but retaining part of that which can be used in portrayal of self as so desired, thus offering wider scope. Such rights form part of the fundamental values necessary to provide each human with the tools to protect their individuality and sense of self balanced with freedom of expression. Direct opposition to the right to be forgotten from outside of the EU, particularly the US emphasis on liberty in the form of freedom of expression, means that it is vital to define more clearly where such right can and should be used and its value in providing informational self-determination. The ability to control access to the information collected and collated about oneself must therefore be of inherent value i.e., that it offers an ability that originates in oneself and is exercisable through one's own experience and need. Although freedom of expression must be respected, it must also be balanced with other rights to provide a rounded approach, particularly within the clamour around the benefits of the Internet. The formalisation of Article 17 provides this opportunity, however to establish the value the right will ultimately provide in such informational self-determination, the next chapter considers the impact and background of the Google Spain case and its role in creating principles that will be applied in balancing competing rights.

Chapter 4 -The influence of the Google Spain case in the development of the right to be forgotten

4.1 Introduction

As shown in Chapter 2, ideas of a right to be forgotten have been developing over a period of time, arguably initially derived from the French, *le droit d'oubli*,[1] with recognition in other jurisdictions, such as Italy, leading to the most recent form within Article 17 of the General Data Protection Authority (GDPR). The intent to rein in the wide-reaching scope of the Internet, where a form of digital memory has been created, was becoming vital. New functions are increasingly impacting humankind through social media and other methods of accelerating the copying of information, however derogatory. These concern not only the rights of privacy and data protection but of dignity and, ultimately, reputation as well. The accessibility of the Internet has moved rapidly from computers to laptops and then to ubiquitous smart phone technology and, through the use of social media, has become an increasingly invasive means of communication in conjunction with the ease of availability and retention of data and its access. This is an area that has not been seriously considered in early data protection but which is fundamental to the changes brought about by the GDPR with its extensive coverage focused on not only consent but accessibility of data.

The breadth of the growing data protection regime, however, has also caused concern. This is reflected by Lucas Bergkamp[2] who considered the impact of the depth of the data protection affecting consumers by giving them more limited choices, as well as potentially higher prices. In his opinion 'EC data protection laws impose an onerous set of requirements on all sectors of industry, from financial institutions to consumer goods companies, and from list brokers to any employer. It applies to personal data processed by conventional or automated means.'[3] He further argued that there was no real evidence to show the harm to consumers or data subjects if privacy was reduced, particularly if compared to the benefits that could accrue from the free availability of information, not just for commercial reasons

[1] Data Processing, Data Files and Individual Liberties Act of 6 January 1978, Law No. 78-17,
[2] Lucas Bergkamp, 'The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy (2002) Computer Law and Security Report 18(1) pp 31,42 https://www.huntonak.com/images/content/3/2/v3/3292/Privacy-fallacy.pdf last accessed 29 March 2020
[3] ibid Lucas Bergkamp, p 32

but also for educational and social activities. As this view was expressed in 2012, as shown in the earlier chapters, the approach to data availability was to change quickly in the next few years. It could therefore be argued that the loss of privacy would be the price paid for access to 'smart' technologies and the resultant power of those entities providing the same. The need for constant online access may have blurred the lines on the real cost to individuals in providing personal information, a concern echoed by leading advocates of privacy,[4] as the debate on the right to be forgotten was fully emerging.[5]

Legal appreciation of the extent of access, almost without limit, to information now available on websites and through the creation of apps to be used on mobile phones as well as on other devices, had been slow in being fully understood, despite the evolution of wider data protection.[6] Even so, within the slow creep of knowledge there had been some farsighted viewpoints that had anticipated future developments and laid the foundations of how protection and control may be required. As early as 1968, Professor Charles Fried[7], one of the initial thinkers on how new technology was beginning to impact daily life, had considered this within various aspects of privacy.[8] In such examinations he concluded that its definition needed to be refined, or reassessed, to ensure privacy was not simply based on secrecy but could include the ability to reduce information held about a person through removal,

[4] Helen Nissenbaum, 'Protecting Privacy in Public, The problem of Privacy in the Information Age' (1998) 17 Law and Philosophy pp 559, 562

[5] Serge Gutwirth, *Privacy and the Information Age*, (Rowmans & Littlefield Publishers 2002) p 61

[6] The challenge of the 'Internet of things' (IoT) is only just being realised with growing awareness in both the EU and the US. The policy statement from the EU highlighted that the IoT 'represents the next step towards the digitisation of our society and economy, where objects and people are interconnected through communication networks and report about their status and/or the surrounding environment.' https://ec.europa.eu/digital-single-market/en/policies/internet-things This is also recognised by the US where the House of Representatives passed a bill on the security of the IoT; "Internet of Things Cybersecurity Improvement Act of 2019" sets baseline cybersecurity standards specifically for IoT devices purchased by the federal government.

[7] Charles Fried, 'Privac*y'*, Yale LJ 475 477-478 (1968) accessed at http://www.jstor.org/stable/pdf/794941.pdf?refreqid=search%3Aa8f896894d0271a6c5f713b3148c1804

[8] ibid Charles Fried, see p 475 'The more insidious intrusions of increasingly sophisticated scientific devices into previously untouched areas, and the burgeoning claims of public and private agencies to personal information, have created a new sense of urgency in defence of privacy' He also foresaw information tracked by a small device that would also be able to collect facts and most importantly store data about the person such as 'his temperature, pulse rate, blood pressure, the alcoholic content of his blood, the sounds in his immediate environment.' Incredibly, he even foresaw brain patterns being recorded, an early forecast of biometric data, now increasingly being categorised as 'sensitive personal data'. The GDPR Art 9 refers to sensitive personal data as "special categories of personal data". The special categories specifically include genetic data and biometric data where processed to uniquely identify an individual.

rectification or even irrelevancy. These early thoughts reflected the idea of a right to be forgotten which would provide for an ability to reduce such information. Key to consideration of such a right would be the idea of informational self-determination. In his opinion the concept of privacy was not just based on less information ensuring more privacy but, more importantly, that:

> "Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves"[9]

The introduction of data, whether processed through automatic means by new entities, the so-called ISPs, or increasingly search engines, in terms of its collection clearly involves the loss of privacy through the availability of such data, as a minimum. This also highlighted the lack of an individual's control over primarily mechanical actions.[10] Increasingly affected by the growth in algorithms, concern was added by additional future developments, such as the concept of block chain, with the ability to hold documents and information in a virtual 'world'.[11] The ability to restrict such processing and storage of data is clearly vital to the control of individuals' personal data. This adds further complexity to a new and not yet fully understood data environment, although now part of everyday life.

Despite the attempts by the EU to develop and future proof the data protection regime with the GDPR and to include rights in respect of personal data, particularly when no longer required, out of date, or in need of rectification, as well as to observe fundamental rights, the impact of the decision to find a right to be forgotten in the Google Spain[12] case cannot be

[9] n 7 Charles Fried p 482

[10] Stavroula Karapapa & Maurizio Borghi, 'Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm' [2015] International Journal of Law and Information Technology, 0, Int J Law Info Tech 23 (3): 261-289

[11] Each "block" represents a number of transactional records, and the "chain" component links them all together with a hash key function as records are created, they are confirmed by a distributed network of computers and paired up with the previous entry in the chain, thereby creating a chain of blocks, or a blockchain. The entire blockchain is retained on this large network of computers, meaning that no one person has control over its history. That's an important component, because it certifies everything that has happened in the chain prior, and it means that no one person can go back and change things. available at https://www.digitaltrends.com/computing/what-is-a-blockchain/ Last accessed 29 March 2019

[12] C- 131/12, Google Spain Sl Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González (Google Spain) 13 May 2014 :EU:C:2014:317

underestimated. The decision was not merely an exercise in data protection but a drawing together of rights that individuals could take advantage of in the sought-after desire to control the availability of, and wide access to, personal information through activities conducted via the Internet.

4.2 The Google Spain decision: the need for formal control over the retention and access of data on the Internet

In previous chapters the development of privacy was seen as an essential component of human dignity also underlying the growth of recognition of data protection as a fundamental right. Both are vital requirements to ensure that the new era of technology did not rob citizens, or the data subjects they had become, of rights in respect of their personal information or data impacting their dignity or reputation. All of these led to an increased interest in a right to be forgotten. With the slow movement to bring regulation and legislation in line with developments of technology ultimately culminating in the final drafting and implementation of the GDPR, a formal recognition of the right to be forgotten, whether as a right of erasure or even a right of de-linking, meant the impact of the decision in Google Spain was of unprecedented importance.

4.2.1 The background to the case being heard

From many aspects it was no coincidence that the most significant case on the topic of an ability to forget information, as debated in the claim of a 'right to be forgotten', came from Spain. Although no specific law granting such a right existed in Spain, there was clear acknowledgment that this right potentially formed part of the human right of dignity, comparable to the personality rights consistent with civil law regimes within Europe. This view had also aligned with the French right, '*le droit à l'oubli*,'[13] partially recognized in various European countries, including the UK, as the ability for a criminal to request removal of reference to past crimes as part of a rehabilitation process and potentially a rebuilding of reputation. Legal reference in Spain had been made as early as 1991 to the existence of such

[13] Law 78-17 January 1978 on Information Technologies Data Files and Civil Liberties Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties
(Amended by the Act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data) available at: www.cnil.fr/fileadmin/documents/en/act78-17VA

a right where information should no longer be available, arguing if the flow of data remained unchecked this would inevitably impact an individual's right of privacy.[14]

An early Spanish advocate for the right to forget or 'erase' information, believing that the unearthing of distant information could impact privacy, was Professor O'Callaghan Munoz.[15] Writing in 1991, he had drawn parallels with the prominent US case, Melvin v Reid. This had bought about initial limited acceptance in the US to a form of a right to privacy.[16] The circumstances in this case concerned the use of the claimant's name in connection with a film about her past life which had impacted her by a 'direct invasion of her 'inalienable right… to pursue and obtain happiness.'[17] The case specifically claimed '[T]he right of privacy has been defined as the right to live one's life in seclusion, without being subjected to unwarranted and undesired publicity'. Examined later by Abril and Lipton there was general acceptance of a right to be forgotten within such premise, but this remained without any legal formalisation.[18] In short, it is the right 'to be let alone', an early forecast of the principles of a right to be forgotten and potentially of greater impact within concepts held in Europe than in the US. However, the early stance expressed in the case did bring about a tort in the US. [19]

Further arguments for such a right were continuing in Spain. By 1981, with the Council of Europe's creating the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data,[20] there was acknowledgement that the automatic

[14] Xavier O'Callaghan Munoz, *Libertad de Expresion Y sus Limites Honour Intimidad* , E IMagen 54 1991,Translated to 'Freedom of expression and its limits, honor, privacy and image' Editorials of Derecho Reunidas, EDERSA

[15] Noted in an article by Patricia Sánchez Abril, Jacqueline D. Lipton 'The Right to be Forgotten, Who decides what the world Forgets' Kentucky Law Journal Vol. 103: Iss. 3, Article 4. Available at: https://uknowledge.uky.edu/klj/vol103/iss3/4

[16] Melvin v Reid, Court of Appeal of California, Fourth District, Feb 28, 297 P. 91112 Cal. App. 285 ,297 p 91 (Cal. Ct. App. 1931).

[17] ibid p 290

[18] Patricia S. Abril & Eugenio Pizarro Moreno, *La Intimidad Europea Frente a la Privacidad Americana: Una Visidn Comparativa del Derecho al Ovido, Indret Revista Para El Analisisdel Derecho*, Jan. 2014, at 1, 25 Translated; *European privacy versus American privacy; A comparative view of the right to be forgotten* (translated by author). Available at http://www.indret.com/pdf/1031.pdf last accessed 18 Feb 2021

[19] US: Restatement (Second) of Torts 652D (1977)

[20] Council of Europe Convention No. 108 on Data Protection, Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.01.1981). Available at https://edps.europa.eu/data-protection/our-work/publications/legislation/council-europe-convention-no-108-data-protection_en

nature of how data could be accessed, or indeed restricted, was of increasing concern to users of the Internet. Consideration of the accessibility of potentially damaging, long neglected information was a slow process, despite the acceptance of the need for more than just data protection. The Audiencia Nacional, the Spanish court that heard the case, had a history of balancing constitutional rights,[21] so the potential conflict between freedom of expression and the right of privacy has already been considered with the courts having often found for privacy. This was particularly where time had rendered the particular information no longer relevant (or not of legitimate public concern). The Spanish Constitution makes provision for individual citizens to appeal to the Spanish Constitutional Court for protection against governmental acts that violate their 'fundamental rights or freedoms'.[22] In addition the Constitution had put in place a basis for what could be considered a constitutional understanding of the freedoms of expression and information. Whether this was in fact a liberal approach or not, it looked at promotion and recognition of full fundamental rights through the court, arguing that these were now contained in the Constitution.

In the Spanish public arena, privacy regulation had become one of the main debates, particularly with questions on the right to oblivion on the Internet. This needed to be balanced with the commercial use of users' data gathered by new practices and tools that were permitting access to personal information.[23] For many Spanish, the Internet was increasingly seen as the platform for all forms of communication. With this change from more traditional forums there were clearly new legal issues (such as the neutrality of the Internet),[24] but also existing key issues such as transparency, privacy, reputation, and freedom of expression.

Even though the debate was not usually conducted in terms of fundamental freedoms and independence, the fact that protection of privacy could interfere with the ability to post or

[21] Elisenda Casanas Adam, *The Constitutional Court of Spain From system balancer to Polarizing Centralist'*, in (eds) Nicholas Aroney, John Kincaid *Courts in Federal countries; Federalists or Unitarists*, (University of Toronto Press 2017) pp. 367-403 available at https://www.jstor.org/stable/10.3138/j.ctt1whm97c.16 Further, the Court has played a fundamental role in securing individual rights and liberties as part of a transition to a fully constitutional system, in particular by incorporating the case-law of the European Court of Human Rights, as well as other international human-rights treaties and decisions.

[22] Michael T Newton, Peter J. Donaghy*, Institutions of modern Spain: a political and economic guide. (*CUP *1997).*

[23] As recorded by Agencia Española de Protección de Datos (AEPD) in 2010

[24] See Christopher C Marsden, *Net Neutrality: Towards a Co Regulatory Solution* (Bloomsbury Academic 2010)

collate information on the Internet led to arguments that this would violate freedom of information in certain cases. This would potentially impact the independence of the media with the freedom to choose what is and what is not news. The case of the Times Newspaper Ltd (Nos 1 and 2) v The United Kingdom at the European Court of Human Rights (ECtHR) in 2008, although a case based on defamation, took the opportunity to debate the importance of the Internet to protect freedom of expression: 'the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally.' [25] Due to the sensitive issues related to the free flow of information on the Internet, the Audiencia Nacional Agencia Española de Protección de Datos (AEPD), the Spanish Data Protection Authority, and other national Data Protection Agencies were arguably the main players regulating privacy issues with their rules and recommendations. For instance, the AEPD, while maintaining a co-operative attitude with the telecommunication companies,[26] has stated that the main ISPs have repeatedly 'overstepped the line of respect for privacy' and that service providers may have exceeded the extent that protection is provided for within the concepts of freedom of expression and information. Even if privacy regulation could be improved, it was arguable whether this would take place due to the importance that economies were placing on the innovation and growth bought by new technology companies. An interview with the public prosecutor specializing in cybercrimes by Marina Mantini, conducted in Madrid in October 2011, confirmed that over recent years the AEPD had increased its autonomy and power in recognition of the new needs, leading to disagreements with the more traditional courts.[27]

As indicated before, Spain had not been backward in rising to the challenge and as early as 2007 the Spanish AEPD had issued a paper on the need to resist the activities of search engines in order to protect privacy. [28] Coincidentally, the early steps in the case by Senor

[25] The Times Newspaper Ltd (Nos 1 and 2) v The United Kingdom, EctHR 10 March 2009 Application nos 3002/03 and 23676/03; [2009] EMLR 14 s.27

[26] E.g both Tuenti and Facebook, as large representatives of social media companies, had been working with it over development of their privacy policies

[27] This interview was conducted through MEDIADEM a European research project which seeks to understand and explain the factors that promote or conversely prevent the development of policies supporting free and independent media. Available at https://www.eliamep.gr/wp-content/uploads/2012/02/Spain.pdf last accessed 25 Feb 2021

[28] Statement on Internet Search Engines, AEPD Madrid I Dec 2007 Director of AEPD to constitutional Commission of Congress Madrid, 28 Nov 2007

González had begun in 2008, reflecting growing interest in controlling information relating to a person contributing to the debates outlined in Chapter 3. With an increasing level of complaints meeting resistance from Google to remove disputed links, Google argued that where there were links to legally held information, there should not be any grounds for removal of such search results. [29]

This debate was not unique to Spain. Early deliberations in other countries, such as Germany, had also occurred; these concerned publication of what was considered 'private' information, albeit in initially limited circumstances, relating to agricultural aid reference. Here an application had been made to the CJEU[30] to determine if the publication contravened EU privacy laws.[31] As a result, the CJEU confirmed a balancing act was required between the objectives of the law, i.e., those relating to the provision of aid, and those relating to the protection of personal data as contained in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the Charter).[32] This publication of information had not been ordered, therefore the action was considered to be a violation of the privacy rights.

In Spain there had been early forages into clearer notions of 'forgetting' information concerning an individual, rather than preventing access. In particular this related to actions relating to those held liable for acts committed under the Franco dictatorship and regime. The concept of '*derecho al olvido*'[33] created an amnesty, where those guilty of such crimes were not prosecuted, gradually providing a rehabilitation culture for Spanish citizens. This gave acceptance that their future would not be hindered by former activities, not limited to crimes but also other actions as well. Similarly, Italy had also developed a concept referred to in similar terms as '*el-diritto all'oblio*'. This however, is often considered as a right not to remain indefinitely exposed to the additional damage that a repeated publication may cause, particularly media commentaries. These could damage the reputation of an individual. Again

[29] For example the Alfaques case where a business case for removal of negative news report impacting the directors was rejected (SAP Oct 2 2012) There was also an unreported case of Hugo Guidotti where links to a malpractice lawsuit were also rejected despite the claimant having been successful in the lawsuit.
[30] Subsequently replaced by the Court of Justice of the European Union
[31] Joined cases C-92/09 & C-93/09 Volker and Markus Schecke GbR v Land Hessen [2010] ECR 1 -11063 9
[32] The Charter of Fundamental Rights of the European Union Dec 2000 OJ C 326
[33] This wording in Spanish actually translates literally to a right to be forgotten.

this idea focused on a person having paid dues to society, not being faced with constant reminders of past, potentially criminal, events impacting not only privacy but also reputation. This was shown in a case where disclosure of past crimes was bought before the court and it was held that, as the sentence for the crime had been completed, continuing to publish details caused damage to reputation with the offence of defamation being upheld. [34]

Within such a background, recognition of a right for the free development of the personality of an individual, had been used to establish its own version of the right to be forgotten using principles of limitation with regard to the collection of data, restricting the purpose of the collection, and ensuring the quality of the data.[35] Although laying a pathway to the challenges of the right to be forgotten, the first Spanish case on whether there was such a right was unsuccessful. Abril and Lipton argue that the ability to establish a right to be forgotten had been slow moving in 'a slow clumsy yet daring fashion.'[36] In looking at how actions against Google were being contemplated in the years before the action by Senor González, they report claims against both the Spanish Constitutional Court and a newspaper in the case *Diario El Pais*. In such case,[37] it was argued that references made to a conviction for forgery were causing harm to the claimant's professional reputation. The claims, together with a claim for breach of privacy, were however overturned. The court held that upholding freedom of expression was necessary to ensure that the public were made aware of the facts. It was made clear that the information was lawfully published online, a factor that would also be relevant in the Google Spain case. Such an arrangement was clearly of public concern and, accordingly, the Spanish Court had a duty to report such cases so the public could be made aware of the facts. Despite this the claimant continued with a further action against Google increasing the number of actions being taken against it.[38] There were also other cases bought by individuals to the AEPD and in over 90 cases Google was ordered to remove links to online

[34] Supreme Court of Italy, case no 3679/1998

[35] Spanish Constitution 1978 as modified 1992. Article 10(1) The dignity of the person, the inviolable rights which are inherent, the free development of the personality, the respect for the law and for the rights of others are the foundation of political order and social peace. Available at: http://www.parliament.am/library/sahmanadrutyunnor/ispania.pdf

[36] Patricia Sánchez Abril, Jacqueline D Lipton, "The Right to be Forgotten: Who Decides What the World Forgets?" (2014) Kentucky Law Journal: Vol. 103 Iss. 3 p Art 4 p 367 https://uknowledge.uky.edu/klj/vol103/iss3/4/ last accessed 20 Feb 2021

[37] SAN, AN 2370, May 12 2011

[38] n 36 Patricia Sánchez Abril, Jacqueline D Lipton, pp 373, 374

news articles. The AEPD stated its clear belief in the existence of a right for citizens with no public interest in them, to be able to ensure that private information made public remains private.[39]

The Spanish Court finding that links to such personal information were in breach of the right of privacy also began ordering Google to remove the links. This response could be considered as actions under an attempted right to be forgotten sufficient to provide limited protection without recourse to a defined right. There was no issue in the court finding such remedies for individuals who were not public figures, relying in addition on the ability of a data subject to withdraw consent.[40] These claims were often in relation to a form of official information i.e., the Spanish Official Gazette, with published information made available usually as a result of an appropriate court order. Clearly, in these instances there was no question as to illegality or inaccuracy of the information which might have ensured correction of the information. This stream of activity was not welcomed by Google which was beginning to feel the heat of opposition to its business activities within the EU. Indeed, it was now being specifically investigated within various forums by the EC despite its proclaimed objectives as being the free flow and accessibility of data to facilitate the use of technology.[41]

Arguments as to the activities of search engines and how they could be construed included the notion formulated by Markou [42] that search engines are only 'blind indexes' of what exists on the web. It is therefore not acceptable for third parties to dictate the content then displayed. Interference should only be tolerated in what she calls 'extreme circumstances' i.e., theft, sexually explicit content, murder. However, the challenge faced by Google at the

[39] Statement on Internet Search Engines, AEPD Madrid, I Dec 2007 Director of AEPD to Constitutional Commission of Congress, Madrid. It was stated activities by a search engine 'could be legitimate at source but its universal and secular conservation on the Internet may be disproportionate'

[40] The Data Protection Act (Organic Law 15/1999 on the protection of personal data) Translation of Article 6.3; 3. 'The consent to which the Article refers may be revoked when there are justified grounds for doing so and the revocation does not have retroactive effect' available at http://apdcat.gencat.cat/web/.content/01-autoritat/normativa/documentos/960.pdf last accessed 12 May 2020

[41] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) ch 1 p 8
Lynskey argues that there were dual objectives in the regime set up with the Data Protection Directive 1995: the facilitation of the free flow of personal data between the member states of the EU whilst ensuring the protection of fundamental rights with the emphasis on privacy.

[42] Christiana Markou, '*The Right to be Forgotten': Ten Reasons why it should be forgotten*' in (eds) Serge Gutwirth, Ronald Leenes, Paul de Hert, *Reforming European Data Protection Law* (Springer 2015)

time of the case was that awareness of its activities meant it was beginning to be understood that Google, in its activities as a search engine, was no longer viewed as performing the function of an information depository, for example a library. Rather it was functioning as an ever-expanding data collector, as yet unrecognized as such by the relevant authorities, whilst using such material and variants of data for commercial purposes. Such activities were also subject to the wider intention to update data protection. Slowly the reality of Google as a commercial organization, not a charity or quasi government task force, was being fully appreciated.[43] Within this came realization that without any real acknowledgment or permissions Google was occupying a unique position in a futuristic new environment where many failed to understand its motivation or indeed its actions. Autocomplete functions also skewered perceptions of such activities. [44]

A better understanding of such functions could potentially have been used to argue the level attributed to any editorial or journalistic input by the search engine, or indeed whether any such input existed. This point was examined in various cases considered by Brock in his review of Google's position. [45] It was a small next step for commentators to then perceive Google as some form of technical monster taking over an element of humanity.[46]

As noted, the case of Google Spain did not come out of the blue nor were discussions concerning the right to be forgotten confined to Spain. For example, CNIL (the French Data Protection Authority) had widely reported an increase in complaints made to it between 2010 and 2014 which asked for information to be taken down or no longer made available. It seemed that during this period there was the beginning of much wider awareness that the price of readily accessible information was not only a loss of privacy but increasingly inadequate control of data.[47] The impact was greater with the recognition that a private

[43] This is further discussed in Chapter 6 where the monopolistic position occupied by the various internet giants is considered more fully

[44] see n 10 Stavroula Karapapa, Maurizio Borghi, 'Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm'

[45] George Brock, *The right to be forgotten- Privacy and Media in the Digital Age*, (IB Tauris, 2016) P29

[46] This may be considered to be shown in the portrayal of the organization in 'The Circle', by Dave Eggers (Penguin 2014) a work of fiction later made into a film, which is widely believed to convey the culture of Google and its influences and long term aims.

[47] Meg Leta Jones, *Ctrl+Z, The Right to be Forgotten*, (New York University Press 2016) ch 3 p 85, Here the author explains the need for increased data protection can be shown by the difficulties of 'calculating risk,

individual had potentially fewer resources in which to carry out such control. Spain had risen to the challenge potentially a year before the initial declared interest by the EU in updating data protection laws.[48]

It was also apparent that the EU was attempting to rein in the Internet giants, including an examination of Google and the potential abuse of the right to privacy during its activities, as well as highlighting wider concerns over data protection.[49] This was reflective of a new approach to the liability of ISPs, particularly the position of search engines which will be explored later in Chapter 6. Concern over the accessibility and potential lack of data control was highly likely to impact the free flow of such data on which the various internet giants had come to rely. This was reflected in responses by Google in particular concerned as to the future of its commercial activities. Google was increasingly vocal in its disagreement with any sanctions, publishing a statement as reported in the New York Times,[50] claiming in effect that the requirement for internet search engines to ignore specific data 'would have a profound chilling effect on free expression without protecting people's privacy'.

It added an interesting angle in arguing that this restriction would also be considered to be harmful to the 'objectivity of the Internet.' Any ideas of a right to be forgotten would only be seen then as a fetter on freedom of expression and public interest. Rosen[51] saw that this

exercising choice and initiating control over so much personal data, resulting in a view that the right to be forgotten is an effective way of procuring participation in data protection regimes

[48] European Commission, 'European Commission sets Out Strategy to Strengthen EU Data Protection Rules', press release IP/10/1462 Nov 4 2010

[49] Jan 24, 2012: Google Inc. stated it would be providing a new privacy policy to replace its former 70 polices, applicable to all its services and products. By Feb 2, 2012 the European Data Protection Authorities (WP29) asked Google Inc. to postpone this after having started to analyse the content. Google, however, did not agree and the WP29 decided to carry out a detailed analysis of the policy, led by CNIL the French Data Protection Authority. Even after a further request to postpone the policy Google produced it with effect from October 2012. This led to the Article 29 Working Party (WP29) & 27 European nations notifying Google of several provisions that were in violation of EU data protection regulation. So, by February 26, 2013, with Google having not put in place the WP29's recommendations, the WP29 & 27 European data protection authorities decided to initiate national investigation against Google Inc. opening the investigation in April 2, 2013, and leading to a €900,000 penalty to Google Inc. by December.

[50] available at https://www.nytimes.com/2011/08/10/world/europe/10spain.html last accessed 20 March 2019. This article reported Google's reaction to the order by the Spanish Government to remove links to information concerning 90 people who had made claims with the Spanish Data Protection Authority which Google had not complied with.

[51] Jeffrey Rosen, 'Symposium Issue; The Right To Be Forgotten,' (2012) 64 Stanford Law Review Online, Vol. 64 p 88 available at
https://review.law.stanford.edu/wp-content/uploads/sites/3/2012/02/64-SLRO-88.pdf

potential restriction was worse in that it changed the nature of the function of ISPs by, for example, placing a burden on Facebook to prove to an EC authority that, 'my friend's publication of my embarrassing picture is legitimate journalistic or literacy or artistic exercise.' He further argued this could turn such entities into 'censor-in-chief for the European Union rather than a neutral platform'.

Various commentators have reported on these early cases which, although based primarily on similar circumstances to those of the Google Spain case, contained diverse scenarios evoking the growing call for a 'right to be forgotten.'[52] It was also noted that this was an opportunity for a 'transatlantic clash' with the US where freedom of expression was paramount and would take precedence over privacy rights.[53] However, the importance of the role that the various agencies of Spain would take in the development of the right to be forgotten was heightened by such representatives' promotion of the need for such protection.[54]

Despite growing acceptance of the need for such a remedy[55] no clarity as to the form of right had yet been advanced other than through debate on the proposed GDPR regulation.[56] A speech given by Artemi Rallo Lombarte, former head of Spanish Data Protection Agency[57] at Oxford University in 2012,[58] focused on the idea of a formal right to be forgotten, thus echoing

[52] see n45 George Brock, see also Artemi Rallo *The Right to be Forgotten on the Internet: Google v Spain,* Electronic (Privacy Information Center 2018)

[53] Muge Fazlioglu. 'Forget me not, the clash of the right to be forgotten and freedom of expression on the Internet' (2013) International Data Privacy Law, Vol 3, Iss 3, pp 149–157, available at https://doi.org/10.1093/idpl/ipt010

[54] See Artemi Rallo, *The Right to be Forgotten on the Internet: Google v Spain,* Electronic (Privacy Information Center 2018) ch II, 47 Here Rallo details the beginning of actions being taken by the Spanish Data Protection Agency (AEPD). In 2007 the first action was taken to order Google to remove search results by the AEPD (application no TD/463/2007)

[55] As was accepted by the Informal Justice and Home Affairs Council, Dublin, 18 January 2013 where Viviane Reding spoke of the importance of the right to be forgotten as an effective guarantee for the control of one's data by way of a response to such technology that provides for the unlimited levels of retention accessibility and exchange of data.

[56] Various forums were taking place with debates as to the challenges being presented *"You can't have an EU right to be forgotten and a Member States right to remember"* Professor Gerrit Hornung, Passau University, commenting on the problem that fragmentation may bring if certain legal powers are not transferred to a central body. See https://dataprotector.blogspot.com/2013/01/

[57] Director of the Agencia Española de Protección de Datos between 2007 and 2011

[58] Artemi Rallo Lombarte, 'The Origins and Importance of the Right to be forgotten' available at https://podcasts.ox.ac.uk/origins-and-importance-right-be-forgotten last accessed 14 May 2018. The talk was the keynote address of the OxPILS Conference 'The 'Right to be Forgotten' and Beyond' held on 12 June 2012

concerns that although the EC had communicated a comprehensive approach to data protection, new technologies and specifically the Internet, had increased the challenges and indeed the necessity of developing and enhancing data control for its citizens. Although responsible for raising initial discussions around the right to be forgotten that would be contained in Article 17 of the GDPR, Rallo was concerned that this proposal would only relate to the erasure of data. This would not bring the debate to an end as it would not fully determine the extent and the scope of the right to be forgotten, rather it would bring initial awareness that the right may provide wider protection in respect of dignity and reputation.

It was clear that trying to use existing legislation for claims under a purported right to be forgotten was proving a challenge and it was imperative that more guidance from the CJEU should be given. In particular, the extent of the role of the Internet search engine, a concept unheard of at the time that the DPD was put in place, needed clear and appropriate clarification with stronger boundaries and regulation. A search engine's responsibilities are not only as a data controller — if indeed it was to be categorized as one — but also as a potential decision maker when considering if and when to remove links to search results containing information that was perhaps no longer relevant or in some form prejudicial, had become a burning issue.

The complexities[59] that up to 2014 had surrounded such ISPs could be summed up in the words of Brock[60] considering if such entities were 'utilities under private ownership but supplying basic needs on such a scale that they require regulations as gas, electricity or telephone companies once were?' He also questioned,

'Are they equivalent because of their importance to all forms of democratic social and commercial communication to a public service broadcaster or do they require more regulation where such an organization might be given decision making authority in respect of

[59] There were ambiguities under the E commerce Directive as to the level of protection provided which would apply to search engines. This was to be applied to entities with no knowledge of content hoisted with them but left questions with regard to specific major players such as Google and Facebook.
[60] n45 George Brock, p 28.

a potential human right, simply the innovative leaders of a modern phenomenon, information capitalism.'[61]

The case of Google Spain was to bring about the first full discussion as to the responsibilities of entities, such as search engines, evaluate their liability and meaningfully consider where a potential misuse of personal data could take place. It would consider the effect on privacy and, ultimately, how a person could be viewed in society, determining the control available over such information and the ability to control how it is used as well as accessibility.

4.2.2 The initial case

In 2007 the AEPD had already published a paper outlining concerns with regard to the issues arising from search engine activities.[62] This had followed the lead from the Italian data commissioner that the unprecedented arena of the Internet was providing a violation of its legal right of oblivion.[63] The increase in concern was marked by the further claims where Google had refused to remove links to information as requested by the AEPD in 2008.[64] By 2010 the Spanish Data Protection Director had ordered Google Spain and Google Inc. to remove the links to information concerning Senor González , leading to an appeal by Google to the Audencia Nacional (the Spanish High Court) against the finding.[65] The failure by the AEPD to enforce its findings of a misuse of personal data therefore created an opportunity to get guidance on this increasingly contentious issue. Unsurprisingly the facts of the case were not dissimilar to those cases already determined, although the links in this case did not refer to a criminal conviction but to civil court proceedings.[66] Senor González's immediate concern

[61] Manuel Castells cited by Emily Laidlaw in 'Private Power, Public Interest: An Examination of Search Engine Accountability '(2009). International Journal of Law and Information Technology, Vol. 17, Issue 1, 121 available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1357967 last accessed 20 Feb 2020

[62] see n39, Statement on Internet Search Engines, AEPD Madrid

[63] Pere Simon Castellano, 'The Right to be Forgotten under European Law, a Constitutional Debate,' (2012) Lex Electronica, Vol 16.1 2012 p.4 Castellano referred to the *Garante reviweig*, Art 11 of its data protection rights to express concern that data quality is not preserved when personal data no longer meets the original purpose that it was obtained for.

[64] Meg Leta Jones, *Ctrl+Z, The Right to be Forgotten*, (New York University Press 2016) ch 2 ,40. Here the AEPD was argued to have 'ardently' recognised and extended this right to be forgotten using Art 10 of the Spanish Constitution which provided a right to the free development of personality to base this on.

[65] It was accepted that the newspaper that had originally published the bankruptcy information was not liable as it had made the lawful publication in accordance with the court's order.

[66] Senor González had originally requested that the newspaper La Vanguardia remove references to his previous insolvency which was refused on the basis that the information was a publication that had been

was that a search against his name revealed links to a court order relating to his bankruptcy. This had a detrimental effect on his ability to continue to work but, most significantly, on how he was perceived within the community, namely his reputation. Legitimate facts revealed through a search engine's results clearly impacted not just on the right of Senor Gonzalez to earn a living but on his private and family life. The result was that he was and would be seen as a different person to the person he wanted portrayed through the Internet for as long as there was a digital memory of his past.

4.2.3 The application to the CJEU

The Spanish Court ultimately indicated that the issue was of significant importance with particular emphasis on defining Google's obligations to the public. The Spanish Audencia Nacional, in determining the main issues around the availability of information, understood that some of them, particularly concerning the position of search engines, could only be dealt with by the CJEU.[67] This would enable proper interpretation of the relevant terms of the Data Protection Directive (DPD) and create the necessary precedent promoting legal consistency with the EU.[68] Specific questions, initially nine in total, were raised for the CJEU to consider. Three concentrated on the major areas within Senor González' claim. The CJEU was requested to determine firstly, the territorial scope of the DPD, secondly, whether a search engine is an entity regulated by the DPD, i.e., a data controller, and thirdly, whether a right to request removal of links to information in search results published by the search engine existed. Despite the background to the case arising from demands for a form of the right of oblivion, the idea of creating a right to be forgotten was not considered part of the aspirations of the referrals as such i.e., no direct request as to whether this existed.

ordered by the Ministry of Labour and Social Affairs. On refusal he then complained to the AEPD which upheld the complaint against Google only as the publication by the newspaper was legally justified.

[67] The questions referred to were firstly whether the activities of a search engine, here Google, bought the search engine within the territorial scope of the DPD, secondly, if the activities of the search engine in collecting, caching, indexing, and retrieving data constituted 'processing' under the Directive the search controller would be the data controller, and thirdly, if so could the individual invoke rights under the Directive to seek erasure or object to processing to have the data removed. The question was also, could individuals ask search engines to suppress information published legally.

[68] The Data Protection Directive, 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31

However, the core for the referral of the case was to deal with the emergence of cases involving specific issues concerning the impact of digital memory, not just on privacy but on dignity and reputation. This also evoked the challenges of decision making with regard to such fundamental rights being carried out by the newly created ISPs. The accessibility and longevity of information on the Internet illustrated the EU's newly developing stance in looking at ISPs not as 'journalists' but as 'publishers' with resultant additional levels of responsibilities. The case of Lindquist formed the basis of this direction. [69] The growth of discontent with the availability of personal information through the results of search engines, and also the increasing use of algorithms, had led to more unease among data subjects as to the impact. Although the suggestion of any editorial or journalistic input could be negated by a clearer understanding of autocomplete functions, as was examined in various cases, this did not seem to be sufficient for ISPs to be considered to be without any form of control over the information.[70] Brock, in analyzing the change in direction, references an earlier French case in which links were made of 'rapist' or 'Satanist' and attached to the claimant's name. The court argued that algorithms were made by human 'thought' and Google, in order to defend their position, would need to prove that autocomplete statements were not done by the company.[71] In the case of Bettina Wulff (previously referred to in Chapter 3) several links to

[69] Case C-101/01 Bodil Lindquist v *Aklagarkammaren i Jonkoping*, [2003] ECLI:EU:C:2003:596
This was one of the first opportunities for the EU court to consider the new development relating to data being placed and accessed through the Internet and not only whether this constituted processing but whether there could be 'free 'movement of such data. By order of 23 February 2001, received at the Court on 1 March 2001, the *Göta hovrätt* (Göta Court of Appeal) referred to the Court for a preliminary ruling under Article 234 EC seven questions concerning inter alia the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)
http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=en The ruling stated 1. The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes 'the processing of personal data wholly or partly by automatic means' within the meaning of Article 3(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.'

[70] n 45 Whilst intermediaries such as search engines wanted to limit liability for autocomplete functions seeking to establish that this was a pure technological function, Brock talks of 'words and phrases popping up' but noted this is not done without human input. He argues at what level does this become editorial input or feature a level of control over the content made available. Similarly Karapapa and Borghi 's view is that the autocomplete function 'introduces during the search process an additional source of informative content of which the search engine is solely responsible' seen 10 p 274

[71] see n45 George Brock, 28, 29 Here he refers other issues reported in France as well as Germany on similar concerns. CNIL had reported 'pent up' demand during the years 2010 to 2012 with the desire to remove or at least obscure information online.

her name of terms such as 'prostitute' or 'escort', resulted in a claim for defamation against Google, despite Google's claim that the connections were made by autocomplete.[72] This also raised concerns both in Europe and the US over the level of protection needed in such instances.[73] The impact of such auto functions on the rights of an individual focused attention on the effect on a person's dignity by specifically subjecting them to an ever-lasting digital image. The insight of the CJEU was sought to provide clarity and direction on such issues.

4.2.4 Questions raised to the CJEU

The initial focus was on the challenging question of jurisdiction, of increasing important where data could be accessed globally as well as indefinitely. The Court confirmed that as Google, through its Spanish company, carried out commercial activities within Spain, it would be subject to existing EU data protection laws. In considering the territorial scope of the DPD the words 'through effective and real activity through stable arrangements'[74] were examined to determine if Google could in fact be considered established in the relevant member state so as to fall within the provisions of the DPD and be bound by its terms. It was apparent that Google Inc., although incorporated in Delaware, had formed local subsidiaries under appropriate national laws which provided incidental economic activities within such countries which, it could be argued, be viewed to be carrying out the majority of Google's activities within that territory. This position was critically viewed as ambitious territory to explore.[75] However, in the CJEU's view, any finding other than that resulting from broad territorial scope would have compromised the intent of the DPD and led to weaker protection for EU nationals being put in place.[76] In the opinion of many commentators, including David Lindsay, this aspect of the Court's decision had 'significant implications for trans-border internet communications especially as it relieves data privacy authorities and courts of the need to

[72] In the case of Bettina Wulff despite several cease -and -desist orders Google refused to take down the links and filed a defamation suit at the Hamburg court. Google defended its position saying the linking was as a result of algorithms which they could not be held responsible for. The case ultimately settled out of court, see https://www.bbc.co.uk/news/technology-19542938 last accessed 20 Feb 2021

[73] see also "Germany's Former First Lady Sues Google For Defamation Over Autocomplete Suggestions". *TechCrunch. 2012*.available at https://techcrunch.com/2012/09/07/germanys-former-first-lady-sues-google-for-defamation-over-autocomplete-suggestions/?guccounter=1 Last accessed 20 Feb 2021

[74] n68 The Data Protection Directive 1995, Preamble, para 19

[75] Google had relied on Opinion1/2008 On responsibilities of data protection for search engines which differentiated between a webmaster degree of responsibility (i.e .for published content) or that of a search engine who were regarded solely as intermediaries

[76] Google Spain, para 17

determine the physical location of data processing,'[77] meaning a much wider application of data subject protection. It did indeed highlight the difficulties faced in restricting access to personal data where the data subject was anxious not only to prevent the information being available at a local level but also on a global one, increasing the potential damage to them. The prospective impact of information not only being available and accessible forever, but also globally, was a major concern.

Once it was determined that Google was caught by the terms of the DPD this interpretation then directly led to the establishment of Google, a search engine, as a data controller — potentially a more controversial issue than even the right to be forgotten, but one firmly in line with the approach developing towards Google's activities within the EU.[78]

The Court was then asked to consider the questions directly relating to the so called 'right to be forgotten' initially focusing on the application of Art 12 (b) and Art 14 (a) of the DPD to assess if a claimant could request removal of links lawfully processed. With the CJEU clearly acknowledging the need to protect the 'fundamental' right of data protection, it was then called upon to consider Articles 7 and 8 of the Charter[79] and the balancing of competing rights to establish if the process was in breach of an individual's right to a private life.

4.3 The Advocate General's contribution

4.3.1 The opinion of the Advocate General (the AG)

The response of the AG, having been asked to review and determine the case as is customary practice where there is a significant referral to the court,[80] summarized the concerns. These

[77] David Lindsay, 'The 'Right to be Forgotten' by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling' [2014] 6(2) Journal of Media Law 159-179 1 Dec 2014, p4

[78] There seemed to be an increasing appetite to challenge Google's market activities with a growth in referrals for anti-trust activities see https://www.theguardian.com/technology/2015/apr/15/google-faces-antitrust-action-from-eu-competition-watchdog

[79] Charter of Fundamental Rights of the European Union 2012/C 326/02 available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT

[80] The mechanism within the EU provides for the Advocate General (the 'AG') to consider any issues considered to be of substantive importance which was unitized in this case. With a role created under Article 222 of the Treaty of Nice the AG acts with complete impartiality and independence making in open court reasoned submissions on specific cases based on law and fact. Article 22 provides that AGs are only required to give their opinion on a case if the CJEU believes that the particular case raises a new point of law and although therefore

were not only with regard to the challenge of finding Google, a search engine, to be a data controller, but to the ability for an individual to manipulate information to the detriment of freedom of expression. [81] In particular, if this right to request the removal of information was granted, how would it then sit within the need for the free flow of data and the ability of the Internet to freely provide increasingly accessible information purportedly for the benefit of all. The view that this availability was not only required but justified was formed in the growing belief that such wide access to information was in the public interest. This now formed part of the changing needs of society to the point where the ability, or even the right, to access such data might be considered the equivalent of a utility service.

It was in light of this viewpoint that the AG found, with a skilled and considered opinion[82], that met with much approval not just by Google but by commentators generally, that a search engine could only carry out an intermediary role and should not be considered to exercise the level of control as would be required of a data controller whilst it only provided such an ancillary function.[83]

This seemed to be in contradiction to the debate on the need for an ability to control data which impacted how one was portrayed, largely through the Internet. In addition, it was claimed that the AG was taking the side of Google, potentially putting commercial interests before the ability of individuals to protect their reputation. However, respected commentators, such as Orla Lynskey, when analyzing the opinion saw it as vastly pragmatic

---

of influence but the CJEU does not necessarily follow the AG's opinion. The opinion is delivered to the judges for them to discuss before giving their judgment. In figures provided the majority of cases ie 80% of cases in 2010, followed the AG's opinion. There are exceptions which have generally been high profile cases likely to be controversial (eg the ECJ notably did not follow AG Bot's opinion in *Kadi II*).

[81] see David Lindsay, 'The 'Right to be Forgotten' by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling' [2014] 6(2) Journal of Media Law 159-179 1 Dec 2014, p 175, also George Brock, *The right to be forgotten- Privacy and Media in the Digital Age*, (IB Tauris 2016) 39,40

[82] - Case C-131/12 Google Spain Sl Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González [2013] ECLI:EU:C:2013:424; Opinion of Advocate General Jääskinen

[83] ibid Opinion of Advocate General Jääskinen - see VIII , para 138 (2) '[H}owever, the internet search engine service provider cannot be considered as 'controller' of the processing of such personal data in the sense of Article 2(d) of Directive 95/46, with the exception of the contents of the index of its search engine, provided that the service provider does not index or archive personal data against the instructions or requests of the publisher of the web page.'

meeting the task of keeping the data protection rules within 'sensible' limits.[84] Overall, despite the growth in the use of data in circumstances unimaginable at the time of creation of the DPD,[85] the AG held that the current data protection rules were not able to provide for a person to restrict or stop the distribution of personal information in particular circumstances, specifically search engine results, even if that person considered it harmful or detrimental generally to their privacy and other rights.[86] With increasing concern as to intrusion into privacy and to the impact of digital memory on rights of privacy, dignity, and reputation, it was clear the approach by the AG was not generally considered to be representative of current views. Kelly and Satola argued that the more data protection rights were recognised, the greater the impact would be on search engines.[87] The AG's opinion therefore seemed to be out of line in not safeguarding individuals in this environment.

The AG was also clearly aware that the new regulation had not yet been implemented and its form was still being fiercely debated. Accordingly, in this instance he was being required to apply an existing directive created at a time prior even to the invention of the Internet and subsequent processing of personal data to provide what he referred to as 'unprecedentedly wide range of new factual situations due to technological developments'.[88] It seemed that ultimately his intention was to follow the moderate approach already determined in the Lindquist case.[89]

---

[84] Orla Lynskey 'Time to Forget the 'Right to be Forgotten'? Advocate General Jaaskinen's opinion in C-131/12 Google Spain v AEPD,' European Law Blog, 3 July 2013 http://europeanlawblog.eu/2013/07/03/time-to-forget-the-right-to-be-forgotten-advocate-general-jaaskinens-opinion-in-c-13112-google-spain-v-aepd/ last accessed 7 March 2019

[85] The DPD was implemented in 1995

[86] n 82, In addition, the AG determined that whether there was a need to consider if such information was already in the public domain even if the search engine was considered a data processor, then it could not comply with obligations under Article 6.2 of the Data Protection Directive so would not be bound by any potential right to be forgotten.

[87] Michael J Kelly, David Satola, 'The Right to Be Forgotten' (2017) University of Illinois Law Review, Vol. 1, May 9, 2017 Available at SSRN: https://ssrn.com/abstract=2965685

[88] Case C-131/12 Google Spain Sl Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González [2013] EU:C:2013:424; Opinion of Advocate General Jääskinen para 30

[89] C-101/01 Criminal Proceedings against Bodil Lindquist [2003] ECLI:EU:C:2003:596, Reference to the Court under Article 234 EC by the Göta hovrätt (Sweden) for a preliminary ruling in the criminal proceedings before that court against Bodil Lindqvist, Para 86 'In that context, fundamental rights have a particular importance, as demonstrated by the case in the main proceedings, in which, in essence, Mrs Lindqvist's freedom of expression in her work preparing people for Communion and her freedom to carry out activities contributing to religious life have to be weighed against the protection of the private life of the individuals about whom Mrs Lindqvist has placed data on her internet site.'

To do so the AG first approached the question of territoriality. He rejected any interpretation in favour of search engine's activities being considered on a broader basis; he considered this as being too far reaching in scope.[90] In the AG's view, the functions carried out by Google's search engine activities could be considered to be 'processing' with an automated function, no direct human intervention, and without recognition of whether data is 'personal' or 'non personal. Due to the peculiar nature of the search functions, he found that Google could not be considered a data controller and was not caught by the provisions of the DPD. In the view of Lynskey, [91] the opinion included the insertion of a 'subjective mental element' which, by adding a form of intervention or awareness required in processing, could be detrimental to providing remedies within both data protection and privacy.

The AG was also vocal in his view that any other interpretation would result in too great a widening of the scope of the DPD. Drafted in the early 1990s, the ability for an organization to perform such functions would have been difficult to envisage. To bring such new services within the scope of existing laws from newly created organizations was, he believed, outside the scope of the function of the court and lay with the provider of regulations. Within its arguments Google had claimed that even if it did 'process' data as part of its search engine functions, it made no distinction between personal and non-personal data arriving in a piecemeal and mechanical manner. The AG accepted that the role carried out by Google was that of a passive intermediary having no actual relationship with the personal data nor the sources from which it was collated, or indeed the content. In Lynskey's view the AG included a 'knowledge' or 'intention' criterion, which she believes was previously unheard of in EU data protection law. The AG could be considered to be applying this doctrine to an understanding of the actual function of a 'data controller', narrowing its scope. This was, however, very much against the recognition that individual rights were being compromised by such automatic processing.

[90] n 82 In the AG's Opinion the approach was to examine the wording of Art 4 (1) of the Directive as to how a single economic unit in an EU state could be bought to compliance under EU laws (para 64 -66)

[91] Orla Lynskey 'Time to Forget the 'Right to be Forgotten'? Advocate General Jaaskinen's opinion in C-131/12 Google Spain v AEPD', European Law Blog ,3 July 2013 http://europeanlawblog.eu/2013/07/03/time-to-forget-the-right-to-be-forgotten-advocate-general-jaaskinens-opinion-in-c-13112-google-spain-v-aepd/ last accessed 7 March 2019

In order to support his finding that Google should not be a data controller in this context, the AG had made a number of observations. First of all, he raised the argument that to interpret the notion in a literal manner or in a teleological manner, as proposed by several parties before the Court, would not take into account that the DPD was drafted pre-Internet and would give rise to what the AG viewed as incongruous results. As a search engine had not existed as an entity or function at such time, it could be argued that such could not be included within any interpretation of the DPD as this would entail considering within its confines totally unthought of processes and outcomes. There was also concern that in interpreting the DPD in the light of new technological initiatives any concepts of proportionality should be taken into account, together with the stated objectives.

Finally, the AG's observations supporting his claim that Google could not be considered a data controller also highlighted the view of Google as a passive intermediary with no actual relationship with the providers or the contents of third-party web pages. In looking particularly at recital 47 of the DPD with Articles 12-14 of the E-Commerce Directive,[92] he was able to confirm his opinion, that such use of technology with regard to data sources is not sufficient to be termed as 'control' over the contents of the search results. He offered this in support of his proposition that facilitating the technical transmission of content does not create control over its content.

The AG's limited approach in interpreting the directive and his refusal to provide an expansive interpretation of any concepts within it posed an argument that would be continued in future years in relation to the new activities on the Internet. His view was that no right to be forgotten could exist under the DPD because search engines were not expected to check the retention of information nor any subsequent impact on data subjects' rights. Reference to Article 8 of the Charter and its guarantees of protection of personal data,[93] however,

92 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 - 0016

93 n82 The AG's Opinion in para 112/113 referred to the right of protection for personal data under Article 8 of the Charter stating; 'in my opinion this fundamental right, being a re-instatement of the European Union and Council of Europe acquis in this field emphasizes the importance of personal data, but it does not as such add many significant new elements to the interpretation of the Directive'

confirmed that such rights existed but, in the AG's view, they could not challenge the DPD nor bring new elements to it. The impact of the creation of a right to be forgotten by maintaining the opposing rights of freedom of expression and the public's right to receive information with privacy was argued to be placing too great a function onto a search engine, one beyond its capabilities. This also upheld many of the views offered through the Article 29 Working Party,[94] where if a search engine acts purely as an intermediary it should not be the principal controller with regard to the content related processing of personal data.

The challenge to the AG's opinion, subsequently followed by the Court's decision, is that despite the approach which would make applications of the right to be forgotten easier, the arguments put forward by him did not lead to any greater certainty. By proposing the restricting of the application to member states this does not recognize the reality of EU treaties being more widely applied through such instances as trade restrictions, financial regulation, and even climate change. The Internet by its very nature is a global force requiring recognition from many jurisdictions as to its regulation. As the right to be forgotten is, as a minimum, a balancing of human rights and, by extension, a potential fundamental right, then this argues more forcibly for the widest application. The AG's arguments were that the nature of human rights makes it not feasible for rights relating to privacy and freedom of expression to be interpreted for other states. It also does not provide for the situation where the balancing exercise has already been carried out before the right is enforced, taking into account such human rights at that time. Miglio goes on to argue that the AG appeared to go a step further, indicating that outside the protection provided by the EU, free speech and access to information always outweighs privacy.[95]

[94] Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain' and inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12 Adopted on 26 November 2014 (WP29,) 4.2.2. This concluded processing that is taking place which must be relevant and not excessive with a legitimate ground for processing.

[95] Andrea Miglio, *Enforcing the Right to Be Forgotten beyond EU Borders, Use and Misuse of New Technologies*, in *(eds)* Elena Carpanelli, Nicole Lazzerini *Contemporary Challenges in International and European Law*, (Springer 2019)

4.3.2 The Court's refusal to uphold the AG's opinion

Following the publication of the AG's opinion, the decision of the Court not to take it into account was considered radical. [96] Such transactions had occurred previously and this was therefore not unprecedented. [97] However, the response to his well-articulated cohesive arguments being rejected was clearly a shock to many commentators who had considered the AG's opinion to be well thought through and appropriate.[98]

A factor that may have influenced the decision could have related to the level of interest in the recognition of such a right with its potential ability to 'rein' in the giant search engines. The Spanish, Austrian, Italian, and Polish governments, who had supported the action before the CJEU had looked to establish the right to be forgotten. However, they also wanted clarity on the 'inextricable link between the activity of the search engine operated by Google and the activity of Google Spain' so that processing of data could be seen to be carried out by part of Google within the jurisdiction of the member state.[99]

The Court did take the trouble to confirm, in paragraph 80, its decision that the processing of data as carried out by a search engine was in fact capable of affecting 'significantly the fundamental rights to privacy and to the protection of personal data.'[100] This expanded upon the search results that a search engine produced for an individual's name and how this enabled much wider access to such specifically linked information. Ultimately, this would contain links to many aspects of an individual's life which were not instantly accessible without the search engine's activities. These may have only been discovered through much research, without the instant connectivity. The actual search results would therefore be

[96] It would be considered unusual for the Court to go completely against the opinion voiced by the AG and figures generally quoted show the majority of cases ie 80% of cases in 2010, followed the AG's opinion. There are exceptions generally been high profile cases likely to be controversial (e.g., the ECJ notably did not follow AG Bot's opinion in *Kadi II C-584/10P*). The court was not obliged to follow the AG's opinion but bound to uphold the law, so if the law had been correctly set out in the opinion then the court would have had to follow this even if indirectly.

[97] Treaty of Nice, Amending the Treaty on European Union, the Treaties Establishing the European Communities and Certain Related Acts, 11 December 2000, Official Journal C 80 of 10 March 2001; 2001/C 80/01, Art 220

[98] David Lindsay 'The 'Right to be Forgotten' by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling' [2014] 6(2) Journal of Media Law 177,178

[99] Google Spain para 47

[100] Google Spain para 80

greater than merely accessing already available information as the search engine result produces a mass of information in one profile.

As a consequence of a search engine's activities meeting the requirement to be designated a data controller, such as through its subsidiary or branch being present in a member state,[101] it seemed that there were initial steps being taken to understand that the real motive behind all of their activities was the commercial outcome. This was despite the posturing of internet giants and their self-acclaimed evangelists [102] and was clearly contra to the earlier concepts of the search engines being a vital component for the freedom for data to be made available on the Internet. This had been reflected in the approach taken by the EU to date despite the announcements concerning an update to the current data protection laws. The judgement in the case was, therefore, closely analyzed to understand the reasoning. The potential for such an organisation as Google to effectively provide the application of what would be considered a potential fundamental right was key to the case.

4.4 The CJEU's judgment – key aspects leading to the finding of a right to be forgotten,

Once the Court had considered the question of jurisdiction[103] and the territorial application of the DPD, it confirmed an establishment within the meaning of Article 4 (1) (a) of the DPD existed.[104] This led the CJEU to consider effectively the scope of the right of erasure and/or

[101] Even if such activities were limited to the promotion and selling of advertising space (already recognized as a key function as opposed to a general making of data available to the public as a 'public benefit').
[102] Compare with the position as to awareness of the material commercial activities of Google in 2019 where the leading French consumer association, UFC Que Choisir the Paris "*Tribunal de Grande Instance*" (TGI), issued, on 12 February 2019, its ruling on the legality of the Google+ Terms of Use and Privacy Rules, both with respect to consumer law and personal data protection regulations. Note, 'Although no monetary payment was required to use Google+, the judges considered that such service was not "free of charge" since users provided their personal data to Google, which Google then monetised. Accordingly, the judges ruled that such personal data constituted goods from which Google derived an economic benefit in return for the service provided to users. The arrangement between the user and Google therefore constitutes a contract for pecuniary interest between a professional and a consumer and consumer law is therefore applicable.' Reported by Norton Rose https://www.dataprotectionreport.com/2019/04/french-court-issues-decision-on-legality-of-privacy-rules-and-terms-of-use-under-data-protection-and-consumer-law/
[103] A search engine would be included in the court's jurisdiction under the application of Article 2 of the DPD, as previously discussed in connection with the AG's opinion, the search engine capable of 'processing of personal data' i.e., could it determine the purpose and means of processing personal data?
[104] Google Spain, para 20

the right to object in the light of the '*derecho al olvido'*, translated as a right to be forgotten but ultimately claimed as a right of oblivion by its critics.[105]

The judges noted it was clear from the preamble and Article 1 of the DPD that there was a requirement for a 'high level of protection of the fundamental right and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data…'.[106] It also focused on Article 8 of the Charter[107] which expressly contains a fundamental right to the protection of personal data. This sets out the requirements for data to be processed fairly for specific purposes on the basis of consent or some other legitimate ground with a right of access to data and a right to have incorrect data rectified.[108] This was key to the decision with regard to the question posed by the Audiencia Nationale for a right to be forgotten.

The DPD also states in recitals 2, 10, 18 to 20, and 25 in its preamble that:

> (2)… data-processing systems are designed to serve man; … they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to… the well-being of individuals.

With the emphasis on fundamental rights in the directive, it was clear the CJEU took into account the EU's intent to protect data subjects' rights with the required high level of data privacy mandated by the DPD. It specifically referred to the consequences of increased accessibility through the Internet.[109] Within the judgment emphasis on such intent of the

---

[105] Jeffrey Toobin**, '**The solace of Oblivion; in Europe, the right to be forgotten trumps the Internet'. September 22, 2014 available at https://www.newyorker.com/magazine/2014/09/29/solace-oblivion

[106] Google Spain para 66

[107] n 32 The preamble states; 'The Charter of Fundamental Rights of the European Union enshrines into primary EU law a wide array of fundamental rights enjoyed by EU citizens and residents. It became legally binding with the coming into force of the Treaty of Lisbon on 1 December 2009.' available at https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data last accessed 22 Feb 2021

[108] Article 8 of the Charter 1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

[109] Google Spain, para 80 'Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society,

DPD to protect fundamental freedoms of natural persons, and in particular their right to privacy in respect to the processing of personal data[110] and general principles of community law, including the Charter, set out the human right foundations to a right to be forgotten.[111] It could be argued that in effect the Court expanded such objectives in the Google Spain case by providing such a wide interpretation to the DPD,[112] albeit with limited guidance on the balancing exercise needed to be carried out in respect of such rights, specifically privacy and freedom of expression. This would lead to consideration of the values provided to such rights and how these could be offset against each other to provide the best possible solution to offer an individual the right to not only have informational self-determination, but to be able to portray themselves as they think best represents them.

Under the data protection regime existing at the time, the background to the case clearly suggested that the ability of the DPD was limited in providing the protection for which certain data subjects were looking. This was not merely in response to the activities of internet players. Article 12 of the DPD[113] was the relevant provision which enabled every member state to guarantee every data subject the right to obtain the 'rectification, erasure or blocking of data' where such data did not comply with the provisions of the existing directive. Certainly, it was clear that the DPD, drafted and implemented in the early days of expanding technology, had not envisaged the abilities that the growth in automation, with regard to the collection and retention of data, would produce. The ability of Article 12 to provide a solution needed a much wider interpretation, at the very least one that the AG had rejected, clearly determined this was in excess of the ability of the DPD to provide.

---

which render the information contained in such a list of results ubiquitous (see, to this effect, Joined Cases C-509/09 and C-161/10 *eDate Advertising and Others* (2011) EU:C:2011:685, para 45.

[110] As set out in the preamble to the Data Protective Directive, highlighting Article 8 of the European Convention on Human Rights 1950

[111] European Convention on Human Rights 1950, as amended by Protocols Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13 Council of Europe, 4 November 1950,

[112] Google Spain, Para 80, this recognised that the court must be aware of the impact that a search engine bought to the need for protection; 'Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (see, to this effect, Joined Cases C-509/09 and C-161/10 *eDate Advertising and Others* [2009] EU:C:2011:685, paragraph 45)'.

[113] Art 12 (b) provides 'as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;'

The Court's decision to determine under Article 12 (b) if the data subject had the right of 'rectification, erasure and blocking of information' produced a form of the right to be forgotten by the erasure of links in the search engine results. This also reviewed the rights of privacy and to data protection compared to the needs of internet users wanting access to information. It was stated[114] that as 'a general rule' data subject rights took precedence, using various reasoning to support this view. It then specifically reviewed the right to be forgotten issue and considered the question as to whether Article 12 (b) and 14 (a) of the DPD applied to enable a data subject to request removal of links to web pages 'published lawfully'[115] on the grounds that information may be prejudicial to him or that he wishes it to be 'forgotten' after a certain time.

It was also clear that the DPD had to be interpreted consistently with the rights-based legal framework established by the Charter and jurisprudence of the ECtHR, but the CJEU took a fundamentally different view when considering the importance of Article 11 of the Charter, the right to freedom of expression, especially in the context of the Internet when compared to an individual's rights in relation to the 'forgetting of information'.[116] The depth of the ruling, and to some, the lack of reasoning behind the findings led to discussions as to whether the interpretation of the DPD had been correctly made, or if the new proposals contained in the Regulation had been, to some extent, anticipated by the liberal approach taken by the CJEU.

Perhaps the most vital part of the decision, and one that would lead the focus following Google Spain, was the CJEU's brief but important expression of views that the interference in

[114]Case C -131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, [2013] ECLI: EU:C:2014:317, Opinion of Advocate General Jääskinen , in the conclusion; Para 4 'As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name.'

[115] Google Spain, para 94

[116] Google Spain, para 91. According to Mr Costeja González and the Spanish and Italian Governments, the data subject may oppose the indexing by a search engine of personal data relating to him where their dissemination through the search engine is prejudicial to him and his fundamental rights to the protection of those data and to privacy which encompass the 'right to be forgotten' override the legitimate interests of the operator of the search engine and the general interest in freedom of information.'

a data subjects right of data protection and privacy could not be justified by the 'economic interest' of a search engine.[117] The CJEU also made it clear that in light of the potential seriousness of such interference, the removal of links from the list of results could, depending on the information at issue, impact upon the legitimate interest of internet users. In such situations a fair balance should be sought, in particular between internet users' interests and the data subject's fundamental rights under Articles 7 and 8 of the Charter.[118] Whilst it is true that, as a general rule, the data subject's rights protected by those articles also override that interest of internet users, the balance may depend, in specific cases, on the nature of the information in question, its sensitivity for the data subject's private life, and the importance of the interest of the public in having that information. Such an interest may vary, in particular, according to the role played by the data subject in public life.[119] This confirmed that it was correct to take into account internet users' legitimate interests in such information being available to ensure that a fair balance of competing rights took place.

At this stage the emphasis was clearly on ensuring that fundamental rights and not simply privacy, although specifically referred to, were protected. The ability to forge a right to be forgotten from this decision could clearly be seen, albeit within narrow parameters as a decision in favour of protecting individuals' wider range of rights. This did not forego either the right for freedom of expression, almost a pre-requisite for the maintenance of liberty and self-expression, nor the right to receive information. Specifically, the CJEU looked at the level of interest in the subject matter, whether this was worthy of protection, and considered it against the data subject's fundamental rights under Article 7 and 8 of the Charter. Interest in the information would need to be carefully balanced to take into account various factors and ensure the best outcome.

---

[117] Google Spain para 97; '[A]s the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results, it should be held, as follows in particular from paragraph 81 of the present judgment, that those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name…'

[118] Google Spain para 99

[119] Google Spain para 99 '[H]owever, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.'

The decision, although consistent with public interest in how long information would be accessible through the Internet, was seen immediately as ground changing because of its impact not only on the widening of rights of privacy with recognition of fundamental freedoms, but on the ability of the ISPs to continue as before. It was also indisputable that one of the greatest outcomes was on the determination of the new role of a search engine with recognition of its impact on the individual's lifestyle and on their rights. The decision evokes privacy, but what would ultimately develop was an understanding of the wider rights involved.

4.5 The impact on Internet Search Providers

As can be seen, the original approach by the EU regarding ISPs as facilitators to the Internet was being challenged with increasing debate on the liabilities of such third parties occupying a vital but controlling presence within the Internet. Recognition of the impact of the decision in Google Spain came from the change of direction towards these organisations and the increased responsibilities they faced. This was particularly noted as being in direct opposition to the respected AG's opinion and raised many questions as to how the EU would ultimately press forward with its change of approach.

The key question that has arisen was why were search engines targeted? The previous stance by the EU was to avoid placing responsibilities on such entities[120] and this had also formed

[120] This was shown in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') The intended aim of the Directive was to: (1) The European Union is seeking to forge ever closer links between the States and peoples of Europe, to ensure economic and social progress; in accordance with Article 14(2) of the Treaty, the internal market comprises an area without internal frontiers in which the free movements of goods, services and the freedom of establishment are ensured; the development of information society services within the area without internal frontiers is vital to eliminating the barriers which divide the European peoples. Within this there was also recognition that such ISPs not only needed certainty of the law applying to them being uniform throughout the EU but that the services they provided were considered of value even if no fees etc were imposed. See Recital 18 'Information society services span a wide range of economic activities which take place on-line; these activities can, in particular, consist of selling goods on-line; activities such as the delivery of goods as such or the provision of services off-line are not covered; information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service…'

part of the AG's opinion. There was no doubt that the case impacted search engines beyond any previously debated responsibilities. In discussions as to the outcome of the case it was noted that new responsibilities with regard to requests for de-linking for the right to be forgotten would be placed on such entities. Also, there were further issues as to whether such a right was specific to search engines or could appropriately be applied to other online service providers or platforms, or even more broadly. It could be argued that the decision by the Court would place 'an undue burden on on-line intermediaries which become the ultimate arbitrator of privacy without judicial or government input'.[121] Without clear interpretation of the maze of existing legislation and regulation, assessing these liabilities by other such entities could be to the detriment of those seeking to protect not only privacy but also freedom of expression.

Despite academics' warnings of the potential impact on a variety of both non-state and state actors which would include originators or publishers of information, those requiring access to such information, even regulators making rules to secure the right, the immediate impact of the decision was clearly on ISPs, and specifically search engines. [122] In the absence of specific directions on how to proceed, the obligation to put into effect a right protecting not only privacy or family life but the more challenging aspects of dignity and reputation was placed firmly on such entities. In contrast to the US approach of protecting such companies, often providing them with a form of immunity, the judgment was considered to reflect the growing diversion between the US and EU regimes as they approached the protection required on the Internet from fundamentally differing perspectives.[123] The decision could be considered as contributing to the 'evolving transatlantic data struggle with potentially serious trade implications,'[124] an aspect that was perhaps not considered by the judges in the attempt to

[121] David Lindsay, *The 'right to be forgotten' by search engines under data privacy law: A legal and policy analysis of the Costeja decision* in (ed) A. T. Kenyon *Comparative Defamation and Privacy Law* (CUP 2016) 199-223

[122] See Michael J Kelly, David Satola, 'The Right to be Forgotten' (2017) University of Illinois Law Review Vol 1 Para II B page 12 available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2965685 last accessed 20 Feb 2020

[123] This was examined in the article by James Q Whitman, 'The Two western Cultures of Privacy Dignity versus Liberty', [2004] Faculty Scholarship Series Yale Law School Legal Scholarship Repository http://digitalcommons.law.yale.edu/fss papers 649. Last accessed 20 Oct 2019

[124] n122 Michael J Kelly, David Satola, see Introduction

preserve privacy, and ultimately reputation, as well as control over aspects of data protection for one individual.

It is not possible to fully assess the impact of the case and the reaction of the proclamation of the new right to be forgotten without also considering the enormity of the decision on Google itself. This does not imply that there was no impact on other ISPs, but due to the volume of on-line traffic through Google[125] the fallout from the case was more than significant to its activities. To some extent the other search engines appeared to be waiting to see the reaction of Google before taking appropriate action themselves. For example, the search engine Bing only responded by July 2017 with an online request form for links to be deleted.[126] Despite having approximately one tenth of the search traffic compared to Google, being the predominant provider of search facilities in the EU,[127] Bing is also the default search engine on Microsoft Windows smart phones, thus it was the first available search engine for many users.[128] The decision not to respond more promptly was perhaps indicative of a belief that the Court's decision was primarily aimed at Google.

The practical outcome of the case had, as might have been anticipated, an enormous impact on Google and raised many questions as to how the company would choose to follow the decision. The key concern would be the way such an organization could determine how to meet the newly determined responsibilities whilst retaining the commercial benefits of providing accessibility to personal data. For many, however, the decision merely confirmed the growing approach by the EU Commission to try to contain, or even curtail, Google's activities within the EU using the DPD and relevant privacy rights to fulfil this aim.[129] As a

[125] The volume of searches attributed to Google consistently above 90% of the volume in the time of Google Spain g with other competitors all achieving on average about less than 5 % of the market. See https://gs.statcounter.com/search-engine-market-share/all/europe/2015

[126] The current request for de-linking under Bing is shown at https://www.bing.com/webmaster/tools/eu-privacy-request Interestingly, it acknowledges the position of the individual in society within the information it requests when making an application. See Part 2 Part 2 – 'Your Role in Society or Your Community Are you a public figure (politician, celebrity, etc.)? Yes/ No' last accessed 17 May 2020

[127] The statistics show less of a gap for search results in the US where the percentages were in the region of 66% against about 20%, although the volume attributed to Google is increasing.

[128] see report https://www.independent.co.uk/life-style/gadgets-and-tech/news/microsofts-bing-implements-right-to-be-forgotten-ruling-asks-applicants-are-you-famous-9612113.html last accessed 15 June 2020

[129] The position of ISPs is considered in more detail in Chapter 6 when the position of the internet giants as potential monopolies is examined

consequence, the Google Spain decision received much opposition in the US, where it was believed that US corporates were being targeted and that protection of the freedom of expression was being challenged. This was also of concern to other countries, including the UK who voiced its disapproval of the decision with its resultant 'right' to those who believed that the development of a concept such as the right to be forgotten was in fact shifting responsibility for regulation of both privacy and freedom of speech from the state, i.e., the government, to a corporate entity.

One of the most argued responses condemning the decision was in the UK where, despite the long-held recognition of privacy and clear developments in progressing data protection, the case was met with a high level of disapproval. In the House of Lords,[130] the new 'ability to delink', as the new 'right' was becoming (somewhat contentiously) viewed, as a right or at least an opportunity to re-write history. In addition, the Lords' report stated that Europe's right to be forgotten which confirms that everyone has the right to wipe their digital slate clean is simply 'wrong', reporting that 'internet search engine service providers should not be saddled with such an obligation.[131]. This confirmed the earlier approach where, in a letter to Lord Boswell, the then Justice Minister, Helen Grant described the right to be forgotten as 'unworkable'.[132]

There was even sympathy for Google that it had been faced with a burdensome and unreasonable situation. This statement was made after official discussion had taken place with such knowledgeable parties as the Information Commissioner's Office and the then Minister for Justice and Civil Liberties, Simon Hughes. The Minister again concluded that the right to be forgotten was unworkable initially focusing on the cost and expense of the process that would be required considering that even if Google could afford this, many other smaller

[130] House of Lords, European Union Committee, Second Report; 'EU Data Protection law: a 'right to be forgotten'?' 23rd July 2014 available at https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/4002.htm

[131] ibid paras 17 and 52

[132] Letter dated 2nd Nov 2012, this was supported by a further letter from Lord McNally dated 2 May 2013

internet search providers would not be able to implement the ruling. In the report it is made clear that the impact would be much wider once other ISPs were involved.[133]

The EC countered this argument stating its intention was to give citizens the ability to defend their own interests and rights through approaches to such entities rather than through government bodies. This was despite criticism that the decision placed increased potential authority on these privately-owned entities forcing them to carry out, as a minimum, a review of the merits of an individual's privacy against the ability to exercise freedom of speech via the Internet. This view was held by many commentators at the time to the extent that the Future of Privacy Forum and US organization voiced, through its CEO Jules Polonestsky, that due to the complexity of the areas the decision now 'requires Google to be a court of philosopher kings', thus expressing doubts that this could be done well and that the decision showed a deep misunderstanding of how this could work.[134] A notion of which results are yet to be seen amidst growing concern as to the power of the Internet players to control not only data and privacy concerns but to also manipulate it to even potentially impact voting patterns and, ultimately, democracy. [135]

4.6 The response by Google to the decision

As can be seen, the decision to designate ISPs, in particular search engines, as data controllers was unprecedented and the outcome, which would give quasi regulatory responsibilities for the application of fundamental rights meant the initial impact, was probably underestimated. Immediately, the number of applications to remove links and the resultant publicity was

[133] The Lords report stated: 'First off, it totally ignores the fact that pretty much every other search engine (bar Yahoo and of course Bing, which rather embarrassingly had to volunteer to be included in the whole affair) doesn't have the spending power and infrastructure to implement the ruling.'

[134]see Jeffrey Toobin, 'The Solace of Oblivion Annals of Law' [2014] available at www.newyorker.com/magazine/2014/09/29/solcae-oblivion

Also note that Jules Polonetsky, the Executive Director of the Future of Privacy Forum, a think tank in Washington, was more vocal. "The decision will go down in history as one of the most significant mistakes that Court has ever made," he said. "It gives very little value to free expression. If a particular Website is doing something illegal, that should be stopped, and Google shouldn't link to it. But for the Court to outsource to Google complicated case-specific decisions about whether to publish or suppress something is wrong. Requiring Google to be a court of philosopher kings shows a real lack of understanding about how this will play out in reality."

[135] See, The Cambridge Analytica story explained, https://www.wired.com/amp-stories/cambridge-analytica-explainer/ last accessed 16 Oct 2020

immense,[136] leading Google to determine how it would then deal with practicalities of the decision. Not only did Google react by putting together a formal process, but it subsequently provided information on the decisions it would be making which would help define the scope and application of the right pending the finalisation of the GDPR and subsequent applications under Article 17. The importance of the role of Google in the development of the right to be forgotten cannot be underestimated. As a powerful commercial enterprise, it was suddenly faced with the need to become an arbitrator of human rights. This moved it far away from its aim to automate and use its generated material for commercial benefit to a more socially responsible role determining that the impact that available data held on an individual could not only have repercussions on reputation and status within a community, but also potentially on a person's dignity.

4.6.1 Google's initial reaction

If commentators were concerned[137] as to how the decision would be implemented, for Google the consequence was even greater. Acceptance that the outcome was not in line with the AG's opinion, which Google had originally welcomed believing it consistent with the importance of freedom of expression, was difficult. That it did not follow the US understanding that search engines benefited from freedom of speech was an immense shock to Google. The AG had been clear in considering that Google, as a search engine, was not under any obligation to vary its search results. Therefore, in response to any requests for links to be removed or 'erased' by individuals, it believed such requests were more correctly addressed by specific requests to websites publishing the relevant information. This mirrored the White Paper[138] that had been commissioned by Google Inc. in which the authors concluded that search engines received the protection of the First Amendment with the result that 'internet speech' through search engines were protected constitutionally and 'this full protection remains when the choices are implemented with the help of computerized

[136] 40,000 requests were received in the first two days, by September 2019 this was up to 845,501. See Google Transparency Report https://transparencyreport.google.com/eu-privacy/overview?hl=en

[137] See in particular, Ignacio Cofone, 'Google v Spain: A Right to be Forgotten', Chi-KentJ. Int'l & Comp L Vol XV available at http://ssrn.com/abstract=2548954 last accessed 17 Oct 2020

[138] Eugene Volokh, Donald M Falk, 'Google First Amendment Protection for Search Engine Results', (2011-2012) 8 J.L. Econ. & Pol'y 883 available at https://heinonline.org/HOL/LandingPage?handle=hein.journals/jecoplcy8&div=39&id=&page= last accessed 15 June 2020

algorithms.'[139] The report had also found that what could be included or not in speech or editorial judgements was not confined to journalists 'but could be exercised by business corporations generally and by ordinary people engaged in unsophisticated expression as well as by professional publishers'.[140] Specific reference had been made to the search engines being included within this journalistic exemption.[141] Previous US cases under the Communication Decency Act[142] had also shown the US stance that a claim for defamation (for loss of reputation) and negligence (including a claim for breach of privacy) would not proceed on the grounds that section 230 of this Act had been drafted to provide immunity for service providers such as Google.

The decision in Google Spain did not expressly analyze the position of Google as being considered a publisher. However, it was generally accepted that a search engine only provided a service which linked information or disseminated it without the intention to publish it or play an active role. In addition, it was acknowledged there could be no actual or constructive knowledge of the content of the search results. Without such a deliberate intention it was thought that a search engine or ISP could not be found liable as had been shown in various previous cases.[143] Without control over search results '… it was hardly possible to fix Google Inc. with liability on the basis of authorization approval or acquiescence',[144] but with the outcome in Google Spain change was imminent.

Hence, with a decision that went against all expectations, but which perhaps expressed a new legal recognition of the increasing interest in an individual's human rights within an internet-based environment, the scale of the response to the decision and Google's new role was unprecedented. Immediately after the ruling went into effect, Google reported that it

[139] n 138 Part III p 7

[140] Hurley v Irish American Gay Lesbian and Bisexual Group of Boston, 1995 Case no 515 U.S. at 574; id.at 575–76 here the court examined how freedom of expression could be protected, finding that the St. Patrick's Day Parade was an example of communication protected by the First Amendment.

[141] Communication Decency Act 1996 47 USC s 230 (Title V of the Telecommunications Act of 1996) Part C p 10. in the US Google, Microsoft's Bing, Yahoo! Search, and other search engine companies are seen as media enterprises, much as the New York Times Company or CNN are media enterprises. in addition, the First Amendment fully protects speech by all speakers, whether they are media enterprises or not.

[142] ibid Communication Decency Act

[143] This was the position in Bunt v Tilley [2007] 1WLR 1242

[144] Metropolitan International Schools Limited v Deigntechnica Corp [2011] 1 WLR 1743

had received more than 90,000 removal requests.[145] Increasingly the decision also resulted in wide media coverage. Headlines proclaimed that there was not only a new right created by the case, but that search engines would now be responsible for determining and implementing what information should be removed. Within media coverage there were diverse reactions; in the UK it was even voiced by the then Culture Minister, Sajid Javid,[146] that by removing content under the new right criminals would be using it to hide their murky pasts. [147] This evoked claims that the decision in the Google Spain case had been misunderstood. The changing approach seemed to be in direct contrast to the increasing pressure for individuals to be able to control how access by direct links is made to information about them. In many ways the opposing views seemed to be from a protectionist approach to the giant tech companies. However, within such opposition were powerful arguments as to restrictions on freedom of expression, although associated claims that history would be re-written and the past erased seemed an over-reaction. As established in the Google Spain case, the pertinent information would remain but would not be so readily available and/or immediately and permanently attached to a search result.

How was Google responding to its new responsibilities? A few months later Google announced that following the case there had now been 216,810 requests for links to information to be removed. This had then resulted in 783,510 links being reviewed and

[145] Google's webform went live on 30 May 2014, 17 days after the Court's judgment. In the first 24 hours they received 12,000 requests (European totals), and in the first four days approximately 40,000. Up to 30 June 2014 they had received more than 70,000 removal requests with an average of 3.8 URLs per request, a total of over a quarter of a million. The top five countries were: France 14,086; Germany 12,678; United Kingdom 8,497; Spain 6,176; and Italy 5,934. By 9 July 2014 the level of requests was approximately 1,000 per day across Europe.

[146] The Guardian online https://www.theguardian.com/commentisfree/2014/nov/13/terrorists-right-to-be-forgotten-online-sajid-javid-tory-bill-of-rights

[147] Mail Online 13th February 2015, 'The full scale of EU 'right to be forgotten' rules revealed: Google says it has been forced to delete 260,000 links by legislation criticised for protecting terrorists and criminals ' available at; https://www.dailymail.co.uk/news/article-2952260/The-scale-EU-right-forgotten-rules-revealed-Google-says-forced-delete-260-000-links-legislation-criticised-protecting-terrorists-criminals.html last accessed 22 Sept 2019

This explanation was widely critiqued by Paul Bernal in the Guardian. 'The ruling in Google Spain is not in any real sense a threat to journalists, and certainly not a threat of the scale of the use of the anti-crime and terrorism law, Ripa, to intercept journalists' communications with sources. Google has built a system to implement the ruling, and has, as Javid notes, received a large number of requests for delisting – as of this morning, for a total of 558,662 URLs – and 41.7% of those URLs had been delisted.' the Guardian, 13 Nov 2014 https://www.theguardian.com/commentisfree/2014/nov/13/terrorists-right-to-be-forgotten-online-sajid-javid-tory-bill-of-rights last accessed 20 Oct 2019

262,280 removed, or in effect hidden, from internet users.[148] If there needed to be any evidence of interest in a right to at least delink information, this was it.

The search engine giant repeatedly emphasized to anyone listening that it was not equipped to deal with the response itself, stating to the media: "This is a new process for us. Each request has to be assessed individually and we're working as quickly as possible to get through the queue."[149]

In spite of this, soon after the case European regulators appeared increasingly concerned at the way Google implemented the decision. Providing compliance with the decision resulted in delinking in more than half of the requests received. It became obvious that Google seemed to have cautiously followed the more usual journalistic approaches in applying the right relating to public interest, particularly with regard to requests by public figures. That diligence also meant Google only removed the search results from its European search engines, in line with the law, meaning anyone could switch to .com or other portals to access any removed links. The EU, however, took issue with this, and in particular to the fact that Google alerted websites to the removals. It also complained that Google was not passing on enough information to national regulators who were being left to deal with all the complaints Google rejected. This might be considered a harsh response although potentially indicative of the hardening attitude towards the increasing power of the internet giants.[150]

4.6.2 A new 'regulator'- the creation of the Google Advisory Council

The clear decision that was made by the CJEU on the existence of the right and how it may arise regrettably resulted in little direction on how it would be applied. Despite subsequent criticism, Google responded very quickly to the challenges placed on it. Co-operating with the Article 29 Working Party, together with three other US based search engines, it met with the parties involved. Confirming its response to the chair of the Article 29 Working Party,

[148] Google's transparency report available at https://transparencyreport.google.com/?hl=en

[149] available at https://uk.reuters.com/article/us-google-searches-eu/google-removes-first-search-results-after-eu-ruling-idUSKBN0F116O20140626 last accessed 12 Oct 2020

[150] Later this increase in responsibilities towards ISPs would be reflected in other areas of law, specifically the introduction of new liabilities under the Copyright Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC

Google set out its intention to meet the challenging new obligations.[151] To solve the problems of interpreting new territory for internet search engines, Google then took steps to form the Google Advisory Council.[152] It secured various experts from the world of privacy and data protection to form a board to advise on how the approach should be determined. In addition, a series of 'roadshows' were set up which presented the decision in the form of a new 'right' to be forgotten actively seeking the public's feedback.[153] This was not necessarily well received by data specialists, in particular the EDRi (a European Digital Rights group) who felt that it was merely a public relations exercise and as such had been used by Google to misrepresent the true position following the case's decision. In addition, it was noted that there were two issues that had not been considered during such discussions namely the position of Google prompting arguments that the case was only about reining in the power Google had over what was revealed and what was retained and its power to set the new agenda.

The first report of the Council however made it clear what the focus would be; 'Google asked us to advise it on performing the balancing act between an individual's right of privacy and the public's interest in access to information.'[154] In effect the company had been given a role to carry out protection of what many were recognizing as a new form of human right,[155] one particularly important in the data driven era. Already, clear recognition of the need to carry

[151] Letter from Peter Fleisher Global Privacy Council, Google Inc to Isabelle Falque-Pierrotin Chair, Article 29 July 31, 2014 https://docs.google.com/file/d/0B8syaai6SSfiT0EwRUFyOENqR3M/preview
Last accessed 1 October 2018

[152] The Counsel included Luciano Floridi, Professor of Philosophy and Ethics at University of Oxford, Frank La Rue former UN Special Rapporteur on the Promotion and Protection of the Right of Freedom of Opinion and Expression (his position had come to an end in August 2014, so he was newly available) Sylvie Kauffman Ed Director, Le Monda, Lidia Kolacka-Zuk, Director of the Trust for Civil Society in Central and Eastern Europe, Sabine Leutheusser- Schnarrenberger, former Federal Minister of Justice in Germany, Jose-Luis Pinar, Professor of Law at Universidad CEU, former director of the Spanish Data Protection Authority, Peggy Valcke Professor of Law at University of Leuven and Jimmy Wales, founder and Chair Emeritus of the Board of Trustees, Wikipedia Foundation.

[153] Referred to as the Google's privacy ethics tour by the Guardian newspaper in the UK this took experts to deal with public queries into major European cities. However only two recommendations were made by the Council following this exercise.

[154] The Advisory Council to Google on the Right to be Forgotten, First Report
https://transparencyreport.google.com/?hl=enhttps://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf
https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view last accessed 8 April 2019

[155] See Bart Van Der Sloot, *Legal Fundamentalism: Is Data Protection Really a Fundamental Right?* in (eds) Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul De Hert, *Data Protection and Privacy: (In)visibilities and Infrastructures*, (Springer 2017) pp3-30

out the balancing act of the human rights was involved. However, it was a difficult undertaking for such an entity to carry out without clear guidelines and with its own commercial interests to protect. It was also fighting for its own right to carry on business within the balancing act.

Within such a report from the Council[156] there was acceptance that the depth of the decision in Google Spain and its wider implications were now understood. The members of the Council even went as far as to indicate that the decision in the case had provided a suitable forum for continuation of the discussion on what was termed, 'the role of citizen rights in the Internet.'[157] It was also acknowledged that awareness of 'how to protect these rights in a digital era' had also come into the public debate. Application forms and notices concerning the decision in the case were created and put online to raise the awareness of the new right and to enable users of the Internet reviewing the results of searches through Google to be immediately aware of the position and their 'right' under the decision reached in Google Spain.[158] There was really no excuse for anyone interested in potentially controlling access to search results not to be aware of the process. Initial responses confirmed this.[159] However, as applications were made there seems to be little transparency in how decisions were being made and there began growing consciousness of the increased responsibilities Google had with regard to processing a potentially fundamental right.

4.6.3 The 'Right to be forgotten' process

Subsequent to the initiation of this procedure and with the creation of the Google Transparency report,[160] Google then made public the route it was taking to deal with the

[156] Report available at https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf

[157] The Advisory Council to Google on the Right to be Forgotten, First Report https://transparencyreport.google.com/?hl=enhttps://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view last accessed 27 Aug 2015

[158] The wording alerted a user to the fact that '*Some results may have been removed under data protection law in Europe'* and provided a link ultimately to the application form.

[159] To understand the complexities arising from the decision it should be noted that by mid-November 2014 when Google published its first transparency report, it was reporting that approximately 170,000 requests had been made for the removal of 600,000 links of which about 40% were successful.

[160] available at https://transparencyreport.google.com/?hl=en Last accessed 1 Oct 2018

number of approaches made for delinking of information, giving examples of decisions. This was also a way to minimise the impact of a full 'right' by giving limited examples of the boundaries applied to the requests. Although the decision in Google Spain was also to affect other search engines caught within its scope, this was generally regarded as minimal as over 90% of searches in Europe were being made through Google. [161] Accordingly, no other entity carried out similar volumes. [162]. The material Google provided was illuminating and as a result the response to the report was significant.[163] The EU Commission expressed concern that the volume of searches carried out by EU citizens through Google had created a virtual monopoly[164] within the high percentage of commercial activity and this impacted how the right to be forgotten would be put into place.

Increasingly the difficulties faced by the internet search engines to meet the obligations imposed by the Google Spain decision made it clear that search engines were now clearly exempted from the protections they had believed they had. They were now also being made fully responsible for policing or regulating such right with ambivalent support from the institutions who had effectively placed such a financial and administrative burden on them. For some this was seen as a move towards the 'outsourcing' of decision-making to a commercial organization responsible for 'policing' the activities on the Internet. This was replacing a former more *laissez faire* approach with a form of self-regulation taking place, but

[161] At the time of Google Spain it was recorded that Google held about 90% of the search engine market, it is now recorded on average at 88%, with Bing at approx. 5%, and Yahoo at between 2.7 and 3.1% https://www.reportlinker.com/market-report/E-Services/456921/Search-Engine?utm_source=bing&utm_medium=cpc&utm_campaign=High_Tech_And_Media&utm_adgroup=Search_Engine_Market_Reports&msclkid=a44c1d1b3f1711c439c043dd9bcc2692&utm_term=%2Bsearch%20%2Bengine%20%2Bmarket%20%2Bshare&utm_content=Search%20Engine%20Market%20Reports Last accessed 21 May 2020

[162] The other search engine, Bing, had put in place similar new processes but largely after the action taken by Google and to some extent mirroring its process and here there was little or no information being revealed https://www.bing.com/webmaster/tools/eu-privacy-request last accessed 12 Oct 2020

[163] Examples given included: 'A high ranking public official asked us to remove recent articles discussing a decades-old criminal conviction. We did not remove the articles from search results.' 'An individual who was convicted of a serious crime in the last five years but whose conviction was quashed on appeal asked us to remove an article about the incident. We removed the page from search results for the individual's name.' available through https://9to5google.com/2015/11/25/right-to-be-forgotten-examples/last Last accessed 8 April 2019. NB: the original response and examples were updated so are no longer available directly from the Google site.

[164] This is explored further in Chapter 6. The position of Google was equivalent to it operating a monopoly due to the high demand for its search engine activities and its powerful exploitation of its search facilities, ie, by allowing advertisers to pay to be ranked first in results.

without the structure of any formal state recognition. With the focus being firmly placed on Google to provide the protection secured by the new right, the intricacies of the balancing act and the policy decisions needed were far from being understood. This leads to a need for clarity not only on how this would be processed but on how and where it would be applied, including its availability globally.

4.7 The geographical scope of the new right

With Google only removing links in search results from its European search engines, it then left the way clear for others using Google's search services to access similar links to information through other portals, such as Google.com. More complex issues would also arise as to how freedom of expression was being applied within the mechanics of the process where a request to remove links had been successful, i.e., where Google had conceded to such request it could be argued to be detrimental to the right of the public to receive all information.

By May 2015, one year on from the decision, a group of 80 legal academics published an open letter calling for more transparency from Google[165] as to its decision-making process, raising public concerns as to how the application of the right was being made. This highlighted the confusion raised by the case and the debate as to whether the outcome could be claimed as a new right to protect individual's privacy. This was despite the right not being provided by any government or state sponsored organization but by a commercial entity whose sole objective was, or indeed is, maximization of profits. It was argued that the lack of clarity in the case's decision had led to a situation where:

"Google and other search engines have been enlisted to make decisions about the proper balance between personal privacy and access to information. The vast majority of these decisions face no public scrutiny, though they shape public discourse. What's more, the values

[165] Jemima Kiss, 'Dear Google: open letter from 80 academics on 'right to be forgotten'. published in the Guardian. https://www.theguardian.com/technology/2015/may/14/dear-google-open-letter-from-80-academics-on-right-to-be-forgotten last accessed 25 Sept 2021

at work in this process will/should inform information policy around the world. A fact-free debate about the right to be forgotten is in no one's interest". [166]

It was clear that the Google Spain decision, although providing an awareness of what was being termed a new fundamental right, was in fact adding fuel to a longer running debate between the protection of privacy and the right to freedom of expression. This highlighted the additional demands of this exercise being carried out by organizations without suitable credentials, or having any vested interest in acting independently on behalf of citizens in carrying it out, and with paramount commercial interests. The lack of information on the decision-making process did not help the debate. A challenge existed whereby the organization was recognized as gaining commercially from the data and, as one of the major players in the Internet era, had become the arbitrator/decision-maker on how the right could be exercised and, more importantly, on how the balancing act between competing rights could be determined. Privacy was emphasized, but knowledge of the impact on other rights such as reputation was also emerging.

Little information on the decision-making process has been made available and many commentators, such as Brock, complained as to the lack of 'transparency' in the Transparency Report.[167] However, at first sight it did appear the basis agreed with the Article 29 Working Party[168] to grant or refuse applications was being carried out and the number of complaints subsequently made to the relevant data authorities was very limited. To fully understand the position a quick analysis of a Transparency report would have shown that as of 1 October 2018 the number of links delisted was 44%, and refusals to delist 56%. The website also contained certain information concerning the refusal/acceptance rates.[169] Google noted on

[166] The letter argued that '[T]he publication by Google of examples of decisions was originally limited to 23 despite the initial response recording 546352 applications to remove URLs within the first period up to Nov 2014 after the case, raising to 2.3 million the end of 2017; see Transparency report available at https://transparencyreport.google.com/eu-privacy/overview last accessed 10 Jan 2020

[167] George Brock, *The right to be forgotten- Privacy and Media in the Digital Age*, (IB Tauris 2016) pp 51-54

[168] Article 29 Data Protection Working Party Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/12 Nov 2014 Available at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf last accessed 17 Sept 2018

[169] From an original 23 examples, 51 examples are currently listed on the website relating to where de-linking has been agreed or disagreed showing how Google has interpreted the requests. It is also able to show from

the Transparency Report that it had a clear policy in line with the Article 29 Working Party's Guidelines and also set out its position concerning the factors raised in the Google Spain decision.[170] Interestingly, it did appear from the examples that generally convictions for crimes would not be removed other than where the convictions could be considered 'spent' under provisions for rehabilitation of offenders' legislation. As will be discussed later, this basis for decision-making, whilst of increasing importance to not only privacy but reputation and ultimately ideas of rehabilitation, was not confirmed as a principle and did not appear to be followed with any consistency. The number of applications for removal of such convictions highlighted the ability of this type of personal information to not only impact family and private life but, significantly, reputation. This reflected not only in how one interacted in society under ideas of privacy, such as the right to be left alone, but also on acceptance within society as a functioning citizen.

To assist the process and inform the public, the EU, via the Article 29 Working Party, had published detailed guidelines on how the new right would be implemented by search engines.[171] The press release was also intended to provide some certainty but perhaps went further than anticipated in proclaiming that the delisting decisions needed to provide 'the effective and complete protection of data subjects' right and that EU law cannot be circumvented'.[172] It was also made clear that the intention, although ultimately disputed by Google, was that in any case de-listing should also be effective on all relevant domains, including '.com'. This led to the first acknowledged case concerning the jurisdiction of the right to be forgotten where the CNIL challenged Google[173] claiming that there was a requirement to delist not just from the European state where the issue arose, but for results

where the delinking requests originate, although this is not necessarily represented by the examples where 15 out of 51 were from the UK. The number of examples had increased from the 14 given in 2014.

[170] Google statement: 'We may also determine that the page contains information which is strongly in the public interest. Determining whether content is in the public interest is complex and may mean considering many diverse factors, including—but not limited to—whether the content relates to the requester's professional life, a past crime, political office, position in public life, or whether the content is self-authored content, consists of government documents, or is journalistic in nature.' available at https://transparencyreport.google.com/eu-privacy/overview?hl=en Last accessed 1 October 2018

[171] see n168 Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"

[172] http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2014/20141126_wp29_press_release_ecj_de-listing.pdf

[173] Case 507/17 Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) [2019] ECLI:EU:C:2019:772

available through Google.com. It was clear one of the main objections to the implementation of the decision was the ability of someone to carry out a similar search and receive unrestricted results in the US, irrespective of a successful delinking taking place in the EU.[174] The initial outcome of the case was subsequently appealed by Google. The final hearing ultimately took place in September 2019 and surprisingly found in favour of Google's argument that the right should be limited to the relevant jurisdiction, this is discussed further on in this chapter.

4.8 Post Google Spain: the impact and debate in further cases

The impact of the Google Spain case, apart from the practicalities of Google's process and the subsequent implementation of a formal right under Article 17 of the GDPR, was vital in establishing how the right to be forgotten has been applied. From this decision there were several cases within the EU member states, but the number of cases this then led to remained low. From the limited information available, it appeared that few refusals to delink were, or are even now, appealed, thus increasing uncertainty. Finland was one of the first countries where an appeal against a refusal by Google to remove links was reported in 2015, but it has confirmed that only 1.5% of data subjects in over 2000 rejections had appealed to the Finnish Data Protection Authority. In this appeal the refusal to delink was upheld.[175]

[174] An initial response was made by France's Commission Nationale de l'Informatique et des Libertés, or CNIL, who challenged the assumption by Google that removal of links would only be necessary in the actual national state where the search results were being accessed. This was not acceptable to the French data protectionists who saw that an individual's privacy, or indeed data protection, could be compromised by access being immediately available purely due to a change in where access was obtained. It then issued a formal order to Google to apply de-linking under the right to be forgotten which had been approved of by them to "all domain names" of the search engine globally, including Google.com, not just those that aimed at Europe, such as google.fr. "For delisting to be effective, it must be world-wide," said Isabelle Falque-Pierrotin, the head of the CNIL. "It is a question of principle. Google must respect the rights of European citizens." Google was given15 days to conform after the decision by CNIL, after which CNIL would then open sanctions proceedings that could lead to a fine of up to €150,000 ($168,000). http://www.wsj.com/articles/french-privacy-watchdog-orders-google-to-expand-right-to-be-forgotten-1434098033

[175] Finnish Data Protection Ombudsman, Reijo Aarnio, agreed with Google's decision to reject a businessman's attempt to remove links to articles about his past business mistakes. Aarnio ruled that "there was no need to delete the search results because Finland's business register lists the man as still being involved in business operations, including debt collection". The rejection was not surprising as Google has consistently been rejecting requests to delink articles related to a person's current profession. http://thefreeinternetproject.org/blog/google-wins-first-appeal-right-be-forgotten-rejection-finland

One of the earliest cases took place in the Netherlands, again involving a criminal aiming to have references to his crime removed. In this case, the principles of Google Spain were applied strictly with the judge determining that 'the [Google Spain judgement does not intent to protect individuals against all negative communications on the Internet but only against being 'pursued' for a long time by 'irrelevant', 'excessive' or 'unnecessarily defamatory' expressions.[176]

Amidst the various cases there were opportunities for the principles of Google Spain to be re-considered when, in the UK, a joined case of two claimants already granted anonymity reached the Supreme Court. The decision provided one of the more detailed analysis of the Google Spain outcome. This was the UK's first case concerning the right to be forgotten to have progressed to the court despite several early forays to Google with applications to remove links. It was backed by the charity Unlocked which supports those seeking to benefit from rehabilitation in respect of past convictions. Unlocked supports applications made for removal of links to information relating to convictions which had been 'spent under current rehabilitation legislation'.[177] Claimed a victory by the UK media,[178] the actual decision, whilst providing a useful interpretation of the decision in Google Spain, did not come to an overall conclusion on how the right to be forgotten would apply in such circumstances. Based on similar facts, one claimant was not able to have the links removed whilst the other was. It almost seemed that the final decision was made on a moral stance as the character of the claimant, NT1, was not sympathetically received by the judge who did not accept that there had been any impact on his privacy or to his family life. In fact, the judge claimed that the nature of NT1's actions had led to a situation where he could not be considered to have any reasonable expectation of privacy.[179] In addition, continued involvement in similar businesses

[176] Case ref. *Zoekresultaat - inzien* (document available in Dutch) ECLI:NL:RBAMS:2014:6118 see also George Brock *The right to be forgotten- Privacy and Media in the Digital Age*, (IB Tauris 2016) p56

[177] Rehabilitation of Offenders Act 1974. Chapter 53. Recital, 'An Act to rehabilitate offenders who have not been reconvicted of any serious offence for periods of years, to penalize the unauthorized disclosure of their previous convictions, to amend the law of defamation, and for purposes connected therewith.' available at https://www.legislation.gov.uk/ukpga/1974/53 Last accessed 26 March 2019

[178] 'Google loses right to be forgotten case', The Guardian, see https://www.theguardian.com/technology/2018/apr/13/google-loses-right-to-be-forgotten-case last accessed 11 May 2028

[179] NT1 & NT2 v Google LLC [2018] EWHC 799 (QB) Para 170 ''His role has changed such that he now plays only a limited role in public life, as a businessman not dealing with consumers. That said, he still plays such a role. The crime and punishment information is not information of a private nature. It was information about business

where the individual had continued to be in the 'public eye' meant that the decision reflected that public interest in the claimant was still maintained. This was compared with the position of claimant, NT2, who displayed more remorse and who also had a young family to consider where the impact of a loss of privacy would be greater. However, the ability for such individual to be granted the right to remain anonymous was clearly of benefit, despite the unclear decision and reasoning as, unlike Senor Gonzàles, they were at least 'forgotten'.

Within the EU, further cases were being considered, again with a variety of conclusions. In Finland, a state supportive of the right to be forgotten, a convicted murderer continued to seek removal of reference to his crime on the grounds that this was causing him to forfeit his right to privacy.[180] Such a crime would have always been considered by Google to continuously remain in the public interest, Google had therefore continued to resist applications to remove the links. However, in this instance the court determined that the crime had been committed whilst the individual was not of sufficient mental ability to have capacity to understand the consequences of his action. This view seems consistent with the idea of not just privacy or data protection, nor even reputation, but with the concept of dignity and, crucially, rehabilitation. This was also consistent with underlying ancient rights which formed the foundation to the right to be forgotten.[181]

The impact of Google Spain also raised further questions focusing on the role of ISPs in the application of the protection of specific individuals' rights. More recently, two cases have revisited and developed some of the ancillary issues. These started with the opinions delivered by Advocate-General Szpunar.[182] As with Google Spain, the cases applied the DPD before the implementation of Article 17 of the GDPR. Both cases were concerned with the processing of personal data but specifically on the free movement of such data. Central to the

---

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.'

[180] Korkein Hallinto- Oikeus Högsta Förvaltningstomstolen (The Supreme Administrative Court of Finland) 2018: ECLI:FI:KHO:2018:112 (case reported in Finnish only)

[181] See ch 2 on 'le droit a l'oubli', 'derecho al olvido'

[182] C-136/17, GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL), interveners: Premier ministre, Google LLC, successor to Google Inc. [2019] EU:C:2019:773 Opinion of Advocate General Szpunar and C-507/17 Google Inc. v Commission nationale de l'Informatique et des Libertés [2019] ECLI:EU:C:2019:15 Opinion of Advocate General Szpunar

issue was the search engine's obligation to respond to requests for de-linking by data subjects. Both cases were referred to the court by CNIL but were based on different scenarios.[183] Within the actions what became of increasing importance was the ongoing question whether search engine operators, now held to be data controllers, required authorization under the provisions of the DPD to carry out processing. The issue had not been fully considered in Google Spain as the form of data was not controversial, but with the case of sensitive or 'special' categories of data the position needed clarification as part of the overall review. This raised, in the case of GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL),[184] the question as to whether the prohibition of processing data falling within certain specific categories also applied to search engine operators. The AG's view was to take a balanced stance and he ultimately determined that any processing carried out would be, by its nature, secondary to a search engine's activities. This repeated, though more successfully this time, the argument raised in Google Spain ultimately resulting in acknowledgment that the Directive would only apply to specific activities, such as referencing activities (searching, finding, and making information available in an efficient way). This included how sensitive information was processed in such activities. Where the search engine had a duty to de-link or remove references, the AG confirmed that the search engine should generally automatically agree to de-link any links to sensitive data other than where there were valid reasons for its retention. However, he continued that if Article 9 of the Directive, relating to journalistic, artistic, or literary purposes, was concerned then a balancing of rights exercise would still be required to determine if a de-linking needed to be carried out.[185]

[183] Case C-136/17, GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL), interveners: Premier ministre, Google LLC, successor to Google Inc. [2019] EU:C:2019:773 (Case C-136/17)
Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) [2019] EU:C:2019:772 (Case C-507/17)
In C-136/17 the CNIL refused to take measures against Google for failing to de-reference various links from search results and the affected data subjects complained about inaction. In C-507/17, by contrast, the search engine operator was sanctioned and then contested CNIL's decision.
[184] ibid Case C-136/17 p 49 'whether the provisions of Article 8(1) and (5) of Directive 95/46 must be interpreted as meaning that the operator of a search engine is required by those provisions, subject to the exceptions provided for by the directive, to accede to requests for de-referencing in relation to links to web pages containing personal data falling within the special categories referred to by those provisions.
[185] ibid Case C-136/17 Part VI para 105(4)

The opinion of the AG in Google v CNIL was also of significant interest in trying to resolve the ongoing issues between Google and CNIL since the decision in the Google Spain case. Of particular interest was the territorial scope of the decision in Google Spain, i.e., whether it could apply to worldwide domains and not just the country of application. In a more controversial stance, the AG decided to agree to limitation on the scope so that, in effect, searches outside of the EU would not be affected by a successful application to de-link in one state. This was in direct opposition to the view taken by CNIL, a view that was considered by the CJEU in weighing up the AG's opinion in this case. The AG had taken the stance that allowing such limitation would significantly reduce access to information and should, therefore, be treated with caution. However, based on this opinion, the basis of a right to be forgotten exercise could be argued to be meaningless because by the action of effectively moving a search to another domain, removed links would immediately be available, thus there would be little or no benefit in applying a right to be forgotten. Should a de-linking exercise be successful, there would be a need to consider all the information to ensure appropriate 'de-referencing' within the EU, including by the use of 'geo-blocking' in respect of an IP address located in the EU, irrespective of the domain name used by the internet user.

As with Google Spain, there was no clear indication as to whether the AG's opinion would be followed at a time when there is more interest in ascertaining the application of the GDPR. To CNIL's dismay the final decision followed the advice of the AG and in September 2019 it was decided that the right to be forgotten would be limited to being applicable within appropriate EU member states. In addition, the CJEU stated that the right when exercised should show:

> '[t]he balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of Internet users, on the other, is likely to vary significantly around the world. [186]

[186] Case 507/17 para 60 'Moreover, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality (see, to that effect, judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraph 48, and Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, point 136). Furthermore, the balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world.

In this decision the CJEU declared that it was not for the EU to stipulate such balancing of these interests outside its own territory. In summing up, however, it stated that the search engine should at the least exercise the right by:

'using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an Internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request.'[187]

Although this decision could present a real threat to the full use of the right to 'forget' information on a global basis, i.e., there remains the simple ability to view full search results through alternative access to the Internet, this proviso offered slight respite. In addition, it would still be that a member state could carry out such balancing exercise according to its own jurisdiction and jurisprudence. As a result, it could be argued that the decision is unclear and there is the possibility for national courts to still order global de-listing if the balancing act supports this.[188] It remains to be seen how the right to be forgotten will work within the global reach of the Internet and how, under this decision, the level of protection can be provided.

4.9 Conclusion

In the development of the right to be forgotten, the decision of the CJEU in the Google Spain case was unprecedented. This clearly defined the concept, albeit without a clear definition of scope or extent of its application. The immediate and most relevant impact was on the liabilities of search engines or, even more controversially, on Google itself. However, when the principles relating to the 'erasure' of data considered to come under the DPD are combined with the balancing act of competing human rights, primarily of privacy and freedom

[187] Case C-507/17 para 74

[188] Case C-507/17 para 72 see comments by Mary Samonte 2019; available at https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/

of expression, they must be applicable to other entities engaged in data driven activities if found to be data controllers. With the GDPR only formalized two years after the decision, the clarity offered to date, whether by jurisprudence or legal commentary, has been in relation to the Google Spain decision. The technical, but potentially widely applicable, provisions of Article 17 of the GDPR which will apply to data controllers and data processors may, whilst potentially expanding a right of erasure (right to be forgotten), also limit it.

As seen in this chapter, the contribution made by the Google Spain decision has involved various elements. The first could be considered the more practical aspect of the decision, i.e., the confirmation of a search engine, an ISP, being designated a data controller, with the additional responsibilities placed on Google in this instance to also administer the right to be forgotten as determined in the case. The role of such a commercial entity as a potential quasi regulator is examined in the following chapters, as is the environment in which such ISPs are operating. Secondly, the case's role in focusing attention on the finalisation of the GDPR has also been vital, not just for formalisation of the new right of erasure but for wider data protection, supporting increased rights for individuals. The third aspect has been to provide a basis for evolution of the principles of applying the balancing act between the rights of, namely, privacy and freedom of expression, but also of further fundamental rights and freedoms. This perhaps highlights the increasing needs to be met in an era of increasing data availability and unforeseen consequences. The importance of the case cannot be underestimated. Provoking a media response has had the effect of highlighting privacy and reputational concerns with regard to how information is presented and retained through the digital memory which is explored in Chapters 5 and 6. The scope of the precedent established under Google remains as valid and essential to the application of the right potentially under Article 17 as at the time the case was determined. However, its scope and application with regard to an individual's ability to maintain informational self-determination remains to be clarified with regard to how a search engine meets its new responsibilities.

Chapter 5 -The scope of the Right to be Forgotten: its use for informational self-determination providing for the protection of reputation and dignity as well as privacy

5.1 Introduction

As seen in Chapter 4, with the decision reached in Google Spain there was an outcry that removal of information would re-write history as well as impacting the exercise of freedom of expression. Although considered a more extreme view, there is no doubt that if a person wins the right to remove links, or actual information, which applies to past events in their life, that this can provide a 'filter' of that person's history, and therefore how such person is portrayed to the public. To restrict access to information would challenge the ability of the public to receive information. This could lead to privacy of the individual being considered more important as is arguable was the ultimate decision in the Google Spain case. However, this process may also impact positively on other rights such as dignity or reputation itself. With the decision in Google Spain followed by the subsequent implementation of Article 17 of the General Data Protection Regulation (GDPR),[1] the right to be forgotten as such now clearly exists for individuals to have more control over access to their personal information which is no longer relevant or which depicts them inappropriately. This enables them to have better control over how they are perceived by the public with an ability to exercise informational self-determination to achieve this.

With the exercise of the balancing act between freedom of expression and privacy, this portrayal of self through such deliberation may involve consideration of the importance not just of past events but of the part a person plays in public life and the resultant public interest.[2] Although looking at politicians specifically, Young argues that pursuing a public profile, or as a consequence of public behaviour displayed by an individual, there is a waiver, or tacit consent of a waiver, of rights of privacy.[3] This, however, does not extend to those who could not reasonably expect that such public exposure may occur without their consent.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. (GDPR)

[2] This has been illustrated in various cases such as the cases of Campbell v MGN [2004] 2004 UKHL 22 and RocknRoll v News Group Newspapers Ltd: [2013] EWHC 24 (Ch), and even to some extent in the joined cases of NT1 & NT 2 v Google LLC [2018] EWHC 799 (QB) which were made under the principles of Google Spain.

[3] Shaun P Young, 'Politicians' Privacy', Ramon Llull Journal of Applied Ethics, [2018] Iss 9 pp 191-210

A comparison of high-profile individuals, such as politicians, and their right of privacy with the public's right to know reveals another facet to the balancing act required in the right to be forgotten, whether under Article 17 of the GDPR or under the principles set out in the Google Spain decision. The use of informational self-determination may, therefore, be claimed to provide more limited rights for a person such as a politician with the public having more right to know more about that person's history.[4] This position is, however, challenged by the approach taken in different jurisdictions, particularly the US attitude whereby information once in the public arena can no longer be considered to be private whatever the result to a person's reputation. This can be contrasted with the view in Europe where laws of confidentiality will provide some protection.[5]

The ability to apply informational self-determination by choosing what information should no longer be accessible may also be influenced by changing views of privacy, incurring additional debate as to the right of the public to receive information. Both of these aspects are examined in this chapter to investigate the opportunities offered by a wider interpretation of the right to be forgotten. This includes consideration of how ideas of identity and reputation may potentially impact the scope of the right to be forgotten. Consideration is also made as to the extent that the ability to be autonomous in respect of personal information can, or indeed should be able to, portray a person in a different light or to change the public perception of a person within the exercise of the right to be forgotten.

5.2 The inclusion of other rights within the scope of the right to be forgotten

As discussed in Chapter 2, concepts of privacy, balanced with freedom of expression, have formed the backbone of the right to be forgotten in order to determine if data needs to be delinked or removed. In contrast to accepting that the right to be forgotten forms a sub-set of privacy and is part of the formalization of data protection, there are alternative views. for example, that the right is closely linked to personality rights such as a right to identity.[6] This

[4] Shaun P Young, 'Politicians' Privacy', Ramon Llull Journal of Applied Ethics, [2018] Iss 9 pp 191-210

[5] See Frederik J. Zuiderveen Borgesius, Dr. Wilfred Steenbruggen, 'The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust Laws of confidentiality exercised in Europe', (2019) Theoretical Inquiries in Law, Vol 20, Iss 1

[6] Giorgio Pino, (2000). *The right to personal identity in Italian private law: Constitutional interpretation and judge-made rights* in (eds) M. Van Hoecke; F. Ost *The harmonization of private law in Europe* (Oxford Hart Publishing 2000) pp.225-237 p.237. https://papers.ssrn.com

provides the ability for an individual to control not just their personal information but how it can be used to portray them. If the right is viewed as previously discussed as, [7] i.e., being rooted in the French right of '*droit a l'oubli'*,[8] the Italian right of personality also supports this idea with one definition of such right being put forward as the 'right to silence on past events in life that are no longer occurring'.[9] The concept of the ability to interpret the right to be forgotten in line with this right to silence can be considered to be linking it to the maintenance of dignity and reputation. The deletion of personal information with the ability to control how much is accessible must be necessary to ensure autonomy with the preservation of dignity and, ultimately, to provide for informational self-determination as well as the protection of privacy. The involvement of such wider rights in the right to be forgotten may play an important role in ascertaining the full value of the right in providing informational self-determination.

5.2.1. A right to personal identity

Article 17 of the GDPR now contains the right of erasure (right to be forgotten) which can be exercised in various ways. The ability to request removal of information is contained particularly within the provisions of Article 17 Para a) which provides for the erasure on the grounds that the information is no longer necessary.[10] However, under Para c)[11] the data subject can object to the processing on wider grounds. This then evokes Article 21 where there is a need for a data controller to show on such objection that its legitimate grounds for the processing 'override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims'.[12]

---

[7] See Chapter 2 p 44

[8] '*droit a l'oubli*' was recognized in the French Data Processing, Data Files and Individual Liberties Act, 6 January 1978, Law No**.** 78-17, which established individuals are entitled to access, alter, correct, or delete personal information.

[9] Giorgio Pino, (2000). *The right to personal identity in Italian private law: Constitutional interpretation and judge-made rights* in (ed) M. Van Hoecke; F. Ost *The harmonization of private law in Europe* (Oxford Hart Publishing 2000) pp. 225-237 p. 237. available at https://papers.ssrn.comhttps://papers.ssrn.com/sol3/papers.cfm?abstract_id=1737392&download=yes

[10] Article 17 para a) states 'the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed'.

[11] Article 17 para c) states 'the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2)'.

[12] The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1),

With this, the right to be forgotten as provided by Article 17 may be construed on a wider basis to be more than just a functional right of delinking or 'forgetting' information. If the data controller has to have sufficient reason to process the information that the data subject objects to and, on the balancing act, the right to freedom of expression is not paramount, this opens the option of interpreting the right on a wider basis. Rather than being limited within concepts of privacy, its use can potentially be extended to provide an opportunity for an individual to manage the availability and use of personal information to retain the persona they desire. With increased awareness of social media and how you can be portrayed there, where the ability, or even the necessity, to project yourself in a certain way has become part of the daily rituals of life, how does the reverse apply, and how do past events whether social, criminal, emotional, or merely the errors of youth, shape the person you want to see portrayed? This, as well as identity, can be acknowledged in a wider interpretation of the right to be forgotten.[13] The impact of such public portrayal of self evokes the need to maintain dignity and reputation as well as privacy.

Cofone expressed the view that privacy is inextricably tied to values, such as personal autonomy, dignity, and individuality.[14] If looking at what the right to be forgotten is actually trying to resolve, he argues that among other rights that can be prejudiced by the accessibility of information through a digital memory, those of reputational harm, financial and discriminatory harm, as well as harm to autonomy and privacy must be considered. He believes that the right to be forgotten 'is a distinct right that seeks to address a wide universe of online harms.'[15]

This provides a link between the right to be forgotten and the idea of one's identity being impacted not only by the ability to present the desired identity, but in doing so to erase past versions in line with the evolution of a person, their character, and their personality.

---

including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defence of legal claims.

[13] See Chapter 2 for the discussion concerning the relationship between privacy and reputation

[14] Ignacio Cofone, *The Right to be Forgotten, A Canadian and Comparative Perspective*, (2020, Routledge Focus) ch 1, p 5

[15] ibid ch 1 p 9

To look at any right to have a personal identity, key ideas of such protection for an individual had developed a wider perspective in Italy. This is despite legal protection in Europe which often focuses on rights over property,[16] particularly before the formal recognition of human rights. The Italian Civil Code of 1942[17] confirming fundamental rights for citizens was followed by ratification of the European Convention on Human Rights[18] in 1955. This moved towards wider acceptance of rights of liberty and personality[19] with the resultant strengthening of personal rights and freedoms.

However the ability to influence how a person can be portrayed has already led to emergence of a new right in Italy, a 'right to personal identity'.[20] This is as a result, of there being an accepted ability to develop new 'fundamental rights' under Article 2 and Article 3 (2) of the Italian Civil Code[21], which permits further development of human personality now recognized as part of dignity.[22] Pino claimed that this right could legitimately be called new as it is only within the last two decades that it has been recognized by judges and legal theorists in Italy and subsequently by the legislature.[23] It is surely no coincidence that this right has been accepted now and potentially re-invented within the era of the Internet where the need for new protection has arisen. Pino's view is that the acceptance of this new concept relies on both cultural and social factors, despite the argument that this was already a historic right within Italian legal culture. The right of personal identity provides the ability to 'own' one's name, address, and status within Italian records. In particular it builds on recent interest in the concept of identity within Europe, coinciding with the growth of technology which has

[16] As explained in Chapter 2 it was only with the period of the Enlightenment that there was recognition that non property owners were also entitled to the benefit of human rights.
[17] *Codice civile*no no 262 of 16 March 1942
[18] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 134 November 1950, ETS 5 (European Convention on Human Rights 1950)
[19] Italian Civil Code, Art 2 'acknowledges and protects the fundamental rights of the human being both as an individual and as a member of social groups'
[20] It is accepted that under Italian law Article 2 of the Italian Constitution permits the creation of wider rights as it has been argued that this is an open clause ie one that permits development art. 2 as Pino states it is considered a necessary technical tool by which the legal system recognizes general moral or social needs. see Pino n6 p ch 4.1 230
[21] The Italian Civil Code enacted by Royal decree no. 262 of 16 March 1942.
[22] See n6 Pino Ch 4.1, p 229
[23] See n6 Pino Ch 4.1 pp. 225-237

potentially resulted in more invasions of individual rights. [24] This argument was explored by de Andrade who argues that such a right must include questions of how a person perceives themselves as well as how such person is perceived by others. [25]

If Articles 2 and 3 (2) of the Italian Civil Code are combined they can create new constitutional and fundamental rights provided these are to ensure the full development of an individual's personality. The argument is made that judicial decisions by the court confirmed the existence of such rights to assist the development and protection of human personality more urgently required by societal changes.

This judge-made right was originally believed to have been founded in the case of Pretura Roma[26] in 1974. As mentioned in Chapter 3, showing a change in attitude to how people could be presented in public it was held that the plaintiffs' right to their personal identities had been damaged by photographs of them being taken and used. In this case, images of a man and a woman had been captured and used in promoting anti-divorce legislation, portraying them as working together in the traditional view of a married couple. The action was based on the claim that there had been a violation of the couple's rights to their own likenesses protected under Article 10 of the Italian Civil Code. In addition, that they had been falsely portrayed because they were not married, and the picture had not been taken with consent. They therefore objected to their images being used in what was effectively a propaganda campaign. [27] The judge accepted their arguments but went a valuable step further by adding that the taking and the using of the photos were also in breach of their right to personal identity. He concluded that this gave an individual the right to repudiate acts or claims relating to acts which had not taken place. The case then led the way for further cases to be considered to offer what Pino calls 'a new protection of the person from the misrepresentations of the mass media'.[28] This development of a right of identity could be

[24] To look at the roots of the right to personal identity, the Italian Civil Code included specific personality rights such as the right to own one's own name and the right to one's own likeness but also included the autonomous development of the person and human dignity in the two parts of the constitution, see Principi Fondamentali and Diretti e Doveri dei Cittadini (Fundamental principles, Citizens' rights and duties)

[25] Norberto Nuno Gomes de Andrade, *Right to Personal Identity*: *The challenges of Ambient Intelligence and the Need for a New Legal Conceptualization* in (eds) Serge Gutwirth, Yves Poullet, Paul De Hert, Ronald Leenes *Computers, Privacy and Data Protection: an Element of Choice,* (Springer 2011)

[26] Pangrazi & Silvetti v Comitato Referendum 6-5-1974 ('Pretura Roma')

[27] In fact, it was reported that they were supportive of the divorce law which the advertisement was opposing

[28] see Pino n6 p 235

seen as providing control of information made available about oneself to determine how one is perceived by the public and also ultimately one's reputation. This then closely links to the scope of the right to be forgotten[29].

5.2.2 The involvement of loss of reputation

The debate on the extent of the right to be forgotten if this is to involve forms of identity, must therefore include consideration of its link to reputation. The concept of reputation represents old, deeply rooted ideas of the value attached to how society sees a person.
As Shakespeare said;

> *'Good name* in man and woman, dear *my* lord, Is the immediate jewel of their souls: Who *steals my* purse *steals* trash; 'tis something, nothing; 'Twas mine, 'tis *his*, and has been slave to thousands: But *he* that filches from me *my good name* Robs me of that which not enriches *him* And makes me poor indeed.'[30]

Despite wide acceptance of its value, reputation, as was seen previously, is not recognized as any express or formal human right as such, rather it forms part of the rights for private and family life. This links to rights considered to provide the foundations of the right to be forgotten. When reviewing such personality interests, Pound looked at the wider aspect of such rights, seen also as co-existing with dignity, where claims for an individual 'to be secured in his dignity and honour as part of his personality in a world where one must live in society among his fellow men.'[31] Without protection as to how one is portrayed or seen within society the value attached to a person's reputation can become meaningless.

However, despite such earlier recognition of its importance, where reputation has been expressly included, it is more or less incidental to privacy, as was shown in Article 17 of the International Covenant of Civil and Political Rights.[32] The European Convention for the

[29] see n 25 p 93 here Andrade even sees a link between the right to be forgotten and a right to personal identity, proposing a stronger case for the emergence and consolidation of the right to oblivion
[30] William Shakespeare, *Othello*, Act 3, Scene 3, circa 1603
[31] Roscoe Pound, 'Interests of Personality' (1915) 28 Harvard Law Review 343 p47
[32] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171 '1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and *reputation*.
2. Everyone has the right to the protection of the law against such interference or attacks.'

Protection of Human Rights and Fundamental Freedoms (the Convention)[33], which followed the Universal Declaration of Human Rights, however, has no equivalent reference to honour or reputation.[34]

In fact, the wording of the discussions around the formation of the Convention clearly shows the omission of "reputation" to be deliberate in the initial draft documents.[35] Other than a mention as an exception to the right of freedom of expression in Article 10, there is no other reference to reputation or its need to be protected in the Convention. Despite this, it is clear that such a right exists and has been in existence from early times. However, its value is often reduced due to ineffective remedies in respect of loss of reputation.[36] Formal recognition was finally given in the case of Lingens v Austria 1986,[37] with the subsequent result that reputation and freedom of expression were now considered to be competing although equal rights. This was also supported by a series of decisions more recently, beginning in 2003, where the ECtHR sought to show a person's reputation as being worthy of protection under Article 8 within the right for a private life. [38]

Aplin[39] specifies four reasons which, in her opinion, have led to the legal, as opposed to societal, recognition of reputation within Europe, specifically the approach taken by the

available at: https://www.refworld.org/docid/3ae6b3aa0.htm last accessed 10 January 2020

[33] European Convention on Human Rights 1950.

[34] Despite the fact that the preamble stated that the parties to the Convention were:
"resolved, as the Governments of European countries which are like-minded and have a common heritage of political traditions, ideals, freedom and the rule of law to take the first steps for the collective enforcement of certain of the Rights stated in the Universal Declaration", this did not reflect the acceptance on an almost universal basis to protect one's good name.

[35] Article 8 of the European Convention on Human Rights Discussion Page 3 states 'this omission was deliberate…' available at https://www.echr.coe.int/Documents/Library_TP_Art_08_DH(56)12_ENG.PDF

[36] See Roscoe Pound n 31 above, also George Spencer Bower, *An actionable Code of the Law of Defamation (*Gale, Making of Modern Law, 2010) where, along with considering the law of defamation, Bower also analysed reputation. In Robert Post 'The Social Foundations of Defamation Law: Reputation and the Constitution', [1986] 74 California Law Review p 691 here he tried to identify various concepts of reputation

[37] Lingens v Austria 1986 8 ECHR 407

[38] Cumpana v Romania (2004) 41 EHRR 200 at 91, Chauvy v France (2004) 41 EHRR 610 at 70, White v Sweden [2007] EMLR 1 at 21

[39] Tanya Aplin, Jason John Bosland, *The Uncertain Landscape of Article 8 of the ECHR: The Protection of Reputation as a Fundamental Human Right?* in A. Kenyon, (ed) *Comparative Defamation and Privacy Law* (CUP, 2016), ch 13.

ECtHR. The first three emerge from the early work by Post,[40] echoing early human rights theories of property, honour, and dignity, with a fourth component put forward by David Howarth arguing for sociality justification.[41] An acceptance of the first three means that the fourth is more intriguing from a societal point of view as it focuses on the ability to maintain social relationships and not be excluded from certain activities which may impact private life. Although this is not 'dignity' based, it clearly involves the perception and value of a person within their community or society. The way personal information or data are made available and how they are presented can have significant impact, particularly with the invasive nature of the Internet and the permanency of digital memory. For certain individuals this can be life changing. The need to find a route through this to secure privacy as well as reputation clearly increases with the availability and the ubiquitous nature of such data, thus emphasizing why the right to be forgotten has such intrinsic value.

The right to be forgotten, as originated in the Google Spain decision and discussed earlier, has come from ideas of privacy as well as data protection involving both dignity and autonomy, thereby forming a normative platform of human rights that have supported development of this new right. Looking at how the retention and accessibility of information which in the pre-Internet era would have been 'forgotten' leads directly to the involvement of such rights. Within this recourse there must also be justification for its use where a person's reputation is at risk, as was seen to some extent in the claims made by Senor González [42].

In the leading ECtHR case of Pfeifer v Austria[43] which was issued several years before Google Spain, the court held that the reputation of a person, even where there is a prospective legitimate debate i.e., potentially under freedom of speech, was still worthy of protection and also drew upon the notion of protection of personal identity:

---

[40] Robert Post, 1986. 'The Social Foundations of Defamation Law: Reputation and the Constitution' (1986). Faculty Scholarship Series. 217. available at https://digitalcommons.law.yale.edu/fss_papers/217 last accessed 25 March 2020

[41] David Howarth 'Libel: Its Purpose and Reform' (2011) 74 Modern Law Review pp 845-877 see pp 49,57

[42] It was argued that the orders made in respect of Senor González' property were so old as to no longer be relevant, see Case 131/12 Google Spain para 98. It should be held that, having regard to the sensitivity for the data subject's private life of the information contained in those announcements and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that that information should no longer be linked to his name by means of such a list.

[43] Pfeifer v Austria 2007 48 ECHR 2252

> 'The Court considers that a person's reputation, even if that person is criticized in the context of a public debate, forms part of his or her personal identity and psychological integrity and therefore also falls within the scope of his or her "private life". Article 8 therefore applies.' [44]

Article 8 was used here to support ideas not just of reputation but also the identity of a person and how an adverse portrayal could truly impact reputation as well as privacy. It is worth noting that the court did take a slightly differing approach in A v Norway[45] where it drew attention to the fact that Article 8:

> '…unlike Article 12 of the 1948 Universal Declaration of Human Rights and Article 17 of the 1966 International Covenant on Civil and Political Rights of the United Nations, does not expressly provide for a right to protection against attacks on a person's 'honour and reputation''.

However, even within this case the court further concluded that:[46]

> 'In order for Article 8 to come into play, the attack on personal honour and reputation must attain a certain level of gravity and in a manner causing prejudice to personal enjoyment of the right to respect for private life.'

This case introduced, or re-introduced, some interesting restrictions on the protection of reputation whether as part of privacy or as a stand-alone right. As was seen in Chapter 2, the ability to protect privacy as recognised as a human right led to wider acceptance of how privacy could be defined. Earlier jurisprudence from the ECtHR had included a definition of reputational harm in it finding it included a "right to establish and develop relationships with other human beings and the outside world". [47] This was especially in the emotional field of

[44] n 43 Pfeifer v Austria, para 35

[45] A v Norway, ECtHR (Application no. 28070/06) judgment of 9 April 2009) para 63 Here the applicant claimed his unsuccessful defamation suit against a newspaper was a failure to protect his right to protection of his reputation.

[46] ibid para 64

[47] X v Iceland 6825/74, 1 ,8 May 1976

the development and fulfilment of one's own personality. It is clear that under such inclusion the ability within privacy to protect your reputation or how you are portrayed in society is key. In addition, however, in this case there was a limitation imposed where the right to protect personal honour and reputation must meet a 'threshold of severity' similar to the issue of gravity also required which would be dependent on the specific facts.

Article 8 can therefore be seen to potentially provide for protection of reputation through the scope of privacy.[48] However, despite this, in the case of Lingens v Austria the court held that 'there is… no need in this instance to read Article 10 in the light of Article 8' [49] Lack of consistency in cases had impacted the position , but an acceptance of such interpretation has developed in more recent years.

The more recent case of Radio France v France in 2005 [50] included the right of reputation, within the rights safeguarded by Article 8 of the Convention as an element of the right to respect of private life. In addition, where allegations of defamation were made, there was a greater obligation on journalistic responsibility.[51] This was acceptance of the responsibilities for the content being made available. It seems, however, that the loss of reputation must impact on the individual's private life, as opposed to business life, for this protection to apply.[52]

Within such rights there are key elements; the first being that protection for loss of reputation only applies if the results of specific behaviour would have produced a foreseeable consequence impacting the person's private life.[53] Secondly, the doctrine would also

[48] This has been shown in various cases e.g., Roberts v United Kingdom (2011) 53 EHRR SE23, [40]; Pauliukienė v Lithuania (18310/06, 5 November 2013); Popovski v Former Yugoslav Republic of Macedonia (12316/07, 31 October 2013), [88]

[49] Lingens v Austria (1986) 8 EHRR 407 Para 42 'No doubt Article 10(2) enables the reputation of others - that is to say, of all individuals - to be protected, and this protection extends to politicians too, even when they are not acting in their private capacity; but in such cases the requirements of such protection have to be weighed in relation to the interests of open discussion of political issues'.

[50] Radio France & others v France, (2005) 40 EHRR 706 ('Radio France')

[51] This was subsequently confirmed in the case of Campagna v Romania 2005 4 EHRR 41

[52] n 50 Radio France, para 37. Moreover, a general requirement for journalists systematically and formally to distance themselves from the content of a quotation that might insult or provoke others or damage their reputation is not reconcilable with the press's role of providing information on current events, opinions, and ideas

[53] This was referred to in the NT cases which will be discussed subsequently. Warby J, in considering the claim by NT1 determined, "A person who deliberately conducts himself in a criminal fashion runs the risk of apprehension, prosecution, trial, conviction, and sentence. Publicity for what happens at a trial is the ordinary

presumably operate in a similar method with a defence of truth as can be argued in defamation or libel claims, although the precise nature and limits of such defence remains unclear.

Despite the ECtHR not yet accepting the wider right to be forgotten as such, it has determined specific recent cases on a balancing of interests exercise between privacy and freedom of expression.[54] In addition, it appears that the question of severity of loss of reputation needs to be proven, i.e., the interference with the individual's private life must be serious before the 'right to reputation' is engaged. This, however, would encourage the ability to consider the full impact of the retention of access to personal information as well as its continued availability.

Here, and as debated in Chapter 4, the right to be forgotten could be called upon in the context of pursuing and maintaining a suitable reputation primarily through means of self-determination of how one is portrayed on the Internet, but at what cost? This idea has produced cries of concern that the public interest element, the right to be informed, is at risk due to the development of, and opportunities to enforce, a right to be forgotten. This is whether it occurs under the principles of Google Spain, or perhaps under the more rigid rules of Article 17 of the GDPR, or by acceptance of the right as a wider form of human right used potentially to enforce other human rights such as the right to dignity. If the Snowden revelations bought about many changes to the way the use of data was viewed, without doubt it opened the door to a route for self-determination amidst increased concern over data leaks and privacy violations.

The ability to create a version of yourself through the use of the right to be forgotten has been widely critiqued with concern against the potential loss of freedom of expression to the detriment of public interest. The reality, as seen in the cases explored previously, has been that the use is limited with few decisions taking place under the precedent of Google Spain

consequence of the open justice principle". In similar fashion, the case of Ireland in Townsend v Google [2017] NIQB 81 under the pre-GDPR data protection legislation came to the same conclusion

[54] This was shown in the case of A v Norway, ECtHR (Application no. 28070/06) 9 April 2009

and with mixed outcomes.[55] However following the change in approach by the ECtHR, a recent decision outside of the jurisdiction of the EU bought about an outcome based on the right to be forgotten. In the case of ML and WW v Germany,[56] the ECtHR refused to grant an injunction made previously by the Federal Court of Germany, prohibiting the media from allowing access to information through the internet which revealed details of the applicants' conviction for the murder of a famous actor. As mentioned earlier, the men involved had already tried to stop any publications of this information and their final application was therefore to this court.[57] German law permits courts to suppress the names of convicted criminals from newspapers/media once the convicted individuals have repaid what could be considered their debt to society, however, in this case the circumstances were more extreme with a resultant higher level of public interest.

With the original action being sometime before the Google Spain case, this case did not refer to the right to be forgotten as such which had been determined by the CJEU. In addition, the court did not consider in particular the position with regard to ISPs, making it clear that any interest in the Internet and the status of search engines was purely that these 'merely amplified' the scope for inference with privacy, rather than being the issue itself. It was also clarified that the public had a valid interest in information concerning the crimes, and therefore the media were tasked with ensuring that such information was available. In these discussions there was emphasis on journalistic freedom with its ability within professional ethics to make decisions as to what should be made available, whereas the search engine only provided the links to information and did not make any similar decision. With no other reason to change the decision of the German national court, the hearing was unsuccessful for the convicted killers with public interest overriding their interests, particularly in the context of the seriousness of the crime committed. However, part of the challenge facing the importance of the exercise of any freedom of expression through the media is the change in approach to journalism. Here, particularly in an online environment, freedom of expression and the concept of public interest may be jeopardized by the rise of 'fake news' and bias. If

[55] This lack of consistency is explored in Stefan Kulk, Frederik Zuiderveen Borgesius, 'Freedom of Expression and Right to Be Forgotten Cases in the Netherlands after Google Spain' 2015] EDPL 2/15 p 113
[56] ML & WW v Germany, appl 60798/10 and 65599/10 [2018] ECHR 554
[57] ibid ML & WW v Germany - At the ECtHR it was determined that what would be required was a balancing act between the right of privacy as set out in Art 8 and Art 10 providing for the freedom of expression.

freedom of expression should be considered to outweigh aspects of control over personal information, then it must be that it is for a legitimate purpose and not designed to provide sensationalist journalism or mere gossip. This is particularly illustrated in the Campbell case where despite being famous, the model Naomi Campbell was determined to be entitled to aspects of her private life being kept 'private'. [58] The new role of journalism and the resulting pressures arising from the growth of social media to pursue stories for commercial advantage rather for genuine journalistic purposes is explored by Tom Baldwin.[59] The risk of the development of popular 'fake news' that impacts an individual negatively also complicates the ability to seek removal of such information as this may have been distributed many times often unknown to the individual concerned.

In such circumstances it may be considered that the right to be forgotten would be easier to apply than to argue purely that reputational rights have been breached.[60] This might occur where de-linking to information, likely to provide reputational risk, could be made simply through the Google process or by application to the relevant Data Protection Authority. What is clear, however, is the link between the right to be forgotten and its impact on the protection of reputation, particularly with regard to the involvement of Article 8 of the Convention. The scope of the right must, therefore, be considered in the light of the ability to use informational self determination to achieve not only protection for privacy but for reputation, particularly where seen as vital for how a person has to engage in society or indeed as part of a process of forming the digital persona required.

[58] See Campbell v MGN [2004] UKHL 22

[59] Tom Baldwin, *Alt Control Delete: How Politics and Media crashed our democracy*, (C Hurst and Co 2018)

[60] This approach may be seen as requiring proof of damage sustained, and it is a requirement that this reflects the seriousness of the allegation as well as the effect on the individual. It can be argued that the recent case of *Lachaux* could be considered to have provided a stricter test than that laid down by the Court of Appeal with Strasbourg and domestic law appear to be travelling in the same direction but not at the same speed. see discussion available at https://inform.org/2019/01/10/article-8-and-the-outside-world-privacy-reputation-and-employment-hugh-tomlinson-qc/ This however was overturned at the Supreme Court where the whilst disagreeing with the analysis by the Court of Appeal, the court found for the threshold of seriousness as was found in the cases of Jameel's case 2005 QB 946 and Thornton v Telegraph Media Group Ltd 2011 1 WLR 1985, but requires its application to be determined by reference to the actual facts about its impact not merely the meaning of the words [12].

5.3 The balancing of interests

Notwithstanding the recognition of the roles reputation as well as identity play in establishing the scope of the right to be forgotten, Article 17 of the GDPR provides the mechanism. This enables a request to be made specifically for the erasure of personal data (which would include a de-linking process under the provisions of primarily para a) and para c)). Under the provisions of para a) the data subject could object to the processing of the data on the basis this was no longer necessary. By analogy with the provisions of the DPD, this would be that the information might be out of date or otherwise no longer relevant; as was argued in the case of Senor González in the Google Spain case. However, the ability to remove information that remains true but is no longer relevant would now perhaps be more easily met under Article 17 c) where only if 'the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims' can the rights of an individual be defeated. Recognition that the commercial interest of a search engine and its activities could not override the privacy rights provides a good starting position for defence of not only privacy but also reputation. This then provides for the exercise of informational self-determination to maintain such rights.

Accordingly, the exercise of the right to be forgotten now under Article 17 may provide more practical recourse. However, Ursula Cheer puts forward a possibility where the remedies, in the form of torts, in respect of privacy and defamation as a result of loss of reputation are seen as 'drawing closer together'. [61] This may prejudice the ability to continue with any claims for loss of reputation as there would be competing rights and resultant reluctance from courts to effectively consider twice the outcome from available information.

In looking for guidance as to what personal information may be 'forgotten' under Article 17 and what fundamental rights must be considered, in particular privacy or claims relating to reputation, recent cases have produced diverse results in interpreting these. In a UK case pre-Google Spain involving the reputation claims of a well-known footballer, John Terry,[62] the

[61] Ursula Cheer, *Divining the Dignity Torts*, in (ed) Andrew Kenyon, *Comparative Defamation and Privacy Law*. (CUP 2018)

[62] Terry (previously 'LNS') v Persons Unknown [2010] EWHC 119

importance of looking at Articles 6, 8, and 10 of the ECHR[63] were noted whilst also considering the common law values that needed to be upheld. Mr. Justice Tugendhat stated that the requirements to do so 'relate to open justice, to the right to a fair hearing, to the right to private life and to reputation, and to the right to speak freely.' However, in this case the ability to argue such interests was lost due to the judge finding that the application was more concerned with the loss of reputation[64] which had a commercial value to the footballer, rather than the impact on his family life. This was held to be distinct from any loss of privacy and to which an injunction would have been valuable. The ability to seek action for defamation was also not fully considered in light of the concern expressed that the case was bought for purely financial objectives.

Subsequently, in Italy a specific case took the opportunity to consider the right to be forgotten following Google Spain in connection with the impact on reputation.[65] Again, this involved commercial interests. An Italian entrepreneur, Manni, was concerned that his name, held on a commercial register (not on the Internet) against a dissolved company, generally a legal requirement, should be removed. Under the right to be forgotten principles preceding Article 17, the case did not focus on the personal needs of the claimant but on whether the processing was in accordance with the data protection laws. Manni was apprehensive that the association of his name with such entity would impact his reputation and business life, particularly as new clients would not want to do business with a director of an insolvent company. There was no impact on his privacy directly as all interests here were commercial. However, the fact that the data could be accessed and re-used continually widened the impact, effectively influencing his personal life by linking it to his 'business' reputation. On referral however, the CJEU thought that it would not be correct to permit the deletion of accurate information intended to protect members of the public, and therefore such information should remain. The CJEU made clear that there could be overriding interests limiting access to such data, but it is for the national courts to determine this on a case by

[63] Art 6 The Right to Liberty and Security; Art 8 The Protection of Personal Data; Art 10 Freedom of expression and information

[64] n62 re Terry **'**I think it likely that the nub of the applicant's complaint is to protect [LNS's] reputation, in particular with sponsors, and so (a) that the rule in *Bonnard v Perryman* precludes the grant of an injunction; and (b) in any event damages would be an adequate remedy for LNS.' Tugendhat J, para 123

[65] Camera di Commercio Industria Artigianato e Agricoltura de Lecce v Salvatore Manni, Case C-398/15, [2017] EWHC 119 Para 149 ii

case basis. It was also apparent that the impact on reputation was considered here to be of less importance than the rights of the public to be informed. The proviso was that such information was not mere gossip but correct facts maintained in a public register and also, interestingly, not accessed repeatedly through search engine operations.

Accepting that loss of reputation might be protected under the right to be forgotten, the recognition that the decision in Google Spain could almost immediately impact reputation was not lost on other organizations which could see commercial advantages. There was immediate acknowledgement of the opportunity for a new commercial slant on the ability to manipulate data and, potentially, the way in which a person was viewed. ReputationVIP, calling itself a 'reputation management company', introduced an example of such practice[66] with a service titled "ForgetMe". This was based on the ability to compare and cross-reference the results published by the Google Transparency Report to requests made through ReputationVIP's services which enabled the company to collect and formulate statistics relating to the nature of such requests. Recognizing that the majority of search results went through Google, these generated statistics only occasionally referred to other search engines, such as Bing.[67] This business model for Reputation VIP was, however, to be short-lived, although others would be created. Despite the availability of further analysis with similar, more extensive data and a retrospective report by May in 2018, it announced a closure of its service partly due to the implementation and actions anticipated to be taken under the GDPR.

The links between reputation and private life seem apparent, but in the opinion of Post[68] dignity is inherently private whereas reputation is tied to ideas of society and interaction with it. The ability to protect reputation by defamation actions, even if that protection is limited, can be argued to be maintaining rules of social conduct or order. The relationship of privacy with reputation, however, becomes more entwined in an 'on line' context. To illustrate the

[66] The company no longer has any English outlets but still trades in France. https://www.reputationvip.com/fr/ last accessed 16 March 2018

[67] The initial data from 2014 for ForgetMe, the year of the Google Spain decision showed the infrequency of requests made to Bing. ForgetMe's initial data from 2014 shows Bing receiving fewer than one thousand requests, compared to Google's nearly two hundred thousand, somewhat to Bing's chagrin.

[68] Robert C Post, 'The Social Foundations of Defamation Law; Reputation and the Constitution' [1986] 74 California Law Review p 691

potential importance of this, Canada is taking a proactive approach, putting into place the opportunity to explore and debate the extent of a right to be forgotten.[69] Its primary aim is to focus on the issues faced by an individual where information available online has had a negative effect on their reputation. The initial scope of the paper recognized the conflict where an individual wanted an 'online' presence but was concerned about their reputation, being aware that information was 'not simply posted; it is manipulated, mined and interpreted.'[70] The specific challenges of the Internet are recognized where online information is duplicated and made widely and readily available while it remains challenging, if not impossible, to delete. The placement of certain information also impacts reputation with a focus primarily on higher ranking search results, meaning the action taken in prioritizing information could result in disproportional 'bias'.[71]

There has been a flurry of activity in Canada focusing on the need to manage on-line reputations, taking a difference stance to that of the EU with its concern primarily on privacy. A recent press release by the Office of the Privacy Commissioner of Canada (OPC) suggested that not only was the right to be forgotten required to provide the right to delink inaccurate or out of date information, but it also called for more tools to manage online reputations.[72] Subsequently, this has been followed in 2018 for a proposal for an digital right for Canadians to manage their reputations online, expanding on the cohesion between the two.[73]

Despite there being no express provision of a right to be forgotten, which remains a European approach, the combination of certain provisions in the Personal Information Protection and

[69] Input into the discussion paper prepared and issued in 2015 by the Policy and Research Group of the Privacy Commissioners of Canada closes in 2020. available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/pos_or_201801/

[70] It was noted that despite being selective about postings of information there was little control over what others posted or how personal information might be interpreted by users. This followed the notorious reporting of how people had been affected by what had seemed at the time to be innocuous postings of parties.

[71] Also within this paper, there was acknowledgement of consent not being a requirement of each posting and concern as to how this could be addressed.

[72] Press Release October 10, 2018 Privacy Commissioner seeks Federal Court determination on key issue for Canadians' online reputation available at: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180126/ last accessed Dec 2020

[73] This was contained in the published draft OPC position on online reputation available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/pos _or_201801/

Electronic Documents Act (PIPEDA), [74] such as an obligation on corporates to only use accurate information and the right for Canadians to challenge such accuracy, can become the equivalent right to have information de-linked.[75] Despite recognition that freedom of expression is specifically protected in Canada, there has been clear acceptance of the need to protect reputation, particularly in respect of younger people and how they are portrayed. The debate has been vigorous with focus often on competing rights, primarily privacy and freedom of expression, as part of the equation. This is however, a clear example of the recognition that the right to be forgotten or the ability to use it to exercise informational self-determination can be linked with the impact on reputation. The level of such impact can be seen in historic instances where behaviour recorded online may prejudice employment or social opportunities, as was shown in the Stacey Synder case.[76] An opportunity to manage your portrayal online can have a lasting impact.

5.4 The link between the right to be forgotten and rehabilitation: where does the right to be forgotten add more scope?

Part of recognition of the value of reputation and the impact that an adverse portrayal of an individual can have on their ability to enjoy many of the rights accorded to them is the realization that past events can dramatically impact your ability to live a good life. This has been exaggerated by the use of the Internet and particularly social media. An example of the level of impact can be seen clearly within concepts of rehabilitation. The availability of information can impact rehabilitation seen not only in the UK under the Rehabilitation of Offenders Act 1974 but also in other EU national states, such as France, Germany, and Belgium.[77] In fact, it was noted that Ireland was one of the only countries in the EU not to have a similar law and this was remedied by its introduction of the Criminal Justice (Spent

[74] Personal Information Protection and Electronic Documents Act 2000 CAN/CSA-Q830-96 (PIPEDA) available at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

[75] This has followed the early discussions and is considered to give the citizens a right to ask for de-linking when there is information accessible which might be inaccurate, incomplete, or out of date, this has also been interpreted to include any defamatory content.

[76] Stacey Snyder v Millersville University & Others, in The United States District Court for The Eastern District Of Pennsylvania, Dec 3, 2008 No. 07-1660

[77] Reflecting this in Olivier G v Le Soir (29 April 2016), n° C.15.0052.F, the Belgian Court of Cassation ordered that under the right to be forgotten a newspaper had correctly anonymised the name of a drunk driver whose crime had been subject to a "rehabilitation decision" on 23 November 2006, more than 10 years after the crime.

Convictions and Certain Disclosures) Act 2016.[78] This reflects acceptance of a global trend towards rehabilitation.[79] Both jurisdictions have had recent cases which have bought into play not only the right to be forgotten in one form or another but also challenged where this can fit with the availability of information through the Internet which opens up even spent convictions i.e., convictions which legal systems have determined should no longer be publicly available. If this concept of rehabilitation is a cornerstone of society,[80] so that everyone has the opportunity to 'repent' their sins and be forgiven through legislation designed to promote rehabilitation by the removal or forgetting of spent convictions, then how does the revelation of such crimes, which are no longer made accessible to potential employers or funders, benefit society?[81] In addition there are arguments that within continental civil law based jurisdictions there is recognition that rights of privacy and dignity can be used to prevent disclosure of criminal records in the absence of any clear public interest to do so.

The approach in Europe can vary[82] but in many other countries, even the US,[83] the intention is still the same; that offenders be given opportunities to reform and continue a different life without the stigma of previous 'spent' convictions being continuously available. For many individuals, the ability to have control of information to be able to exercise self-determination in a way that can change their future within their community must be vital.

[78] see TJ McIntyre, Ian O'Donnell, "Criminals, Data Protection and the Right to a Second Chance" (2017) 58 Irish Jurist (ns) 27. The authors' analysis of the circumstances leading to the new act argue that this was largely based on the UK's Rehabilitation Of Offenders Act 1974

[79] This is illustrated by the position taken at the 13th United Nations of Crime Prevention and Criminal Justice where the Doha Declaration adopted supporting measures to provide for rehabilitation and social re-integration. Resolution 1 para 4 (j) 'To implement and enhance policies for prison inmates that focus on education, work, medical care, rehabilitation, social reintegration and the prevention of recidivism, ….'

[80] As was seen in earlier forms of rights allowing for the forgetting of information as set out in Ch 2

[81] For clarity this could not be considered to include crimes of a nature where public interest would always override them being 'forgotten', such as extreme violence, murder, and sexual crimes

[82] see Sunita Mason, 'A Balanced View – Independent Assessment Safeguarding the public through the fair and proportionate use of accurate criminal record information', March 2010, In this Appendix D sets out a comparison of the various legislation of the rehabilitation of offenders within the European States, available at https://webarchive.nationalarchives.gov.uk/20100408141053/http://police.homeoffice.gov.uk/publications/about-us/ind-review-crim/a-balanced-approach-12835.pdf?view=Binary last accessed 25 April 2019

[83] Unlike many European states the US does not have a federal law with the concept of 'spent convictions'. A state will have different laws regarding crimes that can be expunged or sealed which effectively means these are not immediately disclosable. A person may qualify for expungement in one state but not in another, even for the same crime.

The European attitude towards rehabilitation, looking at the focus on 'labelling' of individuals with criminal pasts and thereby stigmatizing them, regards social integration as fundamentally more important than retaining information about past misdemeanors. An example of this could be seen in Norway where, in 1985, a leading case looked at default removal for any references to suspected, accused, or convicted persons after seven years; with the proviso that if the subject was an occupier of a public or professional position this would not apply. The case was of particular interest as it involved an early example of the impact of digital records creating electronic means of holding old data which were becoming increasingly widespread.

This is in contrast to the approach adopted by the US which prefers openness and accessibility of criminal records whatever the consequences for the individuals. Prioritizing ideas of free speech and open government principles justifies public disclosure of criminal records whatever the consequences to reputation. Such division of approach is, of course, more complicated in global societies where even criminal records, particularly for specific offences, can be made available even outside jurisdictions.[84]

An illustration as to how readily available such information is to the public was shown in the case of Google Spain as it related to a bankruptcy order. This was also shown in the more recent cases of NT1 and NT2, cases with past criminal convictions.[85] In these joined UK cases the information should have no longer been readily available as the convictions had been 'spent' under the relevant legislation,[86] which provided for the rehabilitation of offenders. With formal rights over data originally contained in the DPD[87] now contained in the GDPR, the scope of the right to be forgotten could be considered to be wider than before and more concerned with accessibility of information and its ability to shape the public perception of a person. The fact that the Internet could be an accessory in the loss of reputation through the impact of making available such matters as spent convictions has become only too clear. A

[84] For example, consider terrorism and sexual offences.
[85] NT1 & NT 2 v Google LLC [2018] EWHC 799 (QB)
[86] Rehabilitation of Offenders Act 1974 c 53
[87] See Article 12 (b) 'as appropriate the rectification, erasure, or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;'

slow realisation as to the cost not just to privacy but to reputation and the ability to determine how you live your life without the baggage of past events is being reflected in changing approaches to privacy.

5.5 Changing attitudes to and expectations of privacy; their impact on the need for the right to be forgotten and reputation

The environment in which the right to be forgotten was created has changed in the short period of time since the Google Spain decision. As discussed in Chapter 2, a clear definition of privacy has been difficult to determine but in recent years there has been a change in response to the established ideas of privacy. Prompted by the use of the Internet this led to the initial reaction by the Internet giants declaring that privacy is dead.[88] This is the environment where a right to be forgotten has been utilised however as a response to a desire to maintain privacy, evoking both dignity and autonomy whilst adding concerns of reputation and identity.

With growing awareness of the depth of personal data being held and often the lack of transparency with regard to its use, together with the growing power of the Internet giants (which will be discussed in Chapter 6), the previous notions of the inevitability of data being made available as the price to be paid for the use of various internet services has begun to change. This is developing into an uneasiness over the casualness with which personal data is collected, processed and used with the resultant impact on privacy.

5.5.1 A change in approach to privacy in respect of personal data

In line with this unease, the impact of recent revelations of misuse of personal data and the consequences of such misuse could be seen to be initiating such change. In June 2013, a former NSA contractor, Edward Snowden, revealed to journalists that the US Government, through various of its agencies, had collected on a massive scale information from both US and other national citizens.[89] This was found to be part of a programme called PRISM which

[88] In 2000, Scott McNealy, CEO of Sun Microsystems, made a pronouncement that struck a chord with all who live and work in the internet-connected world. He stated, 'Privacy is dead—get over it'.

[89] In early June 2013 Edward Snowden revealed thousands of classified NSA documents to journalists Glenn Greenwald, Laura Poitras, and Ewen MacAskill, bringing the revelations initially to newspapers the Guardian and the Washington Post. These were also reported globally through news channels such as the BBC,

involved the collection of user data from nine US technology companies compelled to provide records to the US government. The concern raised focused on the potential ability for such actions to have destroyed the integrity, or purported integrity, of the Internet as the advocate of free speech[90]. The response was seen as a result of the unforeseen surveillance, and the impact of the revelations highlighted the potential loss of privacy and data control. This created a greater level of concern with the beginning of a global unease with regard to access, control, and potential manipulation of data. Despite the lack of connection with Google Spain, this was a real indicator of a global change of approach to the accessibility of data. With it came increasing apprehension, not just with regard to privacy but acknowledging how a lack of control over personal data could have such an impact on individuals.

Concern as to privacy and control of data arising from the Snowden leaks[91] led to the mission by Max Schrems [92] to reveal the access and misuse of data largely collected by Internet giants. An enterprising law student, Schrems saw the misuse of data collected from Europe and held in the US under the provisions of the Safe Harbour agreement. Entered into between the US and the EU, this agreement ensured that processing of data would be made in accordance with the principles of the EU data protection laws. Non-compliance with this arrangement led Schrems to take the opportunity to challenge Facebook in connection with the retention and accessibility of his data in the US, ultimately bringing to an end the Safe Harbour agreement.[93] This highlighted the assumption that data would be processed fairly. Despite a degree of complacency by social media users, there has been increased caution with the sowing of seeds blossoming into awareness that the privileges of privacy and data control to ensure dignity and ultimately reputation really do matter.

The Snowden Revelations available at https://www.bbc.co.uk/news/world-us-canada-23123964 last accessed 7 May 2019

[90] What also came to light was the apprehension felt by US citizens in respect of the Fourth Amendment which enabled 'the right of people to be secure in their persons, houses, papers and effects…' Under this the law provides that information that is shared with third parties may be collected where the data subject has 'no reasonable expectation of privacy' in the information. This re-introduced privacy being concerned directly with the control and accessibility of personal data.

[91] see n89

[92] Schrems v Data Protection Commissioner Joined Part Digital Rights Ireland Ltd, ECLI:EU:C:2015:650

[93] See press announcement in connection with the ending of the Safe Harbour agreement and the new Privacy Shield, 'EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield' Feb 2016 https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216 last accessed 22 Feb 2021

The new dimensions of the impact of information being placed and made instantly accessible through the Internet specifically, is viewed a game changer by Solove in terms of looking at how privacy as well as reputation have become re-defined with the availability of data. [94]
As the impact of the volume of data grew it became an early indicator that privacy could not yet be considered dead. Users could see and argue that there should be a limit to such availability and accessibility as was shown with Facebook Newsfeed.[95] This product evoked a swift response to the increased obtainability of personal information, resulting in it being withdrawn.[96]. Solove's view is that such outcries were not just a reaction to new information being made accessible as it was already largely posted voluntarily on users' profiles, rather the real issue was the increased availability of such personal data. The premise had been widely accepted that there is limited concern by users as to privacy, who were becoming complacent about the airing of personal details and social activities with seemingly no area considered so 'private' as not to be shared. Here the response to Newsfeed was not only collective but in the words of Solove 'vehement.' [97] Was this then about 'control' or was the sharing of this information increasingly outside the users' ideas of what should be considered private and therefore not accessible to all with the subsequent impact on how a person is perceived. If there is no right providing informational self-determination, i.e., the ability to filter the data being made available, would recognition of this cause users to stop and consider the impact on their privacy more deeply. Photos posted in various drunken moments had a way of turning up with often devastating consequences.[98]

If commentators spoke of 2018 as the year of data protection with the introduction of the GDPR, then 2019 could be called the year of privacy. Despite the lack of clear definition and wide acceptance of this right and the belief, largely unchallenged, that privacy was a casualty

[94] Daniel Solove, *Speech, Privacy and Reputation on the Internet*, in S. Levmore, M. C. Nussbaum, (eds.) *The Offensive Internet*. (Harvard University Press 2010) pp.19-21.
[95] For example, Facebook launched its service Newsfeed in 2006 which provided alerts on when friends and potentially friends of friends of a Facebook user were loading information. This clearly resulted in a lack of control over who gained access to such data with an immense volume of information being loaded https://www.facebook.com/facebookmedia/solutions/news-feed last accessed 20 Oct 2019
[96] A group created called 'Students against Facebook News Feeds,' was able to challenge the service ensuring that such activities were swiftly curtailed by Facebook https://www.google.com/search?client=firefox-b-d&q=%E2%80%98Students+against+Facebook+News+Feeds%E2%80%99+ last accessed 30 April 2019
[97] see n94 p21
[98] E.g the case of Stacey Snyder see n76

of the digital era,[99] it appears key to the concept of privacy that there is more control within the sphere of data. Ideas expressed particularly by Mark Zuckerberg, the voice of Facebook, are long gone with the promotion of privacy now firmly on the agenda.[100] A lack of privacy, increased access to data and therefore a loss of ability to determine how you are portrayed mixed with a desire for control through informational self-determination means there is much greater understanding of the issues.[101]

In the US, the existing stance on privacy has been challenged by the implementation of the European GDPR, seen as an enormous step forward in giving EU citizens greater rights over their data, and therefore in most people's minds over their privacy. Despite the outcry over the ability of the EU to impose restrictions on US citizens through the GDPR's impact on entities carrying out business within the member states, this has raised increasing calls for new protection over data. [102] Limited attempts had been made to bring about change in the US.[103] More recently there have been increasing calls for Google itself to provide a similar right to the right to be forgotten process, arguing this should be available as part of Google's offering rather than as a result of EU law.[104]

---

[99] Scott Mc Nealy former CEO Sun Microsystems 1999 stated; 'You have zero privacy anyway, get over it'

[100] The new Apple strap line for 'Privacy; Is that iPhone?' is reflective of the change in approach. The surprising element of this development is the public promotion by the leaders of internet giants expressing their new views that privacy matters. Tim Cook of Apple seems to have become the most unlikely advocate for the protection of privacy. Insert link to 2018 conference ref to media responses etc.

[101] 'Debating Ethics, Dignity and Respect in Data Driven Life', 40th International Conference of Data Protection and Privacy Commissioners, October 2018 available at https://www.privacyconference2018.org/en/40th-international-conference-data-protection-privacy-commissioners.html

[102] See GDPR Compliance Checklist for US companies, https://gdpr.eu/compliance-checklist-us-companies

[103] California could now be seen as an innovator in developing its own version of privacy laws. Arguments appear to have reached Washington as reported by Solove with new moves afoot. Despite such actions Solove is hesitant to say that a new Federal law is due, recognizing the size of debate around data and privacy in the US and the need to define and produce clear understanding of the concepts to provide such a law. However, he accepts that routes to provide similar remedies are urgent, citing the California Consumer Privacy Act as an example of innovative legislation providing good results. Solove's view is that the CCPA came into being because US policymakers considered they had less than adequate solutions to privacy problems. It was more common for there to be arguments dismissing concerns as irrational due to the so-called "privacy paradox" where people indicate they want privacy but are prepared to provide personal data freely. However, in California, the public, through certain interested persons, confirmed a true desire for a form of privacy. The referendum ultimately approving the CCPA received 629,000 signatures in favour.

[104] 74% of US citizens would like the right to remove certain personal information from the Internet and call for new rights from Google. This ranged from embarrassing photos (which was 85%) to data collected in connection with law enforcement (which was only 39%). See; https://www.pewresearch.org/fact-tank/2020/01/27/most-americans-support-right-to-have-some-personal-info-removed-from-online-searches/

The response is by no means universal within the US, but that debate is happening with new laws being promoted demonstrates the momentum in the change of approach.[105] The ability to argue for a right to be forgotten which could provide informational self-determination relies on recognition that the misuse of personal data impacts privacy and the right is therefore fundamental to protecting the way you are seen or portrayed. [106]

5.5.2 The UK's approach

Some decisions in the UK legal system have also recently challenged the accepted view of privacy, introducing ideas revolving around how people are perceived and, in particular, their reputation. Although not directly connected with an application under the right to be forgotten, such cases have shown a twist in the approach towards privacy taking a form of moral stance, specifically with regard to reputation which would be shown in later decision on the right to be forgotten. Richards v British Broadcasting Corporation illustrated the approach the UK courts were prepared to take to protect the dignity of a man seen as worth a good reputation. Arising out of an increased interest not only by the police and prosecution service but by the general public in historic sex crimes, the performer Sir Cliff Richard was the subject of highly publicized investigations. After being subjected to a BBC televised record of the police searching his home, the singer made claims against the BBC and other media outlets in connection with privacy and protection of his reputation.[107] Sir Cliff Richard's reputation was not only based on being a well-known entertainer over many decades but also as a 'committed Christian,' one known for his very public participation in his religion. In the case the judge was asked to determine if an individual's right of privacy was such so as to stop

[105] The CCPA amendments regarding the deletion of personal information came into effect on January 1, 2020. This provides for additional remedies such as the right to request disclosure of personal information collected and uses thereof (Civil Code s 1798.110(a)); the right to request deletion of personal information collected by the covered business (Civil Code ss 1798.105(a) and (c)); and the right to receive that information from the covered business (Civil Code s1798.100(d)). Generally, the nearest to a right to be forgotten within the US is found at the New York Assembly which has produced a bill with an American version of the right. The Bill, A05323 is "An act to amend the civil rights law and the civil practice law and rules, in relation to creating the right to be forgotten act," However, although introduced in 2018 there is no confirmation of it yet being passed.

[106] Alongside such recognition of such rights is an increased development of 'Surveillance Capitalism' where, in pursuit of commercial benefits, individuals are now targeted to provide more and more information. See Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power* (Profile Books 2019)

[107] Sir Cliff Richard OBE v British Broadcasting Corporation and another [2018] EWHC 1837 (ch)

the police investigating in conjunction with media reporting.[108] Here, it was frequently noted by Judge Mann that the reputation of Sir Cliff was as 'a good and committed Christian' something that portrayed him as an upright member of society. [109] The stance taken appeared to be that a 'good' man should be offered increased protection for his privacy and that his valuable reputation in both his private and public roles should be maintained.

This stance was a moral justification for the protection of privacy and reputation and was echoed in a further case in the UK which did involve the right to be forgotten. The joined cases of NT1 and NT2, as discussed earlier, were based on the right to be forgotten as determined under the principles of the Google Spain case. [110] The joined cases had mixed decisions, but both claimants had benefitted from the decision of the court to grant anonymity.[111] This ensured that reputational risk was realistically less than was the case in other highly publicized cases. In this instance, although brief facts of the individuals were released, it appeared even the Internet could not reveal their identities. It was clear that where NT1's claim was unsuccessful, his behaviour was an important factor in the judgement, i.e., the judge did not believe NT1 had shown remorse nor that he had come over as a credible witness. Even though his claim for privacy had some merits with NT1's reputation clearly tarnished by details of his spent conviction being made available, this was insufficient to persuade Mr. Justice Warby that the claim should be successful. The judge was scathing in finding that the claimant's level of concern was more in relation to not being able to carry out further business activities than to his private life or even reputation. There was also consideration given to NT1 still being a public figure, albeit in a minor role and certainly not a household name as was shown in other cases. Warby referred[112] to the checklist contained in the Guidelines issued by the Art 29 Working Party for factors that should be considered by data protection authorities in determining whether search results should be delisted. Here, as the Guidelines referred to 'business people' as being 'public figures,' Warby was able to use this with regard to the decision on NT1. This provision had not been fully covered in

[108] The depth of the reporting was considered generally to be extreme particularly as a helicopter was commissioned by the BBC to carry out overhead reporting.

[109] see n 107 p 2 para 7, the judge was generally considered to have taken a very moral approach in determining the case. It was reported that there was mention at least 17 times of the fact the claimant was not only considered a national treasure but 'known of his publicly stated Christian beliefs.'

[110] As discussed in Chapter 4

[111] Joined cases NT1 & NT 2 v Google LLC [2018] EWHC 799 (QB)

[112] ibid para 161

Google Spain despite Gonzalez also being a business man, so it is difficult to see how categorizing individuals in such a way could increase or lessen their ability to control data pertaining to them, or indeed have such data 'forgotten.' Whilst considering the impact on NT1's family life, this became more relevant as without a young family to protect his ability to carry out business or not was not considered to outweigh public interest or the right of freedom of expression when balanced with privacy. The situation differed with NT2 who, with a young family and a more reticent and remorseful approach, was able to have the balance with regard to privacy tipped in his favour.

The unique character of the Internet and its ability to influence privacy, to broadcast information and create the potential for how you are perceived by society was also explored in the intriguing PJS case in the UK. Whilst not directly concerned with the right to be forgotten it looked at privacy, freedom of expression, and reputation as well as introducing the idea of how one can be portrayed at different times during one's life. It also raised interesting questions of law when an application was made for an injunction to stop media coverage primarily of sexual exploits of the partner of a worldwide famous singer/artist. This also revealed a pattern of behaviour by the partners with regard to relationships. The injunction was specifically aimed at a proposed publication in a leading newspaper in January 2016. [113] Refusal at first instance was subsequently granted by the Court of Appeal.[114] However, by April details of the persons involved were widely published[115] in an American journal as well as in Canada, Australia, and Scotland, making what many believed to be a mockery of the original injunction with easy access to the information through the Internet outside of the UK. On this basis, News Group Newspapers Limited returned to the Court of Appeal to ask for the injunction to be set aside. The Supreme Court[116] took a different view. Accepting that the injunction could only provide an interim solution,[117] it determined that this

[113] Here the newspaper was 'The Sun on Sunday'
[114] PJS v News Group Newpapers Limited [2016] EWCA Civ 393
[115] This included details of the activities and identities of those involved
[116] Following the Court of Appeal's decision to discharge the injunction, and on subsequent appeal by PJS
[117] n 114, PJS v News Group Newspapers Limited. It was noted that in the previous action, 'The Court of Appeal noted that the appellant's solicitors have been assiduous in monitoring the internet and taking steps, wherever possible, to secure removal of offending information from URLs and web pages, but concluded that this was a hopeless task: the same information continued to reappear in new places, and tweets and other forms of social networking also ensured its free circulation'

should continue until the trial of the application focusing primarily on the protection required for the privacy of the two children of the public figures. At the Supreme Court, Lord Mance in considering the issues at stake made it very clear that there was:

> '… no public interest (however much it may be of interest to some members of the public) in publishing kiss-and-tell stories or criticisms of private sexual conduct, simply because the persons involved are well-known.'

The case, once the details of the famous singer were known, albeit through alternative means of access, took on a more interesting slant. Within the claims, arguments were made that he had re-established himself as someone now seen as a 'family man' and part of a close integrated family unit, thus there should be no public interest in any arrangement he and his partner made with regard to their sexual relationship.[118] The question around the new public profile of the claimants was considered in a judgment given by Jackson LJ, when the Court of Appeal allowed PJS's appeal. Within this was a review of the balancing act required with regard to privacy and freedom of expression. In the first instance, Cranston J identified the children of PJS i.e., his family as a key factor in such a balancing exercise, however, he failed to expand on how such rights had been considered in his decision.

Before the Supreme Court it was, however, made clear that the main consideration of the case was the weighing up of the interests under Articles 8 and 10 of the Charter of Fundamental Rights of the European Union.[119] Despite the principles under the right to be forgotten not being followed as such, it was apparent that similar criteria were being taken into account in determining the availability of information and the impact of this on how those involved were perceived.

The discussions on the merits of injunctions in a world where a button could access information, if not locally but globally, looked again at the role of the Internet in the mass

[118] n 114, the PJS case, on their evidence, the claimant and YMA were considered a committed couple with the occasional sexual encounters with others not detracting from this. Accordingly, "a bundle of press articles showing the claimant and YMA's commitment to each other does not present a false image requiring correction". Lord Justice Jackson para 51

[119] The Charter of Fundamental Rights of the European Union [2000] OJ C 364/1

dissemination of information. The claim by PJS could be considered to be evoking a right to be forgotten in a different guise by trying also to change his public persona. The view of Lord Neuberger [120] made it clear this might be a way to re–invent or even re-confirm how the claimant was perceived by the public after years of what might be considered wild and very public behaviour.[121] There was some recognition given to the additional risks of information being made through the Internet, and therefore the right to be forgotten being by comparison a similar remedy to that being sought. Despite there not being the same focus of data protection per se in the opinion of Lord Mance, the situation created a new need for a result 'when the case law establishes that neither Articles 8 nor 10 has preference over the other, and what is necessary is an intense focus on the comparative rights being claimed in the individual case'.[122]

This was a significant case not just because of the media reaction that freedom of expression and public interest had been compromised by the non-availability of information, but there was further recognition on how access to personal lives and information had changed perceptions of individuals so that in the words of Neuberger, 'I also accept that, as many commentators have said, that the internet and other electronic developments are likely to change our perceptions of privacy as well as other matters and may already be doing so'.[123]

[120] n114 in the PJS case Lord Neuberger stated in para 63, 'It might be said that PJS and YMA could ask the search engine operators to remove any links to the story pursuant to the decision of the Court of Justice in Google Spain SL v Agencia Española de Protecciónde Datos (Case C-131/12) [2014] QB 1022, but it seems unlikely that the reasoning in that case could apply to a story which has only recently become public and is being currently covered in the newspapers'. Lord Neuberger.

[121] It is, however, interesting to note that sometime later the availability of the information is such that even Wikimedia (published in the UK) makes note of one of the parties being David Furnish, so presumably there was sufficient public interest to make it worth the risk to publish such information. Wikipedia quoted, 'The case was the first time that the Supreme Court of the United Kingdom ruled on an issue related to privacy and the right to freedom of speech and was described as creating a de facto privacy law which would make it difficult for UK newspapers to publish future "kiss and tell" stories, by virtue of placing privacy above the public's right to know' available at https://en.wikipedia.org/wiki/PJS_v_News_Group_Newspapers_Ltd . In addition, media lawyer David Engel was widely reported as describing the ruling as making a distinction between the concepts of confidentiality and privacy, "... has made the practical point that even where people may be able to find the information online, that is qualitatively different - in terms of the distress and damage caused to the victim - from having the story plastered across the front pages of the tabloids". https://www.bbc.co.uk/news/uk-36329818

[122] n114 Lord Mance, para 33

[123] n114 Lord Mance, para 70

Comparing the breach of privacy with ideas of reputation and looking at the PJS case, Emily Dent, director at Rampart PR a reputation management agency, commented:

> If PJS was advised to take out this injunction to protect their reputation then perhaps, with hindsight, this wasn't altogether the best advice. The injunction has fuelled the flames of interest in the story. What's more, the media don't like to be gagged: their response is unlikely to be kind. It could be argued that the story has become more 'juicy' as a result of the case. [124]

This is where the benefits of claiming anonymity were also complex. There was, of course, a frenzy of attempts to identify the individuals behind the case, leading to the situation where an alternative search, perhaps access from another country, immediately provided details of the case. However, in some ways the point of the case highlighted the fact that the injunction would have a purpose even if only on a local basis and that everyone, even public figures, deserves the right to claim a degree of privacy (as was also seen in the leading case of Campbell).[125] What was interesting were the observations made by Lord Manse that exceptions, albeit limited, may take place if there is a need to remedy an impression created by the individual but which was misleading the public. [126] This would be the case even if there was a suggestion of abuse of public office although neither had applied in this case. [127] Similar application must surely apply in any exercise of the wider scope of a right to be forgotten where not only the balancing act between the rights of privacy and freedom of expression need to be applied, but also consideration perhaps of the overall impact of how a person is perceived.

If the idea that even a public person is entitled to a degree of privacy has gained acceptance,[128] then clearly the next step would be to safeguard his/her reputation as far as

[124] https://www.prweek.com/article/1395613/pjs-victory-privacy-case-study-reputation-management
[125] Campbell v MGN [2004] UKHL
[126] n 114 Lord Manse referring to Cranston J's decision at first instance para 14.
[127] As reported by Taylor Wessing available at https://united-kingdom.taylorwessing.com/en/news/supreme-court-upholds-pjs-celebrity-privacy-injunction-until-trial
[128] Despite the approach taken by the US there is now increasing desire that even high-profile individuals can seek privacy and more actions are being taken in order to protect them from media attention.

possible. This could, of course, have an impact on not only the ability to make a livelihood but on future career potential. The importance of how you are perceived is, for many, also related to the ability to be able to maintain dignity, considered an underlying human right.[129] Where the interplay between such rights becomes more complex, the concept of dignity is involved as well as ideas of autonomy used to promote self-development and ultimately respect. These provide the potential to develop relationships within a functioning society.[130] However challenges arise when considering the impact of a loss of reputation as a result of private events being made public. Within this are views on whether the impact of loss of privacy and ultimately reputation on public figures must, by nature of their chosen roles, be justified.[131]

5.6 The right to be forgotten and the link to defamation

As can be seen by the PJS case, and other instances referred to previously, the right to be forgotten principles[132] as applied in a balancing act to protect an individual can be applied to other forms of recourse to potentially achieve similar protection. This includes actions for defamation, for example as provided under the UK's Defamation Act 2013.[133] Within the legislation covering slander and libel, libel is perhaps the most relevant in an era of permanent or lasting 'publications' available through the Internet, again highlighting the new accessibility and permanency of information held. This Act has been designed to take into effect specific provisions of the Human Rights Act 1998[134] which implemented Article 8 of the European Convention on Human Rights.[135] The Electronic Commerce (EC Directive) Regulations 2002[136]

---

[129] The Universal Declaration of Human Rights 1948 enshrines human dignity in its preamble: 'Whereas recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world'. See https://www.un.org/en/universal-declaration-human-rights/

[130] Charles Fried, 'Privacy,' Yale Law Journal, (1968) 475- 493 David Miller, 'Do Politicians and other public figures have (moral) rights which can be asserted against the media', (1996) UCCL Jurisprudence Review, 152, 157

[131] The arguments can be based on the fact that politicians and other holders of public office choose to enter the public realm voluntarily often with the impact of their activities being subject to a greater level of scrutiny. See Lara Sun, 'Draw a Line between Freedom of Speech and Privacy of Public Figures Humanity, 2013, p 41 available at https://novaojs.newcastle.edu.au/hass/index.php/humanity/article/view/36/36 This is not a new argument as can be seen in J Skell Wright, 'Defamation Privacy and the Public's right to know: A national problem and a new approach' Texas Law Review, 46, 1968.

[132] As established in Google Spain and now set out within Article 17 of the GDPR

[133] Defamation Act 2013 c26 which replaces in part the Defamation Act 1996.

[134] Human Rights Act 1998 c42

[135] European Convention on Human Rights 1950, as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, and 13

[136] SI 2002/2013

can also be relevant with regard to cases involving claims of online defamation. Here, once again, the position of search engines can be considered to be protected and so, unlike under the right to be forgotten, there is the option for a search engine to claim protection under the Regulations as innocent 'disseminators' of defamatory material, i.e., where this is placed on the Internet by search engines.[137]

Generally speaking, a statement is not defamatory unless its publication has caused or is likely to cause 'serious harm' to the reputation of the claimant.[138] However, very recently the UK Supreme Court in Lachaux v Independent Print Ltd and another considered that the Defamation Act 2013, Section 1, raised the threshold of 'seriousness.' This looked at the meaning as established in case law before the implementation of the Act, but it also required its application to be determined by reference to the actual facts about the impact of , not just the meaning of the words.[139] The Supreme Court's judgment restored the enhanced threshold of seriousness for the defamation claims as was intended by Parliament and welcomed by publishers faced with an increasing number of claims of defamation. With a number of preliminary issue trials having to take place until the impact of the judgment is tested in individual cases, the remedy is still a more limited response. Here, the right to be forgotten could be considered an alternative once the full scope of the right can be established to provide the use of informational self-determination to protect reputation.

[137] GDPR Art 17 (1) Where an information society service is provided which consists of the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network, the service provider (if he otherwise would) shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that transmission where the service provider:
(a) did not initiate the transmission;
(b) did not select the receiver of the transmission; and
(c) did not select or modify the information contained in the transmission.

[138] DA, s 1(1) 2013. A number of pre-2013 authorities decided that it was necessary for a "threshold of seriousness" to be reached before a statement would be considered defamatory. Tugendhat J stated in Thornton v Telegraph Media Group Ltd [2010] EWHC 1414 (QB)) that a publication was defamatory of a person where it "substantially affects" the attitude of others towards that person. The purpose of the threshold of seriousness was to avoid the courts being troubled with complaints of a trivial nature that did not truly engage rights of reputation, for example, where the publication was of limited extent or was in the nature of abuse or tittle-tattle.

[139] This applies in circumstances where the meaning and context of a publication are not sufficient for serious harm to be inferred, and to avoid a claim being struck out it would be necessary for claimants to seek to establish on the facts that serious harm has been or is likely to be caused.

Liability of search engines and other ISPs with regard to defamation was also considered in Metropolitan International Schools Ltd v Designtechnica Corp. [140] This case provided authority that the operators of online search engines (such as Google) were not to be treated as publishers of defamatory statements or 'snippets' that appeared automatically in lists of search results even where the search engine operator has knowledge of the defamatory material. The High Court decided that the search engine operator (Google Inc) had no controlling role in deciding the search terms and had merely facilitated the provision of the defamatory wording via its search engine service. However, the position could be different for an operator which has stored or is a host of material. Bunt v Tilley[141] had determined a test for a person to be held responsible for a defamatory publication; accordingly, there must be a knowing involvement in the process of publication of the relevant words not merely a passive instrumental role in the process. This must, however, be challenged by the newer responsibilities found in Google Spain for a search engine to be required to implement the right to be forgotten.

Other forms of recourse outside of the right to be forgotten for defamation or impact to reputation can be for malicious falsehood, breach of confidence, misuse of private information, harassment, as well as breach of data protection laws. If, however, reputation cannot be protected by various laws as outlined above, how would a right to be forgotten help? Was Senor González really trying to protect the use of his data? Or was he claiming the fact that the publishing of such data in the search results had affected his reputation so that he was no longer seen as a responsible member of society with an established career, but rather as someone who had so ill managed his affairs to the extent that he was declared bankrupt with the resultant impact on such matters as being able to obtain credit. This had left him with fewer alternative remedies partly because the information relied on was correct. The ability to be able to erase or forget information then offered him a lifeline in protecting his reputation which defamation, and other associated remedies, could not. It also provided Senor González with the option of removing specific links to personal data providing him with informational self-determination.

[140] Metropolitan International Schools Ltd v (1) Designtechnica Corporation (2) Google UK Ltd & (3) Google Inc [2009] EWHC 1765 (QB); [2009] EMLR 27
[141] Bunt v Tilley [2006] EWHC 407 (QB)

The line between the right to be forgotten and actions for reputation can be blurred. In the NT1 and NT2 joined cases,[142] Mr. Justice Warby highlighted Google's claims when defending its right to refuse to de-link information arguing that the cases bought by the claimants under the right to be forgotten were in fact an abuse of the court's process as these were effectively claims for 'damage to reputation'. Therefore, the claimants had no right to attempt to bypass the protection given under the law on defamation. Google argued that if the claimants were concerned about their reputation, they should seek remedies under defamation laws, as opposed to the right to be forgotten, to ensure freedom of expression was not compromised. Mr. Justice Warby, after considering case law, noted that 'protection of reputation is a significant and substantial element of NT1's claim', referring to the claimant's submissions that he felt like a 'pariah', referring to this 'as classic language of reputational harm'.[143] However, he further remarked that it would be wrong to distinguish between the protection of reputation and private life, emphasizing case law authorities[144] showing that damage to reputation could also be considered under Article 8 of the European Convention on Human Rights.[145] Mr. Justice Warby indicated that the case was based on issues that went beyond 'mere reputation', crossing over into areas of private life which were different issues to reputation, so the claimants were instead correctly relying on the new law of the right to be forgotten as set out under the Google Spain case. The claims by Google were dismissed on the basis that the claimants had not specifically sought to evade the limitations of defamation law.[146] Commentators argued that in principle this must be correct or the right to be forgotten would be significantly undermined. [147]

To look beyond the UK, wider understanding of the importance of being able to maintain a person's reputation has been well reflected in Germany where it is common for skills and similar aspects of professions to be rated online. One particular case contrasted the power of

[142] n111 Joined cases of NT1 & NT 2
[143] n111, Joined cases of NT1 & NT2 para 63
[144] Gulati v MGN Ltd 2015 EWHC 1482 (ch) Mann J Khuja (161)
[145] European Convention on Human Rights, 1950. As amended by Protocols Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12, and 13
[146] He also referred to the policy relating to defenses found in section 8 of the Rehabilitation of Offenders Act. This section permits reliance on a spent conviction as a defense to defamation, unless there is malice.
[147] See comment by Christopher Wright QC at https://panopticonblog.com/2018/04/13/nt1-nt2-blogging-to-the-power-of-a-million-words/ last accessed 10 Jan 2020 Here it was stated that its value became more that of a devise rather than a right.

information being disseminated over the Internet with an ability to maintain reputation, thus illustrating the issue. In this case, the website 'Jameda', which had been around for over 10 years, listed approximately 250,000 German doctors and received numerous visitors monthly. This showed the importance attached to a professional being portrayed in a good light in order to attract clients. The website provided two listings for doctors, the main one being a basic free service providing details about each individual.[148] There was also a 'premium' [149] service offered where additional details could be added for a fee. To maintain their reputations, doctors who were subjected to negative reviews either tried to have those reviews deleted or asked for their whole profile to be deleted from the website.

The ability to control information particularly impacting the reputation of a doctor had become of concern when Germany's Federal Court of Justice (FCJ) heard a case where a gynecologist had sought to have his profile deleted from the Jameda website.[150] Due to procedural reasons, the court did not rule upon the distinction between the 'basic' and 'premium' profiles. As a result, the FCJ looked at the website as if Jameda treated all profiles equally, and this emerged as a decisive factor in the conclusion reached. The court's decision in favour of Jameda dismissed the doctor's request for deletion of the profile. According to the judges, Jameda's processing of doctors' data is governed by S 29 BDSG (*Bundesdatenschutzgesetz ,* the Federal Data Protection Act) which states that:

> The commercial collection, storage, modification or use of personal data for the purpose of transfer, in particular when this serves the purposes of advertising, the activities of credit inquiry agencies or trading in addresses shall be admissible if
> 1. there is no reason to assume that the data subject has a legitimate interest in excluding such collection, storage or modification.

[148] The website provided details such as name, academic qualifications, and experience, with areas of specialisation. The organisation tries to list every doctor in Germany on its website with a form of grading next to the name where a user could also leave feedback in reviews.

[149] When viewing a 'basic' profile, Jameda would also show profiles of 'premium' users that had been given higher user ratings than the 'basic' profile. When 'premium' profiles were viewed, no patient reviews were shown.

[150] see commentary Mirko Brüß, German FCJ: doctors can have their profile deleted from rating site - but can they? February 23, 2018 available at https://ipkitten.blogspot.com/2018/02/german-fcj-doctors-can-have-their.html last accessed 27 Feb 2021

As the required 'legitimate interest' (i.e., of the doctor) can only be assumed after balancing the opposing rights and interests at issue, the court looked at the doctor's right to the use of 'informational self-determination' in conjunction with both Jameda's and the reviewing users' right to freedom of expression. While the professional freedom of both parties was also taken into account, the FCJ conceded there was significant importance attached to the inclusion of the doctor in Jameda's database. Any reviews would be able to influence the patient's decision as to which doctor to use. In the court's opinion, although this outcome could affect both the doctor's social and professional reputation, those aspects only touch the plaintiff's 'social sphere', as opposed to the 'private' and 'secret' spheres, which were considered to be more worthy of protection. In this case, with no negative reviews this process had not been utilized as the claimant had 'merely' objected to being included in the database. The FCJ highlighted the considerable interest of the general public with regard to medical services and their quality. While it would indeed be possible for Jameda to continue its business after removing the plaintiff's data, the judges viewed this as endangering the informative value of the website as a whole. Many doctors with negative reviews would ask for removal of their profiles, thereby impeding Jameda's goal to present a 'complete picture' of German medical services. Based on this the decision of the court at this stage was that Jameda's rights and interests outweighed those of the doctor as well as the public's right to receive information, and therefore the profile remained online.[151]

However, two years later another doctor became concerned about receiving negative reviews and a low rating on her profile. She also objected to being included at all in the Jameda website. Other doctors' profiles (those of 'premium' users) were shown next to her entry in the database, impacting the way she was viewed and potentially undermining her profile. On appeal the FCJ agreed with her view, granting removal of her profile. [152] Without the full decision it is unclear as to what were the deciding factors, but it would appear that

[151] Decision made, Az. VI ZR 358/13, 2014, available at https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=69297&pos=0&anz=1

[152] Regrettably the full decision was not available at the time of writing as the court's reasoning was still expected. To this date, only the press release of the FCJ is available. It will be a few months before the written reasons are published. The court gave the complaints (file number 25 O 13978/18, 25 O 13979/18 and 25 O 13980/18), https://limnews.com/tech/2019-12-06--judgment--jameda-has-to-delete-doctors-profiles-under-certain-circumstances-.BkWMtJ_aB.html

considering the distinction between 'basic' and 'premium' profiles was decisive.[153] By providing the two different ways of presenting profiles it seemed clear that Jameda had foregone its position as a 'neutral' information provider. The court found that Jameda's new function as a result on this shift resulted in a lower weighting of the right to freedom of expression on behalf of Jameda. In the balancing of the interests and rights of the plaintiff, the latter came out on top, resulting in an opposite outcome compared to the earlier case. The impact of the case was limited, however, by a change in the way Jameda carries on its business.[154] Concern is that it is unlikely now that doctors will be able to have their profiles removed as even without the two forms of profiles the ruling in the 2014 case appears to remain. The importance of the case is that it brings together ideas of identity, reputation, and public life into a scenario where the ability to arrange for the 'forgetting' of information becomes essential and builds on the changing perception of the need to control personal data however factual and limited i.e., name and qualifications. The use of a right to be forgotten involving such elements promotes informational self-determination despite the issues here not being founded in the private sphere, as such, but in a business environment. In this case, it was also clear that the ability of the public to have access even to such factual information would be challenged, depending on the impact on the individual. The ability of the public's right to receive information becomes of increasing importance in such scenarios where a person's reputation and ultimately livelihood is at risk.

5.7 Considering the public's right to receive information

As the Jameda case showed, there is an issue of how much right the public has to receive information which might impact application of the right to be forgotten. This is not necessarily the type of information relating to crimes committed, for example, but to everyday information, e.g., the names of doctors and medical services. In the approach to considering the scope and extent of the right to be forgotten within areas of reputation and the balancing of privacy and freedom of expression a key component is the right of the public to receive

[153] As it was providing varying information about doctors, depending on whether they are paying customers or not, this became especially visible (or rather 'invisible') when viewing the profile of a 'premium' doctor whose profile was presented without showing any nearby alternatives, as opposed to 'basic' profiles that were shown alongside other doctors who had better reviews.

[154] On the day of the FCJ's decision, Jameda changed its practice and no longer advertises 'premium' customers' profiles on 'basic' customers entries.

information. This was seen in the Campbell case although it was found here that the information was not of public interest.[155] As this position has developed there are three important categories within this right specifically relevant to the right to be forgotten; the right to receive information on public figures, the right to receive information on criminal activities, and the question of the right of the public to receive trivial information.

5.7.1 The right to receive information on public figures

With regard to the information on public figures in considering the case of Google Spain, here was a private man, not a public figure, concerned about the immediate availability of information. Such information concerned only his financial affairs and the subsequent impact on his family life. Would there have been greater interest in retaining the immediacy of the information if Senor González had been a more public figure? The right to be forgotten is fundamentally linked to how a person is perceived within society. If there is a different rule for private and public persons where can the line between these be drawn? In the case of politicians' activities carried out and recorded whilst the individual was unknown, but perhaps when contemplating a role where they would acquire a public persona, there must be valid claims that even old information may be relevant in assessing the character of, for example, the would be politician.[156] It is difficult to see how application of the right to be forgotten can be 'policed' to ensure that valid information remains available, and that a person cannot 'cherry pick' the information they want removed to the detriment of the public's right to know or indeed of freedom of expression. Certainly, public figures often have the means to preserve their persona with reputation management facilities and may also have financial resources to take appropriate action. [157]

The potential loss of control over the right to your own name and any subsequent impact on reputation is, therefore, linked to privacy as well as data control. Revealing information about an individual can often benefit society; it can be used to educate, and to increase knowledge and understanding so as to create and enforce social norms. When information is not

[155] Campbell v MGN [2004] 2004 UKHL 22

[156] Shaun P. Young, 'Politicians' Privacy', Ramon Llull Journal of Applied Ethics (2018) issue 9 pp. 191-210

[157] Available at; https://inforrm.org/2018/10/17/google-and-the-right-to-be-forgotten-four-case-studies-my-clean-slate/ last accessed 16 April 2020-

complete, or has been overlaid with bias, such communication can be mischievous at least and prejudicial at worst. Solove argues that limiting information available to the public can protect individuals by preventing such judgements.[158] The use of informational self-determination provides an opportunity to 'forget' or 'erase' personal data where some form of reputational harm is anticipated or suffered. Where information is spread through the Internet, however created, it becomes a public record, but the benefits to society are not always clear nor the justification valid for prejudicing individual rights to dignity, privacy, and reputation.

There are, however, challenges in determining what would be acceptable to delete, erase, or merely 'forget' with the right of privacy being limited and subject to overriding interests, such as those of the public. When considering how far the scope of the right to be forgotten can protect reputation and dignity, there have been several contemporary examples of attempts to define how much information the public is generally entitled to receive, even if it is to the detriment of those identified. As can be seen in the various significant cases, such as Google Spain, the NT cases,[159] and the case of PJS,[160] it has been made clear that even where there is likely to be public interest, boundaries are required. Whether the impact is on business activities, the ability to raise monies, or a person's sex life there is still a reasonable expectation of privacy unless overwhelming factors weigh in favour of public interest. The question is how such boundaries can be determined, by whom, and what is the effect on the individuals concerned? To many the clash between freedom of expression and privacy can be seen clearly in the right to be forgotten conflicted between two ideals underlying autonomy and, potentially, even democracy[161].

An example of this dilemma occurred in 2014. In an early case based on the right to be forgotten, as established by Google Spain, an Irish politician, Marc Savage, asked Google to delete links to a site which stated: 'Mark Savage North County Dublin's Homophobic

[158] Daniel J Solove, *Speech, Privacy and Reputation on the Internet*, in (eds) S. Levmore & M. C. Nussbaum, *The Offensive Internet,* (Harvard University Press 2010) p16
[159] n 111 Joined cases of NT1 & NT 2
[160] PJS v News Group Newspapers Ltd [2016] EWCA Civ 393 on appeal [2016] UKSC 26
[161] In July 2018 Facebook was fined by the UK ICO for breaches of the UK Data Protection Act where Facebook failed to safeguard its users' information and failed to be transparent about how data was harvested. The data was used by the now defunct Cambridge Analytics in the 2016 US Presidential campaign and in the UK referendum.

Candidate'. The users of the web forum Reddit had been discussing the public behaviour of Savage with regard to what was seen as a negative attitude towards homosexuals. Google refused to remove the link, arguing Savage was a public figure and as such had merely joined a debate on matters relating to the gay community. The public was entitled to access this on the basis that it related to political and cultural views held by Savage. Savage then filed a complaint against Google at the Irish DPA which merely confirmed Google's decision. Following Article 29 Working Party's guidelines,[162] the DPA found nothing that would evoke a claim under the right to be forgotten. However, the matter was not considered final by Savage who progressed it successfully to the Dublin Circuit Court. While Justice Sheahan admitted that the appeal turned on a consideration of a narrow premise finding that the comments amounted to opinions, it was held that Google could not be expected to 'edit' such. It was however disappointing that the court remained silent regarding the ways in which the link to the controversial discussion on Reddit did influence (or could influence) individual privacy and other values underlining the right to data protection.[163] Google appealed to the Irish High Court with the final outcome given in February 2018.

In the High Court, Mr Justice White deliberated on the decision made in Google Spain but considered application of it could only be made on weighing up the full facts. Here it had been noted that if the full debate on Reddit was considered, then the original posting was merely an 'expression of opinion', so the link could not be considered in isolation but must be viewed as part of the whole debate. The High Court ultimately disagreed with the previous outcome finding in favour of the DPA and Google once again. [164]

[162] Article 29 Working Party Guidelines on the Implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v Agencia Española De Protección De Datos (Aepd) and Mario Costeja González" C-131/12, adopted on 26 November 2014.

[163] Mark Savage v. Data Protection Commissioner and Google Ireland, Record No. 2015/-2589, delivered by Judge Elma Sheahan on the 11th October, 2016. '… users of the internet, now more than ever, rely on it for ascertaining information, and therefore the need for accuracy regarding factual information in same is of paramount importance.'

[164] Savage -v- Data Protection Commissioner & anor [2018] IEHC 122 White J stated Google does not carry out editing functions in respect of its activities and to mandate it to place quotation marks around a URL heading would oblige it to engage in an editing process not envisaged by the Google Spain decision.

5.7.2 The right to receive information on criminal activities

Closely linked to the need for rehabilitation is the ability to 'forget' information relating to criminal offences or even suggestions of criminal activities. This has been the subject of many requests under the right to be forgotten and much debate as to how this can be determined. An example of the difficulty involved an action concerning individuals' rights to restrict access to information concerning the most heinous crime of murder. This was vigorously pursued through the German courts.[165] Here, two men had been convicted in the national domestic court of the 1993 murder of a well-known actor[166]. Having served their sentences, they were released in 2007/2008. Subsequently, they felt that access to their personal data relating to the sentences should be restricted and claimed the right for this information to be made anonymous fearing the information could adversely impact how the public perceived them. They did not actually claim a right to be forgotten but the purpose of the actions against various media was ultimately to achieve the same result. Despite an element of sympathy being expressed,[167] the Federal Court of Justice held that the media (in this case a radio station as opposed to the Internet) had a right to freedom of expression which overtook the individual's claim with public interest being paramount. The history of the conviction was not considered to have outweighed such interest.[168] Similar conclusions were reached in other actions against other media.[169]

---

[165] re MW & WW Federal Court of Justice, nos. VI ZR 227/08 & 228/08, 15 December 2009. The Court upheld the appeals on points of law lodged by the radio station and quashed the decisions of the German Court of Appeal & the Regional Court of Hamburg. The Federal Court of Justice observed that the provision of the impugned material constituted interference with the exercise of the applicants' right to protection of their personality (*allgemeines Persönlichkeitsrecht*) & their right to privacy under Art 1 S.1 & 2 S.1 of the Basic Law & Art 8 of the European Convention on Human Rights (ECHR). Those rights had to be balanced against the right to freedom of expression and freedom of the press as guaranteed by Art 5 S.1 of the Basic Law & Art 10 of the ECHR. See Chapter 3 for earlier comments on the claimants MW & WW.

[166] This is highlighted in the various decisions and also case notes, and it is presumably of importance in establishing the public's interest in knowing about the case due to the fact that the victim was a public figure of whom there was likely to be more awareness.

[167] The Hamburg Regional Court found in their favour in 2008, saying the time that had passed since the conviction justified the information no longer being made available to the public

[168] Translation from the case, 'However, according to the Federal Court of Justice, in the circumstances of the case, the disputed portion of the report of 14 July, 2000 did not significantly affect the applicants' personality rights (*erheblich*), on the ground that it was not such as to put the applicants 'in the queue for eternity' or to drag them into the limelight (*ins Licht der Öffentlichkeit zerren*) in a way that would stigmatize them again as criminals'.

[169] Cases were made against Der Spiegel and Mannheimer Morgen

Their next step was to consider an action under Article 8 of the European Convention on Human Rights. In 2010, with a claim that the German court had failed to honour their right for respect for their private life/lives, the men sought an order for an injunction prohibiting media information about their trial and conviction. [170] Key to the decision was the fair balance that needed to be made between the applicants' rights for their private lives and the right of the media to freedom of expression. This echoed the balancing act required under the decision in Google Spain, albeit in a different forum. There was also no action against search engines' listings as the application pre-dated Google Spain and was subsequently recognized by the court which noted the similarities of the claim.[171] In its considerations the court raised the particular nature of a search engine's involvement considering that this performed a new function in the accessibility of information being made available. This was not, however, considered a key interference, rather it was merely an amplification of the scope of the interference. [172] The decision in the case [173] looked at the fair balance to be struck between the respect for private life guaranteed under Article 8 and the rights of the radio station and the press under freedom of expression as well as the public's right to be informed.[174]

The case drew on the history of the claimants' activities and their desire for such acts to be anonymous. It considered whether publication of the activities or the revelation of identify was for the benefit of society because although the public had an interest in being informed as to criminal proceedings, an individual also had an interest in not being confronted by his past actions with a view to re-integration into society. The Court confirmed that there was public interest in being informed about current events and also being able to research past

[170] Applications were lodged with the European Court of Human Rights on 15 and 29 October, 2010, respectively. Affaire M. L. et W. W. c. Allemagne (Requêtes nos 60798/10 et 65599/10)
[171] Case C-131/12, Google Spain SL and Google Inc. [2014] ECLI: EU:C:2014:317 (Google Spain), the CJEU was called upon to define the scope of the rights and obligations deriving from Directive 95/46 / EC.
[172] 'To the extent that the complainants contend that this way of measuring the degree of diffusion does not take into account the ubiquitous nature of the Internet and hence the possibility, regardless of the degree of initial diffusion, to find the information about them. search engines, the Court, while being aware of the sustainable accessibility of any information once published on the Internet, finds that the applicants have not made contact with search engine operators to reduce the detectability of information about their persons'. Fuchsmann, Phil v. Sweden (Dec.), No. 74742/14, February 7, 2017)
[173] ML and WW v Germany ([2018] ECHR 554) reported in French only
[174] see European Convention on Human Rights, 1950. As amended by Protocol Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12, and 13, Article 10 1). '…[T]his right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.' https://www.echr.coe.int/Documents/Convention_ENG.pdf

ones. On these facts the public interest had not vanished and was still relevant to the public. In addition, the claimants, through their own activities, had not vanished from public life and could not be said to be 'private' citizens as such. Within the detailed consideration by the court was the awareness that such convictions were not spent or deleted, confirming belief in what Hugh Tomlinson QC calls the protection of 'media archives' under Article 10.[175]

It was also interesting that the judgment made reference to the issues facing public figures who had portrayals of themselves made available but then needed to correct any false public images. Apart from the issues around the truthfulness of the images, the court indicated that public interest was of such importance that where the person concerned has deliberately set out to present a false picture, i.e., there was the intention of deliberately deceiving the public, there should be no protection from the media publishing such information. [176]

Further developments have come in the form of a recent decision by the German Constitutional Court based on similar facts whereby a convicted murderer objected to his name being linked to details of his crime. Here the argument was based on claims that news stories created a 'violation of his privacy rights' and his 'ability to develop his personality.' The court upheld the claim on the basis that the right to be forgotten overruled the earlier decision which rejected the claim on the basis of press interest and freedom of expression.[177] Here the right of informational self -determination was debated with the balancing act of wider fundamental rights being paramount. The challenge of the continuous availability of details of such crimes means a balancing act is required to weigh up the rights of an individual

[175] Hugh Tomlinson QC represented the claimants NT1 and NT2 in the joined cases of NT1 & NT2 v Google LLC [2018] EWHC 799 (QB) See https://www.matrixlaw.co.uk/judgments/court-delivers-ruling-right-forgotten-applying-cjeus-google-spain-case / last accessed 11 Nov 2019

[176] However, in a wider approach the court dismissed the idea that individuals had a duty to correct any images portrayed online which later became false. This could be compared with the approach in Ferdinand v MGN [2011] EWHC 2454 (QB), in which it was the image portrayed by Rio Ferdinand in an article 2006 that was found to be false and "while that image persisted" there was a public interest in correcting it. This may further be compared with an unreported instance of actions taken against a German Princess in the UK of drunken, insulting, and racist behaviour. This was seen in a Google Transparency report which had detailed the status of the person and then investigated by a journalist, noting that 197 links to information about criminal activities by the person were removed despite this being inconsistent with references to criminal actions generally being considered to be in the public interest. See https://www.vice.com/en_us/article/889kyv/a-princess-is-making-google-to-forget-her-drunken-rant-about-killing-muslims

[177] BVerfG, Order of the First Senate of 6 November 2019 - 1 BvR 16/13 -, paras. 1-157, ECLI:DE:BVerfG:2019:rs20191106.1bvr001613

with the expectations of society as to what information should be made available, here confirming that individual rights, wider than privacy and data protection may still merit protection.[178]

5.7.3 Is there a right to receive trivial information about a person (gossip)?

This third category is more contentious in an era where there seems to be full disclosure of individuals' personal lives through social media. However various cases have focused on the right to receive information only being exercisable where the information is not trivial nor mere gossip. [179] The impact of social media has been universally felt even in countries where the level of technology may not be as sophisticated as within Europe and the US,[180] and the difficulties in curbing this legally, where there is no direct fit, potentially enables similar actions to the right to be forgotten to be applied in certain circumstances. The use of existing laws to meet the need that new technology has created has taken many forms.

In the ML & WW cases there was also reference to how English law has adapted the law around breach of confidence to provide a form of recourse for personal information disclosed without consent, as had been shown in Campbell v MGN Ltd.[181] The Campbell case[182] also raised interesting questions on how images of a celebrity could still have the benefit of privacy through the use of breach of confidence. The facts concerned published photos of Ms. Campbell, a famous model, leaving a drug addiction clinic. Although it was admitted in court that she was a drug addict and publishing the fact that she was receiving treatment was of valid public interest, a claim was made for breach of confidentiality and compensation under the UK's Data Protection Act 1998. Here, in attempting to retain control over her image in

[178] ibid, Here the Court determined that 'the legal order must protect the individual against the risk of being constantly confronted in public with one's past opinions, statements or actions, without any kind of restriction. Only when matters are allowed to stay in the past do individuals have a shot at a new beginning, to live their life freely. The possibility for matters to be forgotten forms part of the temporal dimension of freedom. This concept is figuratively referred to as the "right to be forgotten" [in German: "Recht auf Vergessen" or "Recht auf Vergessenwerden"]' commentary available at https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2019/bvg19-083.html

[179] Campbell v MGN Ltd [2004] UKHL 22; [2004] 2 AC 457; [2004] 2 WLR 1232; [2004] EMLR 247

[180] For example, see the imposition by the Ugandan government of a new social media tax imposing a 200 shilling [$0.05, £0.04] daily levy on people using internet messaging platforms like Facebook, WhatsApp, Viber, and Twitter. President Yoweri Museveni had pushed for the changes, arguing that social media encouraged gossip. https://www.bbc.co.uk/news/world-africa-44315675 last accessed 5 June 2018

[181] see n179

[182] see n179

the photographs and how she was portrayed to the public, the case by Ms. Campbell involved joining elements of breach of confidence, privacy, and data protection. Believed to be one of the first cases on privacy in the UK, this showed how the use of data protection might develop to help with broader control of how an individual is portrayed. This may have been the first opportunity for a claim for privacy to arise where information was being made freely available, impacting the privacy of the individual as well as how she was being presented to the public.[183]

The challenges of protecting an image when the individual concerned is not a public figure as such was demonstrated in the RocknRoll case. [184] In this case, photos of the naked claimant, the new husband of actress Kate Winslet, were taken by a friend and privately posted on Facebook. These then became available to the public due to a change in Facebook's privacy settings. The issue here was largely a question of privacy with the balancing of the claimant and his family's privacy rights against freedom of expression and the public's right to receive information. It was clear that the photos were not intended for wider publicity, were not readily available on the Internet, and that the claimant had not sought any publicity. The court determined that just because material can be accessed via a social networking site, it did not necessarily mean the material was in the public domain and should be 'published'.
Removal of the photos was ordered as there was nothing of particular interest or concern to the public. In such a case the privacy issues must take precedence, particularly with young children of the family likely to be affected. Even though the claimant was only well-known due to his marriage, it was clear that he could expect and receive protection for photographs which were not for public consumption. This might be considered a forerunner of the issues over removal of information (or links to it) faced in Google Spain with the notable difference that here the photographs were considered to be private and intended only to be available to friends and family. However, the information about Senor Gonzalez was public information which a court had deemed should be made available, even if argued to be no longer relevant.

[183] The very recent claims by Meghan Duchess of Sussex against the Media Group have also highlighted the potential use of actions for breach of privacy, data protection as well breach of confidence in respect of a private letter published by a newspaper (the Daily Mail). Initial parts of the claim have now proved successful with Mr Justice Warby confirming a proportionality test in weighing up rights, see HRH the Duchess of Sussex v Associated Newspapers Ltd. [2021] EWHC 273 (ch)
[184] RocknRoll v News Group Newspapers Ltd: [2013] EWHC 24 (Ch)

In both cases the impact on the individual and their privacy, their dignity, and their reputation was substantial. Here, a right to be forgotten as informational self-determination would provide the protection required.

5.8 Does the right to be forgotten provide an ability to define who you are through individual informational self-determination?

Dewey[185] speaks of humans as beings that are constantly changing, "the self is not fixed but grows throughout an entire lifetime". It would seem that not only is the Internet a ground in which data is made available, impacting rights, as explored before, whether posted by data subjects themselves or through posts placed on sites by other sources, but it is also an environment where people can explore and create various aspects of their personality, or identity, in chat rooms, forums, blogs, Facebook, and similar sites, including even dating sites. Ideas of identity or self can be seen as fluid, changing in shape according to the circumstances or the demands placed on the individual concerned. Even without ideas of identity and reputation, the focus on an individual choosing how he/she can be portrayed brings to the fore the challenge of individual self-determination with the question of autonomy. Underlying any right to be forgotten and key to a person exercising autonomy is the ability to have agency either by using privacy, rights to dignity, or the fundamental right of data protection.[186] An idea of the extent of the importance of such autonomy was expressed by Joseph Raz,[187] who stated the view that an autonomous person is a part author of his own life. The view of personal autonomy is the vision of people controlling, to some degree, their own destiny, fashioning it through successive decisions throughout their lives. This can be compared with Rawls[188] claiming that, '[a]utonomy is a constituent element of the good life', thus potentially arguing that a good life is not possible without autonomy, i.e., the ability to make choices. Even a 'legal' definition includes the idea of self-government.[189] To manage this exercise when forces of artificial intelligence and algorithms operate to provide a view of

[185] John Dewey, *Experience and Nature: The Later Works, 1925-1953*: Jo Ann Boydston (ed) (Southern Illinois University Press 2008)
[186] The Charter of Fundamental Rights of the EU [2000] OJ C 364/1
[187] Joseph Raz, *Morality of Freedom*, (Clarendon Press 1986) p. 369
[188] ibid Raz p 408
[189] Merriman-Webster Dictionary of Law. 'Autonomy' as the quality or state of being self-governing, especially the right of self-government. https://www.merriam-webster.com/

yourself over which you potentially have no control, supports those arguing for the widest interpretation of the right to be forgotten and the ability for informational self-determination. For autonomy to function there must be a choice, one to be exercised with free will and in circumstances where there is no undue influence or coercion. This should be exercisable where there is freedom from manipulation which could be argued to be the foundation of issues arising from the impact of the results under a Google search.

This view is expanded by Nissenbaum who, looking at aspects of data manipulation and unconstrained publication, has the view that;

> 'the manipulation that deprives us of autonomy is more subtle than the world in which lifestyle choices are punished and explicitly blocked.'[190]

In pursuit of autonomy, it can be argued that the ability to utilize the right to be forgotten by way of informational self-determination impacts the way a person is perceived by the rest of society so can be justified, but this is not without its challenges. It can also be argued that autonomy has, and must have, a social element which enables the individual to exercise his own free will in a societal manner.[191] This can be in day-to-day life or an online environment. The ability through the internet to portray a person according to the information collated, particularly through search engine results, is vast. It is no co-incidence that those who provide the much watched 'blogs' of activities featuring favoured ways of living are now known as 'influencers',[192] or that advertisers move more towards 'targeting behaviour' to identify and promote products to intended customers, thereby building an eternal digital persona.

---

[190] Helen Nissenbaum, *Privacy in Context: Technology, Policy and the integrity of Social Life*, (Stanford University Press 2009) p 83. Here, Nissenbaum describes that she draws from the work of Gandy in respect of establishing the link between the loss of autonomy and data manipulation leading to a lack of choice for the individual.

[191] see Daniel Solove, *Speech, Privacy and Reputation on the Internet*, in S. Levmore & M. C. Nussbaum, (eds.) *The Offensive Internet*. (Harvard University Press 2010) p18 'Broad based exposure of personal information diminishes the ability to protect reputation by shaping the image that is presented to others. Reputation plays an important part in society …'

[192] Such individuals range from the well-known, i.e., a sportsman, to the individuals created by the Internet and generally having no actual function other than as a person who publishes various items, thoughts, etc on their own site on the Internet. This is a short summary of the main such influencers appearing on social media https://influencermarketinghub.com/top-25-instagram-influencers/

If reputation or a sense of identity is the concern and forms the basis of the use of the right to be forgotten to exercise such autonomy, a series of recent cases, particularly in the UK, have shown the determination of specific individuals, particularly those in the more dubious spotlight, to try to protect the image that is portrayed of them. In particular, the infamous cases raised by Max Moseley have been imaginative in how they have tackled such issues, although without the use (to date) of the right to be forgotten. Many actions were commenced prior to the formularization of the right under Article 17, but they were made in circumstances where the ability to claim such a right would have been beneficial.[193] Moseley had sought to stop publication of embarrassing, but true photographs featuring sadomasochistic dealings with prostitutes, activities unlikely to improve his reputation. In 2008, the UK court found in his favour, confirming that even high-profile characters such as Moseley were 'entitled to a private personal life',[194] albeit with substantially reduced levels of damage.[195] However, Moseley decided to take further action to a French court, suing Google on privacy related grounds. Here he asked for links to the images of his encounters to be removed from the search engine's data completely. Google, in accordance with its US roots, argued for freedom of expression amongst its defences but the French court ordered for the links to be removed.[196] The court implied that there was no defamation but a breach of privacy, resulting in damages.[197] The case was prior to the decision reached in Google Spain and was done without recourse to the data protection legislation then in existence. The precedent of the French case finding in his favour was, however, followed with a similar response by the German courts.[198]

[193] Even if a decision would presumably have been that the facts of the case did not merit removal of links or information.

[194] Moseley v News Group Newspapers [2008] EWHC 1777, [101] (QB)

[195] The court awarded Mr Mosley £60,000 damages after ruling the News of the World invaded his right to privacy by reporting on his sex life.

[196] Press article 'Max Mosley wins privacy case in France' 8 Nov 2011 https://www.bbc.co.uk/news/uk-15641211 the case which took place in Paris was not reported last accessed 8 April 2019

[197] It should be noted however the damages granted here were very low i.e. the amount was reduced from the claim of Euros 100,000 to Euros 7,000.

[198] https://searchengineland.com/german-courts-follow-french-ruling-order-google-to-block-max-mosley-images-in-search-results-182585

Dubbed by the media, in the form of the Daily Mail,[199] as the "Man with a genius for forgetting" as a result of his many actions, primarily aimed at the press, it was believed that a further case may be bought under the right to be forgotten.[200] Although reported in February 2018 by the Press Gazette, there has been no formal action as yet but clearly for Moseley the impact remains that the publication of his private life activities has resulted in a loss of dignity and irrecoverable loss of reputation. Within the press itself there was fierce condemnation and concern that data protection laws could be misused in such a way, creating an instant hostile response towards the ability to use such laws to 'determine' the portrayal of an individual.

The recent Guide on Article 8 of the European Convention on Human Rights right to respect for private and family life, home, and correspondence was published on the 31st August 2018.[201] It also made, in its review of privacy, reference to specified components such as individual reputation and defamation as being aligned with data protection and right of access to personal information. This included identity and autonomy in an arguable right to personal development, revealing the complexity in the protection of privacy but acknowledging the relationships between rights where there could be provision not only of a right to be forgotten but a right of informational self-determination.

The idea that history can be rewritten, particularly in the way individuals are portrayed, was also one of the main areas of criticism of the Google Spain case from various countries, including the UK, opposing the creation of the new right.[202]

---

[199] Daily Mail 8 March 2018 see also https://www.theguardian.com/media/2018/feb/28/max-mosley-half-forgotten-far-right-past-catches-up-with-him

[200] The Guardian quoted Mark Stephens, a senior partner and media lawyer at Howard Kennedy as having said there were good reasons for law and journalism students to study the details of the Mosley-News of the World case, because it was a test case for privacy. He added that if the data protection complaint were to succeed it would have serious implications. "Effectively people will be able to airbrush history. In terms of using the law, this is entirely novel," https://www.theguardian.com/media/2018/feb/16/max-mosley-threatens-sue-papers-orgy-story-data-laws last accessed 20 Oct 2018 However since this, the death of Max Mosley has been announced ending any plans for such action.

[201] https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf

[202] European Union Committee - Second Report EU Data Protection law: a 'right to be forgotten'? July 2014, The House of Lords report concluded,

'Europe's right to be forgotten ruling, which states that everyone has the right to wipe their digital slate clean, is simply "wrong". It also objected to Google being faced with an "unworkable and unreasonable situation" in the attempt to grant such right. following discussions with such bodies as the Information Commissioner's

Baroness Prashar, Chairman of the Committee stated,[203]

> We do not believe that individuals should have a right to have links to accurate and lawfully available information about them removed, simply because they do not like what is said.

In contrast to the view that the right to be forgotten is about re-writing history, i.e., changing the recounting of past events to change the perception of a person, Ioannis Iglezakis has put forward the view that whatever is considered to be the reason for the development or acceptance of a right to be forgotten, the real issue behind it is now understood confirming that an individual has a 'significant interest possibly protected by a legal right in not being confronted by others with data from the past '*which are not relevant for current decisions or views about him or her'* (italics added for emphasis).[204] If this exercise of the right to be forgotten results in a person being perceived in a different way, then this is a 'by product' of the right rather than an intended consequence. However, the exercise can be connected with any right to personal identity or to the consequences of rehabilitation linked to reputation insofar as it provides the ability to reinvent oneself or to have a second chance to start over and present a renewed identity to the world.[205]

As previously explored, ideas of rights over identity are not new and have been shown in other legal concepts. In his work on reputation one area debated by Solove is the tort of appropriation which simply aims to prevent financial gain from the use of someone's name or likeness. Despite this being used to create a form of a protection for privacy, the tort did not provide sufficient recourse, generally focusing on celebrities seeking to prevent misuse of their name on products. Kahn refers to the tort developing into a form of property right,

---

Office, Minister for Justice and Civil Liberties Simon Hughes, and Google, amongst others. Available at https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/4002.htm

[203] Statement by Baroness Prashar on the 30th July available at https://www.thetimes.co.uk/article/peers-to-attack-eu-right-to-be-forgotten-web-ruling-5vr9577ldzp last accessed 11 May 2019

[204] Ioannis Iglezakis 'The Right to Be Forgotten in the Google Spain Case (Case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet?', available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472323 last accessed 9 Sept 2019
See also Bert Koops 'Forgetting Footprints, Shunning Shadows A Critical Analysis of the Right to be Forgotten in Big Data Practise', (2012) Tilburg Law School Legal Studies. Research Paper series No 8/2012 at 232

[205] Norberto de Andrade, *Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization*, in Serge Gutwirth, Yves Poullet,Paul de Hert (eds), Computers *Privacy and Data Protection. An Element of Choice* (Springer 2011), pp. 65-97.

losing the initial focus on the dignity of self and 'integrity' of an individual's persona.[206] Use of the tort had diminished by 1960 with Prosser confirming its use was around 'profit value' rather than personal privacy. However, it did establish the continued questions around how much control individuals need to have over their images, even the image or persona they want to present of themselves, and whether the right to be forgotten could impact this. The position must be separated from that of such public figures who may have already waived any right to claim privacy by virtue of their public activities.[207]

If public interest and freedom of expression remain the priority despite the perceived need for autonomy and developing personality rights, then it could be claimed that the right to be forgotten, when refocused as a right to be able to tailor the information available, cannot be a fully-fledged right as this does not work with such priorities. So, for example, if it can be accepted that a person not in the public arena should be able to 'erase' or have information 'forgotten' which relates to earlier misdemeanours (a different situation would clearly arise with regard to criminal activities), what if such a person then becomes a politician? At what point does public interest take a 'what if' approach, and then should a third-party agent such as Google, who claims not to have any journalistic or editorial involvement, be key to the decision making? Within such differing approaches to privacy for public individuals there are no clear boundaries drawn and debate continues.[208]

Further arguments have been made by Solove focusing on informational privacy rights based on the reputational risks. This introduces an argument that loss of control impacts both your reputation and your ability to convey how you are portrayed in public and is therefore beyond mere control of the actual data. It is clear that the right to be forgotten also works on this

[206] Jonathan D Kahn, 'What's in a Name? Law's Identity Under the Tort of Appropriation' (2001). Temple Law Review, Vol. 74, p. 263, available at SSRN: https://ssrn.com/abstract=1950309 In this a 1905 case referred to the tort of protecting a person's freedom to be 'the right to withdraw from the public gaze at such times as a person may think fit when his presence in public is not demanded by any rule of law is able to be embraced within the right of personal liberty'

[207] Sean P. Young, 'Politicians' Privacy', Ramon Llull Journal of Applied Ethics, (2018) Iss 9 pp 191-210

[208] This is perhaps reflected in an era of scandals, for example, the campaign for the future prime minister Boris Johnson fought for a private life, whilst opposers argued that putting himself into such a position meant he had greater reduced rights to privacy see article available at https://www.telegraph.co.uk/politics/2019/06/24/boris-johnson-defends-right-privacy-insists-not-trying-have/. last accessed 16 Sept 2020

premise in its wider context, thus the information is and will remain accessible largely because it is already available publicly. This was certainly the case in Google Spain, although perhaps not in the situation of the NT cases where, in theory, the information was no longer readily available because the convictions were 'spent'. So, although there are formal rights over data being held as were contained in the DPD and in the GDPR, the right to be forgotten is more concerned with the accessibility of the information and its potential to shape public perception.

This concept is of sufficient interest to have spawned newly formed organizations to manage the process on behalf of such persons. This may not be as specific as reputational management as it is not a question of creating positive 'spins' on events and stories to enhance the perspective through which the person is viewed, but it concentrates on removing past activities where the individual no longer wishes to be associated with them, using the pathways to the right to be forgotten. An example can be given by utilizing the company *mycleanslate.com*[209] which provides what it calls an 'online reputation repair service'. For a low fixed fee the company offers a service where it approaches Google on behalf of its clients and makes applications under its right to be forgotten process to remove links to specific URLs. Such an organization has no other function, it is merely a facilitator, but one that seems to be providing a welcomed service with a simple and seemingly un-contentious ability to tailor how information about you is made available.[210] Interestingly, the experience of requesting the removal of links under the right to be forgotten process has proved anything but easy, and the results according to this organization are inconsistent[211] despite the linkages often creating great concern to those applicants.

[209] https://www.mycleanslate.co.uk/

[210] There are various organisations dealing with Reputation Management, this is a growing area where services are provided. See https://blog.reputationx.com/whats-reputation-management . 'Reputation management is the effort to influence what and how people think of a brand or person when viewed online. Put another way, character is who you are. Reputation is whom other people *think* you are, and today it's based mainly on what artificial intelligence systems portray about you rather than the first-person experience.'

[211] Comments by the organization have referred to it as largely depending on the personality of the Google representative.

5. 9 Conclusion

With a range of recourse in place for the protection of reputation and dignity as well as providing support for autonomy and with a changing view of privacy taking place as the Internet grows, the right to be forgotten does not stand alone but could be considered to be developing towards fulfilling a role where its principles, as so far established, will be expanded to provide wider recourse, specifically slanted towards meeting the very specific requirements of accessibility of information on or through the Internet. Article 17 introduces this by way of requiring data controllers who have made personal data public to also request erasure form all other controllers processing the same data. Similarly, this may well involve further internet service providers rather than being restricted as under Google Spain to search engines.[212] This will develop not only the protection of privacy, but it will strengthen its ability to defend dignity and reputation as well as associated issues, as demonstrated with the potential impact on intended rehabilitation.

The 'right to be forgotten' can be considered in the words of Richard Peltz-Steele[213] to be;

'really a right to be forgiven; a right to be redeemed; or a right to change, to reinvent and to define the self anew. A person convicted of a crime deserves a chance at rehabilitation: to get a job or a loan. A person wrongly charged or convicted deserves even more freedom from search-engine shackles.'

This focus on the ability to rehabilitate is an example of the use of the right for informational self-determination, but this is perhaps a more extreme version. Individuals do not seek to always 'forget' information for such a reason but for more incidental prosaic circumstances. Just as a child is able, under the provisions of the GDPR,[214] to remove information provided whilst underage, so there needs to be recognition that to protect privacy and to control data

[212] See Jef Ausloos, chpt 4 p 237, here he discusses the Right to be Forgotten 2.0 and the expansion of its scope.

[213] Richard Peltz-Steele, 'The right to be forgotten is really a right to be forgiven,' Washington Post, Nov 21 2014

[214] Art 8 of the GDPR applies to the provision of consent by a child. Although not specifically provided for in the wording, it is understood that this means a child can withdraw consent to information being processed when underage. Recital 65 of the GDPR specifically states the right of erasure: "…is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child…"

there must be a right to reveal yourself as you truly are as opposed to how algorithms depict you.

By the drawing together of ISPs, and particularly search engines, into territory where the protection of the press does not apply, the ability for the right to provide new protection into such fast growing areas where the accessibility of personal information and data is key to maintaining other criteria such as dignity and autonomy, becomes of increasing importance . With the necessity for protection of data becoming widely accepted, the more mechanical nature of Article 17 of the GDPR may be sufficient in certain instances to allow for the deletion of inaccurate, out of date, or no longer required data.[215] However, in situations where data can impact reputation, but potentially not sufficiently enough so as to engage accepted legal remedies such as defamation, then the right to be forgotten as originally determined by the decision in Google Spain and in subsequent case law will potentially play an increasing role with scope to develop under the application of Article 17. It is clear that in arguing the fine lines between privacy and its protection and the misuse of data with freedom of expression any opportunities to 'rewrite' history may be minimal, but that the opportunities under the right to be forgotten may offer more scope for the deletion of various links to information, thus permitting tailoring towards a different profile on the Internet. The extent to which this may be provided may well come as more cases emerge or an understanding of the provisions or limitations of Article 17 becomes clearer. It will still represent a different perspective and approach to the fine balancing act that an individual deserves.

In conclusion, the impact of the right to be forgotten, whilst not yet being clearly defined by caselaw following the Google Spain decision nor from examples of actions under Article 17 of the GDPR, is not diminishing, rather it is increasingly important where there is an accelerating change of approach toward privacy and the rolling out of data protection from the EU into global territory. The shape it is taking will recognize that the availability of information,

[215] The process is based on the Data Subject's right to request erasure and a corresponding obligation on the data controller to remove the information. The right of erasure as set out in Art 17 is not only intrinsically linked to other key provisions in the GDPR such as the right of access in Art 15 but is based on pre-conditions or triggers which evoke the exercise of the right. Such triggers are in turn linked to three key principles of the GDPR Art 5 (1) (a) purpose limitation (c) data minimization and (e) storage limitation. The use of Art 17 needs to be applied in conjunction with this and with the data controller providing the data processing systems to effect such removal where there is no valid objection by it to the exercise of the right.

particularly through the Internet, provides unprecedented opportunities for a person to be adversely affected whether by loss of autonomy or dignity, by loss of reputation, or just irrelevancy as to the character or person the particular individual has become. Progressively, as people claim the right to data protection to control over how much data is collected, processed, and made available, they will also claim the right to determine how they are represented as individuals through such data. It may be that in the new world of the tech giants there will be demands that such organizations are no longer the decision makers on such aspects. The following chapter looks at the approach being taken to such entities now and the consequences for the application of the right to be forgotten.

Chapter 6 -The challenges of providing control and protection of personal data on the Internet through informational self-determination under a right to be forgotten.

6.1 Introduction

As explored in Chapter 5, a new age of data awareness with a desire to have the ability for informational self-determination is emerging. The scandals that have broken, particularly with regard to Facebook and Cambridge Analytics,[1] have raised public attention to the fact that there is a high price to pay for the instant availability of information which remains permanently recorded. The cost of providing personal information is not only having access to a social media site or a 'free' app, but a much greater cost that impacts your ability to manage private information about your way of life, your friends, and your activities. The data subject and their information have now become the 'product' for many commercial enterprises. In an increasingly exposed world, the ability for a right to be forgotten to be exercised to provide, if not promote, the required portrayal of yourself takes on a wider significance. As discussed in Chapter 2, human rights have formed the basis of the right of erasure as contained in Article 17 of the GDPR[2] following the influential decision of the Google Spain case,[3] thus triggering part of this new response to how the Internet can portray you. The environment is now more conducive towards an individual's need to be autonomous with regard to informational self-determination. The desire to be able to influence if not control the information attached to yourself can be seen in the numbers of applications made to Google. The latest report by Google shows that the use of the online system[4] set up after the decision in Google Spain has now produced over 1,000,000 requests[5]. These have produced a number in excess of 4 million URLs to be delinked. This represents a huge increase from the period post Google Spain when under 500,000 de-linking requests were received.

[1] The dispute over the collection and use of data through these companies was heavily reported by the media before official investigations took place, https://www.bbc.co.uk/news/technology-43465968

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[3] Case C- 131/12 Google Spain Sl Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González Case, [2014] ECLI: EU:C:2014:317 (Google Spain)

[4] available at https://www.google.com/webmasters/tools/legal-removal-
https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637202230061146146-20083139&rd=11 last accessed 22 Feb 2020

[5] Available at https://transparencyreport.google.com

The percentage of successful applications however remain at approximately 50% with little change (currently 46.8 refused / 53.2 confirmed) since the start of the process). There still remains little guidance on how decisions are made nor the process internally with information supplied stating that Google LLC staff make the relevant determinations. [6] The process is however only open to European citizens leaving some concern in other jurisdictions that users are not entitled to the same benefits or indeed rights as those in the EU.

This is partially reflected in the impact of the right to be forgotten in other jurisdictions showing that it is not only the EU that recognizes such need.[7] Even in the US there have been initial attempts to introduce the right[8] as more citizens acknowledge that they too wish to 'keep things about themselves from being searchable online.'[9] Consideration of the scope and extent of a wider 'right to be forgotten' has built awareness by both data subjects and legal commentators of the need not just for data privacy[10] but for increasing control over how a person is portrayed. This can come through wider forms of protection for the restriction of accessibility of information relating to a person. Increased clarity is now needed to define the extent and scope of the right to be forgotten, to position it and provide certainty around its where and how it is applied. What is being added by the right to be forgotten to data protection and human rights regimes through its use and enforcement also impacts an

[6] Google states 'We have a team of specially trained reviewers for this purpose, based primarily in Dublin, Ireland. Our team uses dedicated escalation paths to senior staff and attorneys at Google to adjudicate on difficult and challenging cases. As of November 1, 2015, just over 30% of requests had been escalated for a second opinion.)'

[7] Similar provisions have been enacted in Israel specifically whilst other states are considering it. see in particular Tamar Gidron, Uri Volovelsky, 'The Right to be Forgotten: The Israeli Version', [2018] Computer Law & Security Review 34, 824-829. Another example is in India where the concept of the right to be forgotten was confirmed in the cases of Vasunathan v. The Registrar General, High Court of Karnataka (2017) SCC OnLine Kar 424); Zulfiqar Ahman Khan vs. Quintillion Business Media Pvt. Ltd. and Ors (2019) 175 DRJ 660. It is also contained in the draft Personal Data Protection Bill, 2019

[8] An Iowa senator has proposed a bill to contain the right to be forgotten to allow citizens to request information be removed from the Internet. He referred to creating a law that would look at a digital right to privacy but also that information once made available can still be removed and updated. See Senate File 2236 available at https://www.legis.iowa.gov last accessed 20 Jan 2021

[9] Pew Research Center reports 74% of US adults want to keep personal information hidden whilst only 23% of adults stated it is more important to be able to discover potentially useful information about others. See 'Americans prioritize right to keep certain personal information from being searchable online' pewresearch.org In addition, researchers found that 85% of US adults thought there should be a right to have potentially embarrassing photos and videos removed from public online search results.

[10] See Lee Andrew Bygrave, *Data Privacy Law and the Internet: Policy Challenges* in (eds) Norman Witzleb, David Lindsay, Moira Paterson, & Sharon Rodrick. *Emerging Challenges in Privacy Law: Comparative Perspectives*. (CUP 2014) Ch 12, 259-289

individual's ability to exercise their autonomy and ultimately dignity in how they are portrayed. A new approach is vital not just with regard to the changing view of privacy for future, more alert generations, but towards a form of safeguarding from what are increasingly seen as the excesses of the ISPs. The view that the development of these organizations is impacting everyday life is still very recent with increasing recognition of their bearing on society.[11] Key to the future of the right to be forgotten will be how it can successfully be applied.

This chapter explores the current position and how recognition of the right to be forgotten for informational self -determination brings a wider remedy to individuals seeking to manage how they are portrayed online. As part of reviewing the application of the right, and how effective it can be, this chapter also looks at the involvement of ISPs, particularly the FAANGs,[12] a term used for those increasingly dominant technology companies, to see how they impact, or potentially threaten, the scope and application of the right to be forgotten. The position will be analysed to see how such entities, now largely responsible for securing the right, can be organized in their approach to it whilst looking at the dangers their growth and market dominance can bring. In doing so there is also the opportunity to ascertain where the right to be forgotten would fit, or be categorized, within existing ideas, laws, and enforcement to ensure its continued use. This chapter also considers how the right, if considered a fundamental right, can be used through the application of human rights such as privacy, dignity, and reputation, and, if so, where and how this can be enforced.

[11] The services and companies now forming an integral part of our digital life are relatively new. Amazon.com began in 1995 as an online shop providing for orders from what was effectively a warehouse system. It now not only provides such shopping facilities considered to be changing the life of the average 'High Street', but also provides communications systems and television services. In the same year (1995) eBay was born, providing 250,000 auctions in 1996 and 2m in 1997. Google was formed a year later, in 1998. The first iPod was sold in 2001, and the iTunes Store opened its online doors in 2003. Facebook went live in 2004, and YouTube a year later.

[12] "FAANG" is an acronym that refers to the stocks of five prominent American technology companies: Facebook Amazon, Apple, Netflix and Alphabet (formerly known as Google) available at https://www.investopedia.com/terms/f/faang-stocks.asp Last accessed 28 Feb, 2020.

6.2 The Right to be forgotten – how to categorize it

From earlier discussion on human rights regarding the issues around privacy and data protection which involved the implications for autonomy, dignity, and reputation for an ability to provide for informational self-determination, it is clear that the right to be forgotten is potentially a multi-faceted right despite it not fitting into normative categorizations of human rights as such. Notwithstanding earlier notions of the need to 'forget' information as seen in the *droit à l'oubli* and *diritto all'oblio*, this right has in effect been formed by the balancing of rights in the decision in Google Spain and subsequent case law. It was then formalized by the more prescriptive right of erasure, as contained in Article 17 of the GDPR. As a minimum, this provides an ability for protection of personal information by removal of the actual information or links to it, through the right of privacy balanced against freedom of expression. It also potentially provides a tool for informational self-determination to promote a sense of self, arising from the rights to dignity and reputation. The parentage of the right may be a result of these aspects of protection, but it may be recognized more by the expansion of rights under the GDPR which has been argued to be a natural conclusion to the decision in Google Spain. The reality is that the right exists behind many doors, meeting the needs of an individual not only with regard to the control of data and the protection of their privacy but through control of information likely to affect their dignity and place in society through reputation.

To some commentators this is not a new right but one that already existed, albeit in diverse forms, and so the ultimate provision of Article 17 to be balanced with freedom of expression merely recognizes its ability to provide such recourse. [13] Artemi Rallo[14] argues that until the right was so recognized 'no other provision had enshrined it because there was no common definition for such legal concept'. He further stated despite such acceptance that it was difficult for any legal system 'to emulate, recognize or protect something that lacked a clear definition in social reality'.[15]

[13] Gabriela Zanfir, 'Tracing the Right to be Forgotten in the Short History of Data Protection Law: The 'New Clothes' of an Old Right' (October 2013) available at SSRN: https://ssrn.com/abstract=2501312

[14] Former director of the Agencia Española de Protección de Datos between 2007 and 2011

[15] Artemi Rallo, *The Right to be Forgotten on the Internet: Google v Spain* Electronic (Privacy Information Center, 2018) Ch 1, 13

In light of the normative requirements for a human right, issues would arise on meeting claims for universality and the right's ability to be an inherent right for all human beings. This should not present the right from evolving with its basis primarily of privacy, as explored in Chapter 2, the influences which would ultimately provide for informational self-determination take an important role in its development and on its scope. The right is gaining definition and clarity as to its extent under the precedents of EU case law, as explored earlier, whilst not yet being clearly demarcated. There is also movement towards its acceptance on a wider basis.[16] This does not mean the right is not now valuable, nor capable of being future proofed, existing as it does as a balancing act between competing humans right. Although it does provide another function, that of a supporting remedy in respect of dignity and reputation, this can be seen to be flexible and used to sustain and support data protection as a fundamental right under the EU's Charter of Fundamental Rights (the Charter) .[17] That is not to say that the right to be forgotten may not develop as values change within societies; certainly, the creation of the International Protocols with regard to cultural rights has shown this.[18] The dividing of rights by the EU towards acceptance of data protection as a fundamental right,[19] accepting and separating this from a right of privacy, has led to greater recognition of the need for new rights. It can also be argued that active data protection representing the fundamental right under the Charter, enforceable through data protection authorities as well as the courts, may have more practical impact than actions under human rights conventions.

[16] E.g, see n7 and n8 See also 'Fujikawa v Google; Japan Case Raises Issue of "Right to Be Forgotten," 'Wall Street Journal, Http://online.wsj.com/articles/google-japan-case-raises- see GF Silvestre, CB Borges, NS Benevides, 'The Procedural Protection of Data De-indexing in Internet Search Engines: The Effectiveness in Brazil of the So called Right to be Forgotten against media companies' (2019) Revista Juridica, Vol 01, No 54, Curitiba pp 25-50

[17] Charter of Fundamental Rights of the European Union [2000] OJ C 364/1

[18] The International Covenant on Economic, Social and Cultural Rights 1966, this involved essentials for life, economic security and cultural identity. Examples of developments can be seen with the African Commission which included a wide range of civil and political rights creating duties on individuals with a first form of 'Collective rights' reflecting the specific needs of the African states, including specifically socio-economic rights. The US had argued specifically against the development of these economic, social, and cultural rights seeing them only as 'aspirations' not specific rights and 'hollow' due under-development. They were however accepted not just within African conventions but on a wider global basis setting out a precedent for new forms of human rights to be recognized. See Alex Kirkup, Tony Evans, 'The Myth of Western Opposition to Economic, Social and Cultural Rights A Reply to Whelan and Donnelly' [2009] HRQ 31 221-238 The John Hopkins University Press

[19] Treaty of Lisbon amending the Treaty on the European Union and the Treaty establishing the European Community 2007c 306/01

However, if the right to be forgotten can also be treated, and ultimately recognized, as a fundamental right in its own right in its widest scope, it could offer additional recourse other than through application of the GDPR. It would seem indisputable that the right to be forgotten exists to support rights of dignity, autonomy, and reputation in its application. As was seen in Chapter 5, the application of the right in various cases has, in particular, resulted in a more moral tone with regard to rehabilitation being taken by the courts.[20] Its usage as a wider concept has also been seen in the decisions made through a similar balancing act at the ECtHR.[21] Increasingly it is seen as a developing right in non-European states, in particular in South America, where we have already seen, the concept of removing information that prejudices the individual's reputation has been acknowledged.[22] This wider acknowledgment is not only due to the implications of the GDPR with its application to protect EU citizens in other jurisdictions[23] but also acceptance of wider controls required over information shown on the internet for an individual as being necessary. An example of the right's broader impact can be seen in Israel where a private bill was proposed to provide for an explicit right to be forgotten,[24] recognizing its involvement in values of human dignity and freedom as protected under Israel's Basic Law but also through legal protection of data privacy.[25] Before this action, cases that have reflected the principles of the right to be forgotten in Israel in the aftermath of Google Spain have been based on the law on defamation accepting the impact on reputation.[26] The use of the right in such a way has also increased the chance of being rehabilitated into society without the prejudice of personal information being readily available, potentially portraying the person in a way that no longer exists or is no longer relevant. The right can also be seen to have value with regard to promoting reputation in

[20] See Franz Werro (ed) *The Right To Be Forgotten, A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia*. (Springer 2018) Ch 12 & 13 review the current situation in Argentina and Brazil with regard to growing acceptance of the right to be forgotten.

[21] see A v Norway (Application no. 28070/06)

[22] ibid Franz Werro

[23] See under Article 3 of the GDPR, the law applies to organizations that process personal data in three circumstances: when a controller or processor is established in the EU and processes personal data in the context of the activities of that establishment; when a controller or processor is not established in the EU but processes personal data relating to the offering of goods or services to individuals in the EU; or, when a controller or processor is not established in the EU but monitors the behaviour of individuals in the EU.

[24] Draft Bill amending the Protection of Privacy law (Amendment - the right to be forgotten, 2017) (P/20/3867) (Isr)

[25] The Basic Law Human Dignity and Liberty 5752-1992 SH no. 1391, p. 150

[26] LCA 4673-15 Barnoi v Savir Mar 8 2016, CA 1139-17 Miller v Ha'Aretez Newspaper Publishing, Nov 19 2017

such a way, confirming existing ideas of identity and personhood, as was seen in Chapter 5, with potentially wider impact than was originally foreseen.

The ability to apply the right to be forgotten as a human right does call into question not only where such a right could fit within the existing treaties and conventions on human rights, but also raises issues regarding new forms of recourse through what have been proposed as digital rights.[27] Defining this new right needs not only to call ISPs to account but to ensure its application is made appropriately. To do this, established rights may need to be translated into binding principles applicable to the Internet. These would not only evoke existing rights but also new rights and freedoms specifically required for protection within the Internet and the digital environment.[28] Although there is no doubt about the difficulties in establishing a global reach, the ability to create any such rights would rest on the capacity for such rights to be universal and global in scope, in fact for these to meet the usual criteria of human rights particularly, as described in Chapter 2. Commentators[29] looking into how such rights would evolve have argued that these would only be formally recognized or promoted when a response is given required, such as, for example, to the Edward Snowden revelations[30]. This scandal had the impact of increased attention being paid to not only privacy but to the transfer and collation of data with the lack of transparency and consent[31] setting alarms bells ringing for many citizens, both in the EU and the US.[32] Before considering how rights could

[27] Giovanni Buttarelli, Privacy Matters: Updating human rights for the digital society, Health Technol., [2017], 7:325-328

[28] ibid Buttarelli '…there has never been a greater need for safeguards against unjustified intrusions into people's personal space by powerful state actors and corporations '

[29] Dennis Redecker, Lex Gill & Urs Grasser, 'Towards Digital Constitutionalism? Mapping attempts to craft an Internet Bill of Rights', The Int Communications Gazette, [2018], 1-18, Here the authors also noted marked increases in the occurrence of the right to data control and self-determination.

[30] The Edward Snowden revelations see: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 last accessed 12 Jan 2021

[31] This is confirmed in the recitals to the GDPR particularly Recital 39 which states 'Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.' In addition, Recital 40 provides for 'In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law,'

[32] Case C-362/14 Maximillian Schrems v Data Protection Commissioner, joined party, Digital Rights Ireland Ltd, [2015] ECLI:EU:C:2015:650 (Schrems I) this case was a natural progression of the concern that arose over access being given to personal data leading through this case to the failure of the entered into the Safe

be secured in the light of the behaviour of the ISPs, it is clear that innovative ways of intervention within the Internet to secure protection for its users must be vital, particularly in light of the growing global strength of ISPs. The ability to store and access data through the internet has created the phenomenon of the digital memory which, unlike the human mind, does not fade as information ceases to be relevant.

Whilst the right to be forgotten is not yet capable of being seen or formally recognized as a human right within existing conventions, it does offer a new ability for a person to not only control data in line with the EU's holding of data protection as a fundamental right but to protect privacy, ensuring the desired portrayal of self, whilst maintaining an online identity. in accordance with requirements of reputation and rehabilitation. This meets the requirements of societal order with time allowed for memories of past events to fade and for matters that would be detrimental, if forming part of an eternal digital identity, to be made less easily available. Ideas attached to the value of privacy which recognize the need to observe human dignity through autonomy can provide additional protection for reputation through the use of a wider form of the right to be forgotten. Focus on the right to be forgotten as a limited recourse, argued by Artemi Rallo, [33] considers it 'purely a right in the face of technology providing endless access to personal data'. However, he notes, 'are we forgetting that this is a wider right once to be exercised in other contexts not just against search engines as was found in Google Spain or against data controllers under Article 17 can it also be the case that this could be exercised in a much wider field?'[34] Where the right to be forgotten can be considered as evoking much wider scope, it is clear that in an online based society it has additional and valuable impact to ensure other human rights are also respected.

There are counter arguments to acceptance of the right to be forgotten in its widest form to be seen as a potential fundamental right. These can be based on it not being considered as

Harbour agreement between the EU and the US and subsequently to the challenges of its successor the Privacy Shield (see Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, [2015] ECLI:EU:C:2020:559 (Schrems II)

[33] see n15 Artemi Rallo, Ch 1, 13 -46

[34] ibid, here Rallo also raised concern that the information making profiling easy did not just impose on privacy but may also 'threaten the reputation of individuals and hence their own liberty and dignity' questioning whether the right included a right not to only 'leave the past' behind but also to a 'clean slate' see p 17

essential or even as important a right if all that is required, other than any process created by Google or other search engines or under the implementation of Article 17 of the GDPR, is for a global data deletion principle. [35] Rallo has contrasted proposals offered by Benjamin Keele[36] arguing for the destruction of data securely when no longer required in line with principles of consent with explanations by Jef Ausloos[37] concerned with regard of the maintenance of freedom of expression. Rallo argued that effectively the right to be forgotten can be claimed to have become an obligation to adopt technical measures to achieve the intended purpose.[38] It is on that basis that it can be argued that the right of erasure under Article 17 now supersedes previous debates in an attempt to define the limits of the scope of the right. However he believes that this is not truly the case as on this basis, the use of it would be more purposed towards the elimination of the supply of information.[39] Rallo's view is that the wider debate on the right to be forgotten involves future risks for the Internet for not just privacy but 'for reputation, privacy, liberty and human dignity.'[40] In this instance, despite the right to be forgotten being termed as similar to a fundamental right, he looks at how data protection only operates on a balancing premise so in a similar way to how the right to be forgotten can be exercised meaning increased status is not required. The right to be forgotten could be considered, however, to take equal place in obtaining a new level of control outside data protection and privacy and therefore, beyond the scope and limited principles of Google Spain and the procedural requirements of the GDPR. It is clear that recognition of the right to be forgotten as a fundamental right is still ongoing and subject to further debate. This has been considered most recently by the German Constitutional Court (the *Bundesverfassungsgericht*) where it deliberated on a request for removal of reference to a

[35] See n15, Artemi Rallo, p 20

[36] Benjamin J Keele 'Privacy by deletion; the need for a global data deletion principal'. (2009) Indiana Journal of Global Legal Studies Vol. 16, Iss , Art 14, p363- 384. in particular p 366 'Until a data deletion principle is adopted as an integral part of a data protection regime that protects privacy while permitting global data transfers, no data protection scheme will be complete.' Available at: https://www.repository.law.indiana.edu/ijgls/vol16/iss1/14 last accessed 24 Feb 2021

[37] Jef Ausloos, 'The Right to be forgotten - Worth Remembering?' (2012) Computer Law and Security review, vol 28, p. 147. Initially stating 'Enabling a more effective control by the individual the introduction of a (well defined) "right to be forgotten" therefore seems appropriate at first sight.' he goes on to argue 'In its original form, the 'right to be forgotten' only comes *ex post*, conflicts with free speech (enabling subtle censorship), is very hard to effectively implement in practice and only postpones the illusion of choice.'

[38] see n15 Artemi Rallo p 40

[39] see n15 Artemi Rallo p 40

[40] see n15 Artemi Rallo p16

murder conviction[41]. Here the Court did not focus on privacy but on the balancing of freedom of expression through the press with other rights such as 'personality rights.' Recognizing that these rights are not fully harmonised by EU law, it fell back to considering the fundamental rights guaranteed by the German Basic Law and applied these. A further case at the same court even more surprisingly followed the principles of Google Spain but confirmed the Court's competence to hear applications concerning fundamental rights with the CJEU only hearing general questions not yet settled.[42] With applications still to be made under Article 17 acknowledging the fundamental right of data protection provided by the Charter, it is still not clear where the right to be forgotten whilst recognized as a right fits into concepts of fundamental rights and how such should be fully enforced.

6.3 The exercise of the right to be forgotten; has it made a difference to an individual's existing rights?

Within recognition of the right to be forgotten it is important to see, whether as a fundamental right or as a process under the GDPR, how this can support an individual to offer protection in terms of how they are perceived in society. The purpose of the right is ultimately to lessen the impact of easy accessibility to personal information about their lives and to provide additional support for the control of such information thereby providing informational self-determination. This however can only be successful if there are the means to enforce such right.

6.3.1 Application of human rights in an online environment

It is accepted that the use of the Internet has created an environment where 'the web has become a forum where everyone can effectively exercise their civil, economical, and political rights' and that increasingly 'it is the place where one can develop one's social personality'. [43] The acceptance of the loss of privacy due to activities online is now challenged, as already discussed, with debate on

[41] 1 BvR 16/13 6 Nov 2016

[42] 1 BvR 276/17 This was based on similar facts to those of Google Spain involving the reputation of a business man however the decision weighed this with the potential restriction of a TV's channel's freedom of expression finding in favour of Google. The controversy raised by this case reflected that for 30 years the review of such cases had been left to the CJEU now it was the turn of the German court to intervene and supervise national courts to carry this out.

[43] Mario Viola de Azevedo Cunha, Luisa Marin, Giovanni Sarto, 'Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web' International Data Privacy Law, (2012) Vol 2, iss. 2, 50-67

the inability to protect how you are portrayed to prevent the use of personal information impacting your dignity and your reputation. The loss of dignity indirectly impacts how you are considered within society, after all nobody wishes to be ridiculed or ostracized. Despite acceptance of how widely privacy can be compromised within the Internet, freedom of speech, once considered to be the redeeming feature of the availability of data, is considered by many to be in jeopardy, arguably as a result of the new acceptance of the right to be forgotten, in particular when the ability to 'forget' past events is seen as providing an opportunity for history to be rewritten.[44]

There is a clear need to consider the balancing of interests when deliberating on how an individual can now assume responsibility for using their ability to exercise the right. This is primarily through the Google process[45]- to determine how they are portrayed, or as a minimum, to protect the use of their personal data. Through this they would be able to control the building blocks of identity via the erasure of information, or by a process of de-linking. When looking at the right to be forgotten from this angle of informational self-determination, whether there can be the ability to choose the personality desired to be portrayed is dependent on the success of this process. The individual will determine which information they want removed and use this to form the 'shape' of the person they wish to have portrayed. However, as we have seen, freedom of expression and public interest may well override the privacy interests of the individual. As recognised by the EC in an earlier factsheet; 'the right to be forgotten is not about rewriting history'.[46] Any exercise of this right is made through a balancing of human rights, although carried out by a party that must be considered to be less than interested in considering the impact on an individual,[47] leaving it

[44] In a movement away from the priority of freedom to express opinions, make comments, etc., the companies now hosting such forums, e.g., Twitter and YouTube, are now being held accountable for posts that promote hatred, crimes, acts of terrorism, violence, and similar activities. An alternative reaction, also restrictive, has been the approach by the former US President Trump to demand that such platforms are no longer allowed to 'note' posts that might be inciting such the use of guns. See The New York Times 29 May 2020 available at https://www.nytimes.com/2020/05/29/technology/trump-twitter-minneapolis-george-floyd.html This has resulted in further action whereby Twitter has now suspended the accounts used by former President Trump as a consequence of the use of language likely to incite violence, an action widely held to be unconstitutional as against freedom of expression under the 1st Amendment of the US Constitution.

[45] Google's 'Right to be forgotten' process available at https://policies.google.com/faq?gl=uk

[46] Factsheet on the 'Right to be Forgotten' ruling (C131/12) Issued 03-06-2014 http://ec.europa.eu/justice/dataprotection/files/factsheets/factsheet_data_protection_en.pdf

[47] Evan Selinger, Woodrow Hartzog, 'Google can't forget you, but it should make you hard to find', "Wired", 20 May, 2014. Available at https://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-

questionable as to how the right can be applied beneficially. The ability of a commercial entity to apply the right and for an individual to be able to progress any recourse should they wish to dispute the decision to remove or de-link information is, at the least, questionable.[48] It is clear that the position of enforcement of the right has presented many challenges, not least the fact that there was a need to balance the right to apply it with other fundamental rights.[49]

In examining how other rights may be included in the widest interpretation of the right to be forgotten, the rights of dignity and autonomy form the underpinnings together with privacy but this wider approach to the right to be forgotten allies more closely with ideas of reputation and acts that evoke informational self-determination. This was shown indirectly in the PJS case,[50]and to some extent in the NT cases,[51] and is often linked to a person's reputation. In PJS, the intention was to secure protection that would stop information (i.e., a journalist's report being made readily available) which would then impact the public perception of the individual as a family man, not one whose sexual life would have been seen, at the least, unconventional. Being able to 'forget' accessible information would have retained this persona so anxiously desired. To enforce reputation as a right can be troublesome and limited, as has been shown in Article 10 of the ECHR and discussed in Chapter 2, where reputation is only declared to be an exception, or limitation, to the right of freedom of expression, which remains of paramount interest. Where information is made readily available, e.g., through the Internet and on a global basis, claims in respect of reputation can be difficult to pursue through the courts and do not necessarily result in the removal of information.

hard-to-find/ last accessed on 24 May 2018.

[48] Patricia S Abril, Jacqueline D Lipton, 'The Right to be Forgotten: Who Decides What the World Forgets?' (2014) Kentucky Law Journal: Vol. 103, Iss. 3, Article 4 available at: https://uknowledge.uky.edu/klj/vol103/iss3/4

[49] David Erdos, 'EU Internet Enforcement after Google Spain, Report of Proceedings' Centre for European Legal Studies Faculty of Law. University of Cambridge, 2015. Looking at the need to apply a balance of fundamental rights, he stated 'there would seem to be support for the idea you did need to have a balance with other fundamental rights', but also that this idea would only come into place and change when such resources and in particular budgeting resources that regulators have available in this area can be used to perform what, in an Internet area, are more and more important tasks of balancing people's rights to be protected against freedom of expression.

[50] PJS v News Group Newspapers Ltd [2016] All ER (D) 120 (Apr) see also European Law blog, http://europeanlawblog.eu/?p=2931 last accessed 10 Nov 2019

[51] NT1 & NT 2 v Google LLC [2018] EWHC 799 (QB)

Also, within this convention, as indicated by Aplin, there is no balancing of two competing rights of equal importance to be applied in respect of protecting reputation, as was seen in the decision in Google Spain. This trend may be changing as the ECtHR has shown, albeit inconsistently, in recent cases. For example, the ECtHR found in Radio France & Ors v France [52] that freedom of expression and reputation could be treated as equal rights with a requirement for a fair balance between the two but, regrettably, there has not been any development since these early steps. In another later case, pre-Google Spain, there was indication that harm to reputation would not always involve or evoke remedies under Article 8, the right to privacy.[53] Aplin goes on to argue that the approach by the Court has been 'inconsistent and confusing'.[54] None of this helps the individual to take control of how they are portrayed in an effort to maintain dignity through their reputation.

Aplin also refers to there being an acceptance that reputation is a new concept distinct from 'character' approving the view that character refers to 'actual attributes or personality of a person.'[55] This is where a person may look for informational self-determination through the right to be forgotten as a way of ensuring their portrayal within their community matches and fulfils their reputation to enable them to continue a successful life within that society. Reputation can be claimed as a concept that is founded by your role in society, how you go about your life within it, and most importantly how you are perceived by others. There are clearly consequences if your reputation changes or is compromised, whether by your own actions or by those of others. Ideas of personality or character are often now less focused on carrying out roles within society than they are on the ability to determine how you are portrayed as an individual, particularly now online. A lack of character would also have subsequent consequences on reputation. The ability to allow information about you to be

[52] France & Ors v France (2005) 40 EHRR 706

[53] Karakó v Hungary (2011) 52 EHRR 36 [23] Here it was shown that the necessity of often proving the 'seriousness' threshold introduced under the jurisdiction of the Strasbourg court[53] has linked the harm to reputation to the impact on the private life being substantial so as to have constituted 'such a serious interference with his private life as to undermine his personal integrity'.

[54] Tanya Aplin, Jason Bosland, *The Uncertain Landscape of Article 8 of the ECHR: The protection of reputation as a fundamental human right*. in A. Kenyon (ed) *Comparative Defamation and Privacy Law* (CUP, 2016), Ch 13. Available at SSRN: https://ssrn.com/abstract=2674113

[55] Eric Barendt, 'What is the point of libel law?', Current Legal Problems, Vol 52, Iss 1, 1999, 110–125, available at https://doi.org/10.1093/clp/52.1.110 last accessed 20 Jan 2021

disclosed, or to be made available, links with the human ability of people to forget past events linking this also to universal concepts of dignity and autonomy. Choosing how much information is available can influence how you are portrayed, whilst ensuring the ability to exercise autonomy as well.

6.3.2 The ability to re-invent yourself through the right to be forgotten

To many the question of reputation is key to the value of the right to be forgotten and the need to exercise this through whatever methods are available. Just as a convicted murderer seeks the chance to 're-invent' themselves, for many the loss of control over how one is presented to society is more than just advantageous and protective of reputation, it is vital in impacting many aspects of life, both public and private. For example, the Google version of a person may be very different to that presented on Facebook or Snap Chat, or even LinkedIn. To some extent such persona is under the control of the individual, so for example the happy, inspirational, pleasure seeking life portrayed on Facebook may not be of concern as this is largely provided by the subject themselves, or generally by persons known to them (i.e., friends or friends of friends, rather than Facebook). However, there could be a different view provided to the public through official routes, e.g., bankruptcy orders or criminal convictions. The alternative offered by Google may well include removal of access to deeper, darker secrets or at least omissions from a more usually acceptable social existence. There may be various public versions available of one person with some versions under their control, but with many which are not. Various remedies may be activated to help regain control of this situation, whether recourse through defamation or other legal actions, but often attempts to gain such autonomy fall between existing remedies. This leaves the right to be forgotten as a potential solution to provide informational self-determination to help the 'data double' be reconstructed.

6.4 The future of the right

The right to be forgotten as a complex tool for informational self-determination needs to be enforceable to ensure the protection of such rights. Examining the current way in which the right is enforced can help bring into focus a way forward which ensures that the right is used to maximum effect, and that it can be expanded to provide a future proofed remedy.

6.4.1 The ability to apply the right through Data Protection

Challenges exist not just in determining how the scope of right to be forgotten can be viewed, but if accepting the ability to use it as a tool for informational self-determination, how this can be enforced through data protection. The provisions of the GDPR, superseding the DPD with the right to be forgotten, as created under Article 17, have ensured that the relevant data protection authority is at first instance the appropriate entity to safeguard this right. The application of such provision, however, is not as straight forward as would initially appear.[56] It is also clear that with regard to enforcement under Article 17 this could be limited in scope by a stricter interpretation to a right to be delisted, primarily excisable against search engines. However, if looking at a broader approach to the right as determined under the provisions of the Google Spain case, then it would appear that the controller of the data is also the arbitrator or decision maker as to what information is being 'forgotten'. There is a process to appeal to a data protection authority or ultimately to a court, but when looking at the figures made available the percentage of applications following rejection of claims for delinking by Google to a data authority remains very limited.[57] This might be considered to be part of a natural reluctance to incur the expense of taking an action, certainly when accounting for the amount of time it will take or when an inherent belief is held that the end result will be the same. In looking at how the ability of the GDPR generally offers the required level of protection it is already being noted that in the initial two years after its implementation, despite being considered to have provided a model for other jurisdictions, it is argued to be failing in the challenges of enforcement. It is also clear that although the recourse, whether under Article 17 or the perimeters of Google Spain, is through application to the member states of the EU that there are, and will be, different approaches to the application in different member states, removing the ideas of consistency.

[56] Alberto Miglio, *Enforcing the Right to Be Forgotten beyond EU Borders, Use and Misuse of New Technologies*, in (eds) Elena Carpanelli, Nicole Lazzerini, *Contemporary Challenges in International and European Law* (Springer 2019) pp 305-326. Miglio has looked at what he refers to as the global nature of the web which makes the most online activities intrinsically multi-national, thereby potentially justifying jurisdictional claims by multiple states.

[57] For example as of November 1, 2015, just over 30% of requests to Google under the right to be forgotten process had been escalated for a second opinion.

Artemi Rallo[58] puts forward an argument, closely linked to ideas of informational self-determination, based on the need to resolve enforceability of the right by looking at concerns around '[i]ndividuals' inability to review, update, rectify or challenge personal information available online [which] necessarily implies a restriction of individual freedom which basically translates into self-censorship rather than digital withdrawal.'[59] Here he places an obligation onto the data subject to ensure that only information they want to be available is made available, for example on social media platforms such as Instagram and Facebook. In effect this is a form of self-regulation aimed at reducing the information available, but it cannot take into account the freely available information being collected by algorithms and manipulated to provide this digital identity. If the right to be forgotten is imposing another form of regulation, it is not just on the entities collating the information but on individuals themselves. Other than by actions taken by the individual to limit their personal information, the ability to request removal of information, or specifically links to information (URLs), through an accepted process is vital in order to reduce potential universal access to information deemed irrelevant to that individual's life now. Is the necessity for such vigilance, not to mention the potential for such applications to fail, to be part of the price paid by members of society to be able to enjoy the free flow of data through the Internet? This however can only be a limited response, it does not consider the total data collected and accessed which is collated from other sources, applied by other entities, and shared outside the confines of where it originated.

Universal access to personal data shared on the Internet to which the subject has not agreed or been aware of can be detrimental to the level of social recognition and access to social activities needed to maintain one's place in society and take an active part in fulfilling usual human social needs. In addition, as argued earlier, such unwarranted access can be harmful to an individual's reputation and potentially be self-limiting on the ability to be oneself or to live your life as required. The ability to provide self-censorship in the form of determining the information made available through the use of the provisions of Article 17 takes only a limited step toward the utilization of the right to be forgotten. As discussed in Chapter 5, only if there

[58] see n15 Artemi Rallo p17

[59] see n15 Artemi Rallo p17 see also Viktor Mayer- Schonberger, '*delete*' *The Virtue of Forgetting in the Digital Age,* (Princeton University Press 2009) p 128-134

is an adequate process or application of rights can the right provide a form of self-determination in respect of information available and present an individual in the way they so require ideally portraying the best version of themselves.

Underlying the ability to enforce fundamental freedoms and rights, not only for privacy but for data protection or control, must be to focus on 'fairness.' This concept also forms the basis of the ethical approach within the EU to anti-competitive behaviour and consumer protection generally.[60] Should an individual need to be restrained in their ability to provide or permit access to information because of the wider activities of the Internet giants? If so, how would this fit with such ideas of fairness. It is arguable that data processing and similar actions can be challenged if they do not meet the EU's criteria for the protection of the individual in such a data driven environment. Whereas data protection systems appear to provide effective enforcement routes, established by mature development of individuals' rights and backed by laws and regulations and a wealth of precedents, the right to be forgotten is not only new but relatively untried. Accordingly, the ability to define its scope and outline the nature of its function, particularly as to whether it is a new form of fundamental right, has been limited.

However, it could be argued that these existing legal regimes may be useful in ultimately identifying how the right to be forgotten can be focused to bring about appropriate protection. This can be seen in the actions taken by the Italian Competition, Communication and Data Protection Authority, the *Bundeskartellamt* (the German Federal Cartel Office), and the French Data Protection Authority (CNIL). The challenges bought about by the need to enforce the right, initially through application to search engines, has inflated concerns not just with regard to fairness but to the integrity of these entities themselves. An analysis carried out by Stuart Hargreaves[61] has shown that the use of algorithms to automate large volumes of requests for removal of contents that could range from copyrighted material to

[60] Inge Graef, Damian Clifford, Peggy Valcke. 'Fairness and enforcement: bridging competition, data protection and consumer law' International Data Privacy (2018) Vol 8, No 3, 202, here the authors state '...the overlaps between the field of competition, consumer and data protection as regards their substantive principles are particularly apparent in relation to practices involving the collection and use of personal data of individuals'.
[61] Stuart Hargreaves, 'The Trouble with Using Search Engines as the Primary Vector of Exercising the Right to be Forgotten,' The Chinese University of Hong Kong Faculty of Law, Research Paper No. 2016-23 available at SSRN-id2873391.pdf last accessed 12 Dec 2020

pornography has had to be developed to be applied in right to be forgotten requests. This he describes as a much more complex process and one that does not work well with machine learning techniques. As he states, '[p]roper implementation requires a complicated balancing off of the privacy rights of the data subject against the free expression or access to information rights of the public; this is not something that can be decided algorithmically'.[62]

As these entities would be applying and enforcing the right but are not regulated, are there sufficient regulation or enforcement practices in place to ensure a uniformly consistent approach to how the right is applied? This leads then to examination of not only the role but also the extent of the power of the ISPs, and in particular the search engines, and how this can impact the ability to fully exercise the right to be forgotten to provide informational self-determination.

6.4.2 Enforcement of search engine responsibilities

With the finding of a search engine being construed as a data controller in Google Spain, the tide began to turn away from forming a protective regime for search engines.[63] Without doubt the ability to enforce and ensure protection under a right to be forgotten, whether under the principles established by Google Spain or under the GDPR or indeed under developing regulation within other jurisdictions, relies very heavily on such entities as Google, albeit reluctantly, being the main recipient of the ability to determine the right, potentially a quasi-regulator. The extent of the power of Google can clearly be seen in the level of profits it has been able to command and particularly its virtual monopolistic behaviour. The reality is that since its start up in 1996, initially created to rank the importance of different websites in Internet searches, its ultimate income has risen from $40 million in 2001 to $55 Billion in 2013. [64] The latest figures available suggest that for quarter two of 2019 the income for Alphabet, the Google holding company, had risen to $38,782 billion. However, another

[62] n 61 Stuart Hargreaves p. 21

[63] n15 Artemi Rallo, Here Rallo argues that in fact this was a natural reaction in trying to deal with the new environment as such entities could no longer get the protection of being construed as having no journalistic control over contents.

[64] The last formal figure recorded before the formation of a holding company structure. The parent company Alphabet was formed in 2015 to hold Google and various other subsidiaries https://money.cnn.com/2015/08/11/technology/alphabet-in-two-minutes/index.html last accessed 4 Sept 2019

measurement of the power of the online service providers is also to compare this with the loss of revenue from mainstream media. Newspapers noted a corresponding loss of revenue which accelerated with the growth of the Internet and its increasing ability to attract advertising. In the opinion of Tom Baldwin, the initial idealism of the Internet and its usage began to evaporate in the first decade of this century.[65] The importance of this is slowly being realized in conjunction with the impact on the freedom of expression as well as privacy. This is partly due to the escalation of the new criteria of 'fake news', reflecting and building a feeling of mistrust in more traditional means of journalism.

Originally, some member states decided to expressly provide for the protection of search engines, potentially to encourage the free flow of information and aid commerce. Whilst a consultation paper on the Electronic Commerce Directive published by the UK's Department of Trade and Industry in 2005[66] advised that "[w]hilst it was not necessary for member states to extend the provisions of Articles 12 to 14 of the Directive to cover ... location tool services [i.e. search engines] to correctly implement the Directive, the Commission encouraged member states to further develop legal security by so doing". The idea was to provide protection for 'online service providers' to provided such services whilst only observing the rules of the EEA country they operated in. Additionally under Article 14 there was protection from liability where the was no actual knowledge of the harm. The UK chose not to extend regulations to expressly cover search engines, apparently on the basis that no cases have emerged that suggested such a provision was necessary or desirable; a decision that would later be shown to be ill-advised as the power of such entities increased.

The initial approach to search engine activities, as discussed, was to offer protection from liability, certainly by the EU but particularly in the US.[67] The decision in Google Spain without

[65] Tom Baldwin, *Alt Control Delete: How Politics and Media crashed our democracy*, (C Hurst and Co 2018) Ch 4, 133/135

[66] Available at; https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/272133/6536.pdf last accessed 20 July 2020

[67] The EC has encouraged member states to extend protection to search engines since the borderless nature of e-commerce was thought to require that the framework put in place for its operation should provide legal certainty both for business and consumers: see the observations made in the Commission's first report on the Directive, dated 21 November 2003.

doubt confirmed a differing approach, representing the start to a change in focus with new recognition of the values that potentially could be impacted by such activities. This was clearly indicated by the CJEU ruling against the opinion of the AG in Google Spain, which perhaps represented the status quo at the time of the decision.[68] The position in the US with regard to search engines remains clearly one of commercial protectionism.[69] For US commentators the forging of the right to be forgotten was of great concern as the impact of the case increased the resolution of the EU to finally hold a search engine accountable. This not only went against the opinion of the AG, but it also went against the protection previously offered towards such entities.[70] Despite the clear arguments as to why search engines should not be liable (an aspect that was re-explored in the NT1 & NT2 decisions[71]), here Google had been unable to persuade the court that mere automation had created the results, and that therefore it could not be held liable. The CJEU did not apply the benefits of the previous directives and existing caselaw with an approach that seemed finally as if it was determined to rein in Google's activities.[72]

The views on search engines, as previously expressed, had been demonstrated in various cases, in particular the case of Metropolitan International Schools Limited.[73] Here there was an opportunity for a review from the UK's perspective of the approach towards search engines with Goggle arguing that it had been joined in the action incorrectly. As a result, the judge determined that an explanation of a search engine's role was necessary in this case to set out the position succinctly. Stating that, '[o]bviously Google has no control over the

[68] Case C -131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, [2013] ECLI: EU:C:2014:317, Opinion of Advocate General Jääskinen in para 32 -35

[69] There is an important provision contained in s.230 of the Federal Communications Decency Act,1996, 47 United States Congress, to the effect that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".

[70] This was a recent case in the Court of First Instance in Madrid on 13 May, 2009: Palomo v Google Inc. The complaint was in relation to search results providing hyperlinks to sites carrying defamatory content. The claim was rejected, and the Third Defendant held not liable in law for disseminating third party content. Reference was made to European legislation moving towards the position that there should not be any obligation on Internet intermediaries to supervise such content. Where "actual knowledge" (in the sense defined above) has not been established, the law provides for "exoneration from responsibility" on the part of businesses offering intermediary services.

[71] Joined cases of NT1 & NT 2 v Google LLC [2018] EWHC 799 (QB) para 161

[72] This was consistent with the approach taken by the EC with regard to anti-competition measures at that time.

[73] Metropolitan International Schools Limited (t/a SkillsTrain and/or Train2Game) claimant - and -(1) Designtechnica corporation (t/a digital trends) (2) Google UK limited (3) Google Inc. [2009] EWHC 1765 (QB)

search terms entered by users of the search engine or of the material which is placed on the web by its users',[74] Mr. Justice Eady determined that,

> 'There appears to be no previous English authority dealing with this modern phenomenon. Indeed, it is surprising how little authority there is within this jurisdiction applying the common law of publication or its modern statutory refinements to Internet communications'.[75]

Reference was then made to the relevance of the role played by Internet intermediaries in the cases Godfrey v Demon Internet Ltd and Bunt v Tilley.[76] In determining whether the relevant Internet intermediary was 'knowingly involved' in the publication of the relevant words,[77] it was held as a matter of law, that if the search engine had no more than the role of a 'passive medium of communication,' it could not be characterized as a publisher in common law. Despite arguments that this was potentially against the public policy underlying Regulation 17 of The Electronic Commerce (EC Directive) Regulations 2002[78] for a search engine to be liable for what was viewed by the judge to be 'placing signposts at the end of conduits, thereby assisting the public to choose which routes to take, when the operator of a conduit would be exempt from liability,' it was argued further by the claimants that,

> 'If it is in the public interest for such conduits to be freely accessible it must be in the public interest for information to be made available to assist the public in deciding which conduits to access.'[79]

However, key in this decision was the concept of 'free services' being offered which, with hindsight, shows how the prevailing attitude to the regulation of search engines has so fundamentally changed with acceptance that the price being paid for such services is personal data. A mere ten years previously it had been said that,

> 'It is difficult to see how the Third Defendant's search engine service could, in any ordinary meaning of the term, be described as "for remuneration" in circumstances

[74] n73 para 13 f)
[75] n73 para 35
[76] Godfrey v Demon Internet Ltd [2001] QB 201, Bunt v Tilley 2007] 1 WLR 1243at 22-23
[77] Bunt v Tilley [2007] 1 WLR 1243 at 22-23
[78] 2002 Regulations (Electronic Commerce (EC Directive) Regulations (SI 2002 No 2013)
[79] n73 para 46 (v)

where the user of the Web does not pay for the service. It is true that remuneration is obtained through advertising, but it would be a distortion of language to describe the service as being "for remuneration" purely for that reason.'[80]

This would normally mean that the person receiving the service had to pay. Much may depend, however, on specific statutory definitions, although the view is now largely superseded by acknowledgement that this is no free service, a loss of privacy and control are in fact the fees paid.

Despite the change of approach, whether the right to be forgotten can be effectively and fully enforced against search engines brings further challenges. Some of these have already been touched upon with regard to the jurisdiction and the extent that the search results are affected. [81] The approach taken by CNIL has been to argue ceaselessly for the removal of links to be more extensive. The success of this approach, which has taken Google through various appeals, has now changed direction as the result of an opinion issued by AG Szpunar in Google LLC v Commission nationale de l'informatique et des libertes 2019 [82] and the subsequent decision in the case.[83] The focus of the opinion rested on how the right could be applied geographically, looking at the difficult determination of the extent between territorial limitations and domestic jurisdiction It seems as if Google has been using geo-blocking techniques to prevent access within the EU but not outside it. This was despite arguments, largely from France and Italy, that wider removal was essential to ensure the right to be forgotten was fully applied, and in France this came with practical deterrents in the form of hefty fines. [84] The outcome of the referral was of great interest, receiving conflicting support so that, for example, whilst France, Italy, and Austria have advocated for worldwide

[80] n73 para 82

[81] The position ensured that ultimately under Google Spain principle only the removal of links within Spain was allowed, but it was felt that without recourse to Google.com the right to be forgotten would be limited and therefore ineffective.

[82] Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), [2019] ECLI:EU:C:2019:15, Opinion of AG Szpunar

[83] Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) [2019] ECLI:EU:C:2019:772

[84] In March 2016, a fine of Euros 100,000 was levied against Google 'The only way for Google to uphold the Europeans' right to privacy was by delisting inaccurate results popping up under name searches across all its websites', the Commission Nationale de l'Informatique et des Libertes (CNIL) said in a statement on Thursday https://www.reuters.com/article/us-google-france-privacy-idUSKCN0WQ1WX last accessed 14 Dec 2020.

application, Greece, Poland, and Ireland have sought limited application. The opinion of the AG, however, was firmly that searches made within a member state and searches made from third countries should be treated differently, primarily due to territorial considerations. Here, the AG stated that Art 52 of the TEU[85] only applies to member states and does not therefore create external obligations, arguing that only very specific European provisions should have ex-territorial effect and these did not justify application to the Internet as they were only 'extreme situations of exceptional nature.[86] This has subsequently been confirmed by the court's decision in the case largely accepting Google's argument that to allow the extent of the delinking on a global basis was against international law which continued to be applicable.[87] However, here the case did validly cite concern that the exercise of the right together with the balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users on the other is likely to vary significantly around the world.[88] There is no guarantee that a consistent approach would be taken. For some this represented promotion of the ability to export 'EU data ethics' to the wider world, potentially increasing the European approach to the wider world.

There is undoubtedly a resulting lack of reasoning behind this decision with regard as to why the right to be forgotten would be limited to such an extent.[89] It is clear that leaving the ability for full search results to be viewed through alternative access to the Internet effectively removes the 'forgotten' aspect of the right. The CJEU's decision did however reconfirm that there would still be provision for a state to carry out the balancing exercise according to its

[85] Treaty on European Union (OJ C 191, 29.7.1992, pp. 1-112) (TEU) also known as the Treaty of Maastricht on European Union

[86]. C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) [2019] ECLI:EU:C:2019:772 para 47

[87] C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) [2019] ECLI:EU:C:2019:772 para 38. 'In addition, by adopting such an interpretation, the CNIL disregarded the principles of courtesy and non-interference recognised by public international law and disproportionately infringed the freedoms of expression, information, communication, and the press guaranteed, in particular, by Article 11 of the Charter.'

[88] ibid para 67

[89] Although it was accepted that the EU's use of the GDPR did not give it the ability to compel other states to accept the right to be forgotten especially under international law which did not recognize the concept it was also clear that the decision would not impede the coverage of the GDPR and that the CJEU was considered to continue to prompt debate on the global extent of EU data protection including where appropriate the right to be forgotten. By co-incidence a case (Case C-18/18, *Glawischnig-Piesczek*) had held just days before the CNIL case allowing the blocking by a member state for access to unlawful information on a worldwide basis.

own jurisdiction and views. This potentially makes it possible for national courts to order global delisting by a search engine in certain circumstances where the balancing act results in favour of an individual's privacy.[90]

Despite the decision in Google Spain and the implementation of Article 17, the case does provide a roadblock to the effective roll out of the right. As was seen in the PJS case, use of the Internet comes with the result that personal information is readily available on a potentially global basis. Whereas the AG's opinion and the CJEU's subsequent decision were understandable, the ultimate result is that the right is effectively fettered. It will need to be seen how the new precedent will be followed strictly and interpreted to provide for some additional restriction of information and how the loose reference to the balancing act required will be defined and implemented.

6.4.3 The application of competing rights by ISPs

With a balancing of competing rights now confirmed as being required for the exercise of a right to be forgotten, recent arguments have increased for the strength of the internet entities to be limited. Such restriction could already be seen to be provided through the application of existing rules, increased taxes, and through fines, or more vehemently through Internet regulation. This is not something new as more or less since the evolution of the Internet some form of unease has been expressed regarding the growth of such entities with a desire to create such boundaries. Recent years have increased the pressure, particularly on states, to provide valid and effective forms of control. This has been referred to by some academics as 'digital constitutionalism' in view of the lack of acceptance of a more specific term to describe the debated process[91]. Such ideas may also provide what might be considered political aims which focus on the governance and limitations of power of the ISPs.

With regard to this ambition, there have been various proposals put forward, particularly since the late 1990s, although with no uniformity of approach. However, there is some

[90] Mary Samonte, available at https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/ last accessed 12 Feb 2020

[91] Dennis Redeker, Lex Gill, Urs Gasser, 'Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights', [2018] The Int Com Gazette pp 1-18

commonality of theme which largely involves ensuring that existing civil rights are extended to an online environment so that legal principles are followed where appropriate, albeit in new forms.[92] This would also include specific new 'rights' formulated for the Internet and the online environment, i.e., potentially a bill of rights for the Internet. From the various drafts made to meet such requirements, it could be argued that there are distinct areas which appear to have been prioritized, namely from the rights of freedom of expression and privacy through to much more prosaic rights such as accessibility. Key themes include transparency and openness, both of which appear to be of significant concern when considering how data is collected and accessed. Most recently progress in establishing rights in the form of the EU Digital Services Act has been made where it has been made clear that search engines are included in the intention to define the roles and impact of providing digital services. [93]

There have been futile initial attempts at providing a draft to incorporate the type of rights required with no universal theme as yet agreed. However, it should be noted that the attempts to date have come from many other organizations and have included initiatives by private individuals.[94] This must be considered to be a fair response to the lack of, or limited, involvement by the Internet based companies themselves and the diversity of opinion on how much stance a government or regulatory body might take. Other organizations who have taken on the issue include the Electronic Frontier Foundation, leading the way with an initial offering for a bill of rights in 2010. The subsequent European Digital Rights group (EDRi) also

[92] This could be argued to have included the right to be forgotten in its application of existing data protection regulation as well as existing human rights, such as privacy and freedom of expression. See Dennis Redeker, Lex Gill, Urs Glasser; 'Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights' [2018] The Int Com Gazette, pp 1-188

[93] As part of the European Digital Strategy, Shaping Europe's Digital Future, it was announced that the European Commission would upgrade the rules governing digital services in the EU. The European Commission proposed two legislative initiatives: the Digital Services Act (DSA) and the Digital Markets Act (DMA). The DSA and DMA have two main goals: to create a safer digital space in which the fundamental rights of all users of digital services are protected; and to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally. see https://ec.europa.eu/digital-single-market/en/digital-services-act-package last accessed 20 Feb 2021

[94] Council of Europe's Declaration of Internet Governance Principles 2011, formed the draft Charter of Digital Fundamental Rights of the EU 2016, proposed by a German group of individuals seeking to propose a charter to modernise the existing Charter on Fundamental rights, recognizing the need to update rights in the light of an ever-changing technological society. e.g., Art 1 (3) of the digital charter says: 'The rights under this Charter shall be enforceable vis-à-vis State agencies and private individuals'. available at https://www.dw.com/en/controversial-eu-digital-rights-charter-is-food-for-thought/a-36798258 last accessed 22 Feb 2021

wanted to achieve reassurances from the candidates in the 2014 EU election to undertake to commit to the principles set out in the Charter of Digital Rights.[95]

As part of the wider acknowledgement of how the need for a right of erasure or, in its widest form, a right to be forgotten can be applied, one of the significant recognitions has come in the form of Convention 108. Initiated in the early 1980s, this is a movement towards regulation of information protection potentially on a global basis. [96] Many countries have signed up to this agreement and more are continuing to do so, building up a more global focus to data protection and privacy whilst acknowledging the need for the free flow of information.[97]

Those opposing regulations, in any form, have relied on the importance of this free flow of information and the changes this is bringing; not just in terms of connectivity, but in the ability for the information to be utilised for educational purposes and to ultimately benefit mankind by enabling economic growth. Does the importance of proposed regulation aiming to rein in the activities of the Internet giants then take precedence over the free flow so envisaged by the EU and the US? It would appear, in the EU specifically, that there is increasing awareness of the importance attached to the need to conserve privacy rights and the ability to control data. Key is the ability to ensure that where data might adversely impact a person with emphasis on required consent to the access and use the data has not just to be balanced with the need for a free flow of information, but also with the strength of the increasingly monopolistic organizations. These are seen to be channelling the free flow of data to benefit their own economic goals, not to philanthropically benefit society by increasing global wealth.

[95] The Charter of Digital Rights - a guide for policy makers. EDRi https://edri.org/wp-content/uploads/2014/06/EDRi_DigitalRightsCharter_web.pdf

[96] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), The Council of Europe is updating its Personal Data Protection Convention - "Convention 108" – with two key aims: 1) addressing challenges for privacy resulting from the use of new information and communication technologies; 2) strengthening the convention's follow-up mechanism. The modernisation process also aims at bringing together the various normative frameworks that have developed in different regions of the world and provide a multilateral framework that is flexible, transparent, and robust, facilitating the flow of data across borders while providing effective safeguards against abuse, available at https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet

[97] Currently 54 states have signed

These opposing goals lead to the challenge of how to resolve the conflict of approaches. One way being considered is to establish the dominance of such entities in the data driven world.

6.5 The power and opportunities for abuse by internet giants in the exercise of the right. Are we in the era of Data-opolies ?

The right to be forgotten, as originally determined in Google Spain, was considered by some to be a response to the particular ability of ISPs, in this instance a search engine, to provide instant access to information stored on the Internet.[98] With the recognition of a search engine to be not only a data controller within the provisions of the Data Protection Directive, thereby forgoing any protection as a 'publisher,'[99] the decision threw further focus on the abilities and attributes of such search engines. Forced recognition that these would not constitute publishers or journalists therefore meant that they could no longer take advantage of protections previously offered.[100] It has become apparent that search engines were not only targeted in the finding of a formal 'right to be forgotten' but also were increasingly being viewed in connection with potential abuses in relation to data processed and accessed through the Internet.[101] These issues clearly involved issues of privacy, dignity, and ultimately reputation, being impacted as well as freedom of expression. However, due to their stature these concerns now evoked competition and other laws, such as copyright.[102] Various

[98] See n61 Stuart Hargraves

[99] n3 Google Spain para 28. The court also drew an analogy with the finding of data processing in the case of C-101/01 Lindqvist [2003] ECLI:EU:C:2003:596, para 25

[100] The EU have expressed on several occasions that the aim of the Digital Single Market is to ensure the free flow of information. See Directive 2000/31/EC of the European Parliament and of the Council of 8 June, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Recital 10 (10). In accordance with the principle of proportionality, the measures provided for in this Directive are strictly limited to the minimum needed to achieve the objective of the proper functioning of the internal market; where action at Community level is necessary, and in order to guarantee an area which is truly without internal frontiers as far as electronic commerce is concerned, the Directive must ensure a high level of protection of objectives of general interest, in particular the protection of minors and human dignity, consumer protection, and the protection of public health; according to Article 152 of the Treaty, the protection of public health is an essential component of other Community policies.

[101] This has most recently been reflected in the case C-136/17, GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL) [2019] ECLI:EU:C:2019:773 where four cases were held together. These all involved the processing of sensitive personal data. and were subject to the specific provisions relating to such data under the GDPR and formerly under the DPD (there referred to as 'sensitive data'). Here the court confirmed that the indexing activities carried out by the search engine were processing of personal data, therefore caught by such provisions. This meant the applicants could then request removal of such information.

[102] Following much debate, the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and

commentators have been critical to the change of approach within the EU with particular concern being voiced from the US relating to the potential abuse of freedom of expression, but also with a protective slant towards the income generating tech giants. [103]

The legal responsibilities of ISPs, and particularly search engines, was and is still complex with varying competing interests, not least in the opposing views of the US and the UK.[104] George Brock[105] raised the issue as to whether there would, or indeed should, be advantageous treatment for ISPs if the services provided by them were indeed without charge and viewed as not merely educational but also as fulfilling a socially desirable role. However, his concern was that if the complexities relating to ISPs, particularly search engines, could be summed up they could be considered to be 'utilities under private ownership but supplying basic needs on such a scale'. If this applied would they then require regulation as required for gas, electricity or telephone companies? [106] Utility companies have such regulations regularly updated and have even become nationalized. Do they then provide an equivalent function to a public service broadcaster because of their ability to perform various forms of democratic, social, or commercial communication? Moreover, should such services now be considered essential? If more regulation is required it might need to take into account instances where such an organization might also have a decision making role in respect of a potential human right or be 'simply the innovative leaders of a modern phenomenon, information capitalism'[107] providing the use of data as a product vital to many commercial organisations. This poses a question with more significance to the individual seeking informational self-determination under the right to be forgotten than theories explored in connection with the regulation of the Internet as a whole.[108] Recognition of the potential to impact individual

2001/29/EC has recently been finalised (2019), providing that a search engine will no longer be able to claim that they have no involvement in copyright infringement.

[103] W Gregory Voss, 'Obstacles to Transatlantic Harmonisation of Data Privacy Law', (2019) University of Illinois, Journal of Law Technology & Policy, Vol 2019, p.405. The New York Times has also reported that trade deals between the US and other countries may include legal protections for such companies.

[104] The differing viewpoints have led to increased protectionism from the US in respect of the tech giants which are primarily US corporations compared with an increase in favour of the rights of citizens in respect of data, privacy, and even consumer rights within the EU.

[105] George Brock, *The right to be forgotten- Privacy and Media in the Digital Age*, (IB Tauris), 2016 p19.

[106] ibid p28.

[107] Manuel Castells as cited in Emily Laidlaw 'Private Powers, Public Interest: An examination into search engine accountability, (2009) International Journal of Law and Information Technology Vol. 17, Issue 1, pp. 113-145, p121 Available at SSRN: https://ssrn.com/abstract=1357967 last accessed 20 Jan 2021

[108] Lawrence Lessig, *Code and other Laws of Cyberspace*, *Version 2.0*, (2nd ed. Basic Books 2006)

rights as opposed to group rights has increased in line with the power and control effected by these entities. The power of the ISPs can be considered a factor contributing heavily to changing attitudes, not only to privacy and data protection but to wide ranging ideas of consumer rights, even to democracy with the ISPs influencing the ability to vote independently.[109]

This was highlighted in 2015 when the EU produced a report looking in more depth at the digital single market.[110] Concerns were then raised as to how ISPs or online platforms[111] could use the power they were building and the impact on areas 'beyond the application of competition law.'[112] Certainly some activities, such as those taken by Cambridge Analytica,[113] highlighted the depth of influence extending to, purportedly, the ability to manipulate elections. Such companies now exercise a form of control previously unimaginable where the ability to influence sellers, buyers, advertisers, developers, even voters is growing at a speed which is in sharp contrast to the time the law takes to catch up with the necessary protections and recourse to forms of wrongdoing or abuse. Where action has been forthcoming, particularly by the EC, it has largely been focused on the abuse of power in anti-competitive behaviour.[114] This has led not only to large fines and public outcry but further recognition of such entity's total power and its impact.[115] One of the many criticisms of the

[109] The Economist branded the four main players as BAADD claiming this was for 'too big, anti- competitive, addictive and destructive to democracy' see Evan Smith 'The Tech lash against Amazon, Facebook and Google and what they can do', The Economist, 20 Jan 2018, last accessed at 15 Nov 2020 https://www.economist.com/briefing/2018/01/20/the-techlash-against-amazon-facebook-and-google-and-what-they-can-do

.[110] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, at 12, COM (2015) 192 final (May 6, 2015) ('the Report')

[111] The Report set out in 3.3.1; 'Role of online platforms; Online platforms (e.g. search engines, social media, e-commerce platforms, app stores, price comparison websites) are playing an ever more central role in social and economic life: they enable consumers to find online information and businesses to exploit the advantages of e-commerce. Europe has a strong potential in this area but is held back by fragmented markets which make it hard for businesses to scale-up.'

[112] ibid, The Report para 3.3.1

[113] see Cambridge Analytics, https://www.theguardian.com/news/series/cambridge-analytica-files last accessed 14 Dec 2020 also https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal

[114] Under Margarethe Vestager, the EU Commission fined Google €1.49 billion for abusive practices in online advertising see https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770

[115] Not only do such corporations face action for anti-competition behavior, they have also been charged with providing incorrect or misleading information, see EC Press release IP/17/1369 'Mergers Commission fines Facebook Euros 110 million for providing misleading information about WhatsApp Takeover', 18 May 2017 http://europa.eu/rapid/press-release_IP-17-1369_en.htm In addition a new proposals in connection with the

acknowledgement of a right to be forgotten was that it did not take power from Google but provided it with even more control over what information would be available or not, e.g., links shown in search results. The ability for an individual to determine what information should describe them, relate to their activities, and impact their presentation lay not with them exercising their rights but in the hands of an anonymous and unaccountable organization. Figures since the Google Spain case show that despite approximately half of the requests to remove links to personal data being refused,[116] the number of applications to data protection authorities remain limited, as do applications to the relevant national courts to appeal decisions made by Google.[117]

The focus on reining in the activities of the big tech companies has primarily been by the EC although there had also been some limited response by the US, in particular with initiation of actions under the US FTC Act. [118] These US actions were against Google and Facebook in respect of privacy violations.[119] Shockwaves were felt as one of the first clashes resulted in Facebook being fined a record $50 billion in respect of action taken for the breach. This was clearly an enormous fine which took many concerned by surprise, but this was put into focus by the realization that the fine represented only one month's income for this tech giant.[120] Arguments for such concepts as data-opolies have included the fact that many services are provided free to use. This originally led such corporations being considered as 'noble' organizations, although it became clear that their purposes are not so altruistic when looking

Digital Services Act (see also n 90 the review of the Digital Services market with focus being placed on the platforms with over 45 million users)

[116] Up to date figures are available from Google Transparency Report. The figures from 28 May, 2014 to 1 July, 2019 show 44.7 % of links delisted. https://transparencyreport.google.com

[117] Letter sent under FOI request on 9th July to ICO. The response made 8th Aug 2019 stated 'There have been 102 requests received (25 May 2018 – 9 July 2019) under the provisions of Article 17 (GDPR) the right of erasure also known as the right to be forgotten'.

[118] The Federal Trade Commission (FTC) was established as an independent administrative agency pursuant to the Federal Trade Commission Act of 1914. The purpose of the FTC is to enforce the provisions of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in commerce". https://definitions.uslegal.com/f/federal-trade-commission/

[119] Google FTC File no 102-3136 DKT c-4336 (Oct 13, 2011) Facebook In FTC 092-3184 DKt No C-4365 July 27, 2012

[120] As of January 2020, Google net worth is estimated to be around $300 billion. Its parent company's (Alphabet) net worth is estimated to be around $900 billion making it the third most valuable company behind Amazon and Apple. https://www.trendrr.com/google-net-worth-revenue-valuation-wiki Last accessed 30 Jan, 2020.

at the vast income generated.[121] Although many of these organizations would not meet the economic requirement of monopolies in either the EU[122] or in the US,[123] this does not mean they would fail to be seen as a form of monopoly. Their action results in anti-competitive effects, such as less output, higher prices for products or, as would be the case here, reduced quality i.e., the users are more at risk of some form of negative result as a result of increasing data. Legal commentators have begun to unearth aspects of where data protection and competition intersect, giving particular attention to privacy protection as a dimension of 'quality'. [124] Professor Maurice Stucke, an early advocate of the link between data protection and competition,[125] raises interesting arguments when examining this position. He contends that even though such companies considered as data-opolies do not charge or increase fees they can still have a monopolistic power.[126] This is largely due to considerations of an arguably degraded quality aspect, i.e., the service is not as beneficial as could be procured with more competition. In particular, more competition should be welcomed where privacy protection is involved as is seen and supported within the EU's views.[127] A data protection

[121] Earnings announcement for Google: 3 Feb,2020. According to Zacks Investment Research, based on 13 analysts' forecasts, the consensus EPS forecast for the quarter is $12.76. The reported EPS for the same quarter last year was $12.77
www.nasdaq.com › Market Activity › Stocks › GOOGLAlphabet Inc. Class A Common Stock (GOOGL) Earnings last accessed 30 Jan, 2020

[122] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2012/C 326/01 ('Treaty on the Functioning of the European Union')
Art 101 of the Treaty prohibits agreements between two or more independent market operators which restrict competition. This provision covers both horizontal agreements (between actual or potential competitors operating at the same level of the supply chain) and vertical agreements (between firms operating at different levels, i.e., agreement between a manufacturer and its distributor). Only limited exceptions are provided for in the general prohibition. The most flagrant example of illegal conduct infringing Article 101 is the creation of a cartel between competitors, which may involve price-fixing and/or market sharing.
Article 102 of the Treaty prohibits firms that hold a dominant position on a given market to abuse that position, e.g., by charging unfair prices, by limiting production, or by refusing to innovate to the prejudice of consumers.

[123] US Sherman Anti Trust Act 1890 15 US s 2. '1) the possession of monopoly power in the relevant market, and 2) the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product business acumen or historic accident.' Available at https://www.law.cornell.edu/uscode/text/15/chapter-1

[124] Allen P Grunes, 'Another Look at Privacy' [2013] 20 George Mason L Rev 1107, 1110;

[125] Maurice E Stucke , Ariel Ezrachi, 'When Competition fails to optimize Quality; A look at search Engines' [2017] 18 Yale J of Law and Tech 70, p 86

[126] Maurice E Stucke, 'Should We Be Concerned About Data-opolies?' (March 19, 2018). 2 Georgetown Law Technology Review 275 (2018); University of Tennessee Legal Studies Research Paper No. 349 available at SSRN: https://ssrn.com/abstract=3144045 last accessed 20 Sept 2020

[127] European Commission Press Release, IP/16/4284 Mergers: Commission approves Acquisition of LinkedIn by Microsoft Subject to Conditions (Dec 6, 2016)

breach can be a clear indicator of how an organization is conducting its business and how much attention is paid to such regulation.

Clearly, if a person can be encouraged to provide free personal data which has a commercial value then the organization will be looking to procure more such data to use in profit forming ways. So, for example, the more data that Google can garner the more valuable its searches then become to the detriment of its competitors (who would consider Bing if Google can provide so much more in its search results?). This enables Google to occupy a monopoly position with the risk of it carrying out 'short cuts' to the collection of data and its accessibility. This increases the use of recourse, such as the right to be forgotten, becoming increasingly vital to provide for the additional layer of protection of data and self-determination in terms of what information is readily accessible. This is not a new situation, rather it is one that builds on the recognition now being given to such activities. As long ago as 2007, the FTC approved Google's acquisition of DoubleClick, an ad serving company, increasing Google's targeting capacities. However, Commissioner Jones Harbour disagreed with the decision and set out several objections observing that such acquisition would harm not only future competition but also privacy, demonstrating early awareness of the potential damage ahead.[128]

There is also focus on the lack of accountability of entities, an area that the implementation of the GDPR has specifically been designed to cover. Buttarelli has recently argued that within the views held on the potential monopolistic positions of the tech giants, one school of thought is that 'Big Data' is just the latest fad in public policy and, as with past fads, competition principles and enforcement practice would again prove robust enough to prevail.[129] However, in his opinion a second school of thought could also argue that

[128] In the matter of Google/DoubleClickF.T.C. File No. 071-0170, Dissenting statement of Commissioner Pamela Jones Harbour p 10 Part III, available at https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf Here the Commissioner states 'In addition, I have considered (and continue to consider) various theories that might make privacy "cognizable" under the antitrust laws, and thus would have enabled the Commission to reach the privacy issues as part of its antitrust analysis of the transaction.' last accessed 3 Sept 2020

[129] Giovanni Buttarelli, 'Strange Bedfellows: Data Protection, Privacy, and Competition' (2017) 34 Computer and Internet Lawyer 1, 3.

competition enforcers have lost sight of the founding objectives for anti-trust. Buttarelli believed such objectives were conceived as a means to reduce the potential monopolies now considered to be imposing a threat to democracy and freedom, and therefore endangering basic values from dignity to privacy.

An example of how using competition to enforce data protection has begun to emerge took place in 2017. This was where the *Bundeskartellamt* (the German Data Protection Authority) found Facebook to be in breach of its dominant position by 'making use of its social network conditional on it being allowed to limitlessly amass every kind of data generated by using third party websites and merge it with the user's Facebook account'.[130] The authority advocated that even where the service is free, the amount of competitive advantage provided by the collection of such data made the position unfair and an abuse of market power. By analogy, the collection of the data was therefore an excessive price that consumers were paying. Once this is acknowledged then questions arise as to how data subjects learn what data is being accessed, collated, and modified for use by Facebook. In addition, the question of consent along with privacy concerns has created clear data protection questions, not least around the principles of such consent. There must also be alarm that competitors need to match such practice to remain within the same marketplace, again increasing the loss of data control for individuals. Stucke asks if it can be considered that there is real pressure for a data-opology to change its privacy practices for the better whilst in this situation, the answer must surely be not if it wishes to retain a competitive edge amongst rivals who do not improve their practices.

Considering the dominance of such organizations, how would a right to be forgotten, whether under the principles of the Google Spain case and subsequent case law or under the new provisions of Article 17 of the GDPR, provide help for an individual to regain control? [131] A right to have information 'forgotten' once made publicly available would at least be a clear

[130] *Bundeskartellant* Press release; Preliminary assessment in Facebook proceedings: Facebook's Collection and Use of data from Third Party Sources is Abusive, (Dec 19 2017) available at https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html last accessed 3 February 2020

[131] The provisions of Art 17 of the GDPR would ensure clear cut categories of personal data could be removed if the circumstances set out in the article are met.

step towards the exercise of such autonomy. However, for many of these organizations a 'privacy policy', even if required by the GDPR, is really an option to 'take it or leave it' because without accepting the privacy policy the service is not available. For organizations such as Facebook and Google, if there is a challenge to the economic interest of such data-ology then it is more probable that the protection of privacy and data protection will take a lower priority[132]. Without other companies offering similar services, the choice facing a user is therefore limited, often with only one player in the field. As mentioned before, Google still accounts for more than 90% of searches in the EU marketplace,[133] so choice is restricted. The burden placed on those wishing to have information removed or erased is that when it is accessible it is also available to a greater percentage of the public, not merely a few users of the facility but by a much wider global audience with the potential for further copying or sharing of the information. The availability of protection through anti-competition activities is a poor solution, and it is a short term-one compared to the volume of activities that the tech giants carry out. However, this may be one of the only ones available as the law struggles to catch up with the swift changes occurring. Ultimately, the reality is wider recognition that data subjects have limited options in order to protect the accessibility of their data. It has already been pointed out that a private commercial entity, in this case Google, has been left to determine what information should be forgotten and what is retained purely for the benefit of the public, potentially forming a role of a quasi-regulator.[134] This has reduced options available for individuals to apply this right freely. In addition, despite the Transparency Report there has been little information made available as to how decisions are reached.[135] This has also been explored by the media, echoing concerns that, '[t]his case, five years in the making, is the latest and perhaps the largest, battle in the struggle to establish

[132] It will be noted that as concern increases with regard to the accessibility and longevity of available information that there are changing attitudes towards privacy by such organisations with recognition that further steps need to be taken.

[133] http://gs.statcounter.com/search-engine-market-share- Worldwide share as at June, 2019 equal to 92.6%

[134] Patricia Sánchez Abril, Jacqueline D Lipton, 'The Right to be Forgotten: Who Decides What the World Forgets?' (2014) Kentucky Law Journal: Vol. 103: Iss. 3, Art 4, available at: https://uknowledge.uky.edu/klj/vol103/iss3/4

[135] Available at https://transparencyreport.google.com/eu-privacy/overview?hl=en_GB last accessed 13 Sept 2020. This lists relevant information under the heading 'Requests to delist content under European Privacy Law'. It shows the number of requests made and links removed. It also shows the percentage of successful removals. More information is obtained through the categories of requesters which, in principle, shows the various reasons why requests are successful or not. For example, one mention is to there being a lack of public interest. However, other than referring to the Article 29 Working Party guidelines, little information is given that reveals how Google makes the decision how it or its technology decides what to remove as not being in the public interest.

democratic control over the giants of the digital economy'.[136] It is clear that the outcome from mergers of data from other sources used for commercial purposes increases both the accessibility and potential misuse of data. New innovations, such as third-party tracking which provides for unprecedented volumes of data as well as wider use, could be considered to collate information that might provide insight into a person's personal and professional life, activities, interests, and health and develop how such person is portrayed without concerns as to the potential impact on their rights. Within this there is scope for numerous issues around privacy, democracy, consumer protection, as well as competition.

In 2016, as data concerns focused on the finalization of the GDPR, the OECD noted that the development of products obtainable through social media, apps, or simply via internet access, at a low or zero cost meant more users, more data, and more manipulation of data. The latter concerned Google in particular, i.e., with the ability to manipulate the data collected to such extent so as to offer more products than any competitors. This provided significant advantage and other opportunities for 'creative content'. Stucke[137] expands on this by explaining that users' photos and other information concerning identity can be made available, particularly if no opt out or withdrawal of consent occurs, resulting not just in increasing advertising revenue but also providing an on-going digital identity and potentially indefinite accessibility to such data. He also expresses concern that a so called data-opoly can use its dominant position to both access and utilize data, noting in particular that this enables it to use this to reduce competition but also to gain significance not only in an economic market place but in the conduct of individuals' private lives.[138] The information being collected links to individuals

[136] The Guardian newspaper reflecting media interest commented that 'Competition law appears to be the only way to address these imbalances of power. But it is clumsy. For one thing, it is very slow compared to the pace of change within the digital economy. By the time a problem has been addressed and remedied it may have vanished in the marketplace, to be replaced by new abuses of power. But there is a deeper conceptual problem, too. Competition law as presently interpreted deals with financial disadvantage to consumers and this is not obvious when the users of these services don't pay for them. The users of their services are not their customers. That would be the people who buy advertising from them – and Facebook and Google operate a virtual duopoly in digital advertising to the detriment of all other media and entertainment companies. The product they're selling is data, and we, the users, convert our lives to data for the benefit of the digital giants.' see https://www.theguardian.com/commentisfree/2017/jun/18/the-guardian-view-on-digital-giants-they-farm-us-for-the-data last accessed 15 Nov 2020

[137] Maurice E Stucke, 'Should We Be Concerned About Data-opolies?' (March 19, 2018). 2 Georgetown Law Technology Review 275 (2018); University of Tennessee Legal Studies Research Paper No. 349 available at SSRN: https://ssrn.com/abstract=3144045 p 296

[138] ibid p 306

providing the type of profile that may impact their portrayal online, potentially impacting and creating an everlasting digital identity.

Although it can appear difficult to clearly reconcile the threat of anti-competitive behavior with an abuse of human rights in the form of a right to be forgotten rather than consumer protection, there is no doubt that such organizations with an overall power in respect of new technology are shaping the way life is lived. There are already situations where data-opolies have had an impact on individual autonomy and their ability to exercise free choice to protect dignity and reputation. Stucke sets out various examples of this ranging from informational privacy to associational privacy where we, as users of the services provided, can no longer have free choice as to whom we disclose information to nor with whom it is shared. [139] In addition, recent issues have concentrated on the ability to influence voting preferences through social media.[140] There is however growing evidence of the sharing of information between platforms.[141]

There are examples which are clearly based on more commercial activities[142] and relate to the targeting of consumers. Certainly, it must be noted that the collection of data relating to an individual's patterns of behavior can, if linked and portrayed in a search result, have a dramatic outcome. It becomes common gossip when specific targeting can reveal intimate details of an individual's personal life; this has been seen in revelations relating to celebrities private lives.[143] How accessible such information can be and how to stop it being linked to

[139] n 133 Maurice E Stucke p 312

[140] see 'How Facebook is changing democracy' Opinion FT available at https://www.ft.com/content/a533d5ec-5085-11e7-bfb8-997009366969 last accessed 1 Feb 2021

[141] This can also be seen in the fact that during the period of 2008-2018 none of the 400 takeovers by the five largest digital companies were blocked by a regulator. However a proposal by WhatsApp to amend it terms and conditions to pass information to Facebook its owner was met with public outcry forcing it to suspend the proposal and commit to observing the data protection provided in the EU and the UK. See https://www.bbc.co.uk/news/technology-55573149 last accessed 10 Jan 2021

[142] Data-opolies have every financial incentive to maintain (and increase) their profits. Google, Apple, Facebook, Amazon, and Microsoft had the largest absolute increase in market capitalization between 2009 and 2017. As of June 2018, they were the largest U.S. public company by market capitalization. In 2017, it is reported that Google "spent over $18 million lobbying politicians", which was "the first time a technology company has spent the most on lobbying costs in at least two decades". Similarly, compared to 2016 levels, Facebook increased its lobbying spending by nearly $3 million ($11.5 million), Apple by $2.3 million ($7 million), and Amazon by nearly $2 million ($12.8 million).

[143] Actions reported in the media included actions in respect of photos of celebrities Jennifer Lawrence and Taylor Swift

search results is clearly an issue, particularly viewed through the necessity of providing for a right to be forgotten in respect of information to be de-linked or erased.

Orla Lynskey follows a similar approach closely allied to that of viewing the tech giants as data-opolies and focusing on the depth of the 'data power' held by them whilst also recognizing that this power can diminish the autonomy of those using the services provided.[144] She examines the fact that the reach of such entities is providing a form of invasion into the ability of data subjects to effect control of such personal information but without there being any form of recourse against the corporations. Similarly, she and Stucke both see the analogy that having such a strong market position aligns these entities with those occupying monopoly positions but without the subsequent consequences. The view of information gathering being monopolistic behaviour is discussed by Viktoria Robertson when looking at the new activity of excessive data collection increasingly of concern where this leads to a loss of control. [145] Primarily concerned with activities such as third-party data tracking and its impact on targeted advertising, she writes that these activities and the width of them must also impact issues such as privacy autonomy and ultimately democracy. Such behaviours should be reviewed to see if they may be considered of sufficient importance to warrant being caught by anti-competitive endeavours.

However, there must be a point where a sense of distrust in such entities can then influence the availability of data, thereby restricting the developing uses and potential commercial value. [146] The implementation of the GDPR and the revised focus of individuals' privacy rights have produced a wariness among data subjects and growing unease over parting with data.

[144] Orla Lynskey. 'Grappling with "Data Power" Normative Nudges from Data Protection and Privacy', [2019] 20 Theoretical Inquires L 189 'This data power is a multifaceted power that may overlap with economic (market) power but primarily entails the power to profile and the power to influence opinion formation.'

[145] Viktoria H.S.E Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data' (June 24, 2019) available at SSRN: https://ssrn.com/abstract=3408971 last accessed 18 October 2019

[146] Since April 2018, the first full month after news of the Cambridge Analytica scandal broke in the Observer, actions on Facebook such as likes, shares and posts have dropped by almost 20% according to the business analytics firm Mixpanel. Taking that month as a baseline, total actions fell by more that 10% within a month, recovered a bit over the summer and then fell again over the autumn and winter of 2018, except for a brief rally over the period of the US midterm elections. The issue has continued on a global basis, see the Guardian report available at
https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-shows

Such awareness has been followed by an increase in the desire to exercise rights over it, however, this may not be reflected in actions taken under the right to be forgotten. Despite the introduction of the GDPR, the number of applications under the right to be forgotten are consistent and although no detailed figures currently exist for applications to data protection authorities under Article 17, there have been few recorded outcomes of cases bought under the principles of Google Spain.[147]

It could, therefore, be argued that with a lack of immediate action through the right to be forgotten, the potential or actual abuse of this market position must result in a greater need for what Lynskey refers to as "special responsibility" to be imposed on such firms, analogous to the idea of special responsibility imposed by competition law on dominant companies with market power.[148] It is not certain that a data protection breach would be an abuse of a dominant market position, but in May 2019 Margrethe Vestager, the European Commissioner for Competition since 2014, linked fair competition to compliance under the GDPR in response to the recent German Facebook case where initial action was being taken against Facebook in connection with bundling of consents to give it a competitive edge with regard to its products but which then potentially jeopardized privacy. [149]. It is being made clear that the EU in particular will not shirk from such action to meet what they see as a 'fairness'

[147] Whilst some analysis has taken place in various countries the number of reported cases are few. For example in Finland there have only been two cases fully reported. One of these is still being processed by the Data Protection Authority having been determined by the Finnish court and the other referred to the highest court in Finland. The case is reported in Finnish only and available at;
https://www.kho.fi/fi/index/paatoksia/vuosikirjapaatokset/vuosikirjapaatos/1534308651626.html
This is also highlighted by the referral to the CJEU of four cases by CNIL to establish principles of application of the right which only took place in 2019, several years after Google Spain see case C-136/17, GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL), [2019] ECLI EU:C:2019:773

[148] See Case C-457/10P, AstraZeneca AB, AstraZeneca plc v European Commission [2012] ECLI:EU:C:2012:770
Here the position was referred to as, 'in so far as an undertaking in a dominant position is granted an unlawful exclusive right as a result of an error by it in a communication with public authorities, its special responsibility not to impair, by methods falling outside the scope of competition on the merits, genuine undistorted competition… requires it, at the very least, to inform the public authorities of this so as [to] enable them to rectify those irregularities.'

[149] The initial decision of the German Data Protection Authority (German Federal Cartel Office (*Bundeskartellamt, BKartA*)) was followed by the court's confirmation BGH, Order of 23.06.2020, Case KVR 69/19 (BGH 2020a) see also Wolfgang Kerber, Karsten K Zolna, 'The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law' (September 20, 2020). where the authors stated that the case would arise much interest in supporting rights of informational self - determination through the use of anti-competition actions; available at SSRN:
https://ssrn.com/abstract=3719098 last accessed 20 Jan 2021

criteria.[150] If the ability to control the width and depth of the collection of data collection is essential to meet such criteria, the right to be forgotten must therefore be seen as an increasingly important tool in this aim as specifically providing informational self-determination within a right that potentially offers wider recourse than more conventional data protection.

The position in the EU, with notable action often directly targeted towards the tech giants in various forms, contrasts considerably from that of the US. The situation in the US offers differing views not only on privacy but on market trade and more recently on a stance often seen as protectionism of US commercial interests. With such a position supporting the US companies based in the EU, the latter has been the innovator of significant privacy protection, although this is believed to be changing with the global increase in awareness of privacy issues and data leaks.[151] Although considered to be against data–opolies' interests for data subjects to have increased rights, whether by way of property rights or general legal remedies, it appears that such entities might be prepared to take counter action to shape any such initiatives.[152] The abilities for these companies to hold such power has increased the call not just for formal regulation of the Internet to be increased but for new guidance to be introduced to reduce the expanding influence of these companies. This is not only reflected in the debate as to the way forward to provide some form of control over the Internet, but it also recognizes how the lack of control impacts how people can protect their rights to portray themselves as they so desire.

[150] With regard to competition, Commissioner Vestager argued: 'If a company's use of data is so bad for competition that it outweighs the benefits, we may have to step in to restore a level playing field'. See speech; Commissioner Vestager, 'Competition in a Big Data World', DLD 16 Munich, 17 January, 2016. https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big-data-world_en

[151] California Consumer Privacy Act 2018 was passed in California, the home of many of the tech giants, but other states have followed suit, e.g., Illinois proposing three acts: Data Privacy Act, Illinois Data Transparency and Privacy Act, Consumer Privacy Act. Maine; An Act to Protect the Online Consumer Information.

[152] The original bill was stalled by pressure from Californian based companies in 2017 due to their concerns over restrictions being placed on their use of data. The final form was agreed between representatives from the industry and state legislators, see: https://www.oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf

6.6 How the growth of digital ethics can support the right to be forgotten

6.6.1 Recognition of the need

Following a similar approach to the tech giants, and in view of the above-mentioned increasing awareness of the power of such ISPs, not only Google as the dominant search engine,[153] there is recognition that,

> The power to shape people's attention is increasingly concentrated in the hands of a few companies. It takes a real effort to assert and defend what John Stuart Mill called 'the freedom of mind'. There is a possibility that once lost, people who grow up in the digital age will have difficulty in regaining it. This may have far-reaching political consequences. [154]

In addition, in November 2018, in his defining speech called the 'Current Moment in History', George Soros spoke openly of the issues facing the world and of the impact of the rise of the tech giants.[155] In late 2018 to early 2019 awareness of issues such as data-opolies had led focus towards to a new area of concern labelled 'digital ethics', largely arising from the strength of these entities and the potential impact of their activities on privacy and data protection. This was not a new idea. Some years before, in 2006, an Internet Governance Forum had initiated ideas of what had been referred to loosely as an Internet Bill of Rights

[153] See n149, the German Federal Cartel Office found that Facebook, in requiring its customers to agree to an extensive data collection process in order to have an account, prohibited the practice going forward. "Facebook will no longer be allowed to force its users to agree to the practically unrestricted collection and assigning of non-Facebook data to their Facebook user accounts", FCO president Andreas Mundt said in a statement announcing the decision. This was at last recognition that an entity in a dominant position was able to impose such conditions that consent could not be considered to be freely given. The decision is one of the first to articulate the human rights issues facing regulators where there is anti-competitive behaviour, see: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html last accessed 14 Jan 2021

[154] George Soros, 14 Feb 2018 'The Social Media Threat to Society and Security' available at https://www.project-syndicate.org/commentary/social-media-security-threat-by-george-soros-2018-02?barrier=accesspaylog

[155] Speech available at https://qz.com/1480543/the-george-soros-speech-at-the-center-of-the-sheryl-sandberg-facebook-controversy/

founded in the growth of the Internet to include both traditional and innovative rights to which each citizen should have recourse.[156]

In its recent opinion on ethics involving information and communication technologies, which included looking at the impact of access to personal data, the European Group on Ethics in Science and New Technologies (the EGE)[157], concerned as to the impact on humanity and individual choice with regard to the increasing accessibility of personal data, also drew attention to this new area stating, '[t]he debate on ethics and governance of ICT is complex and needs to address a wide range of considerations, values and principles, such as: autonomy; identity; privacy and trust; responsibility; [and,] justice and solidarity.'

There is no doubt that, as mentioned previously, the behaviour of the internet companies was and is impacting autonomy, privacy, and trust as well as, importantly, a person's projection of their identity. Concern was increasing not only in the EU but globally. When an analysis by a leading management consultancy[158] starts to talk about digital ethics and privacy, calling it a '[g]rowing concern for individuals, organisations and governments', acknowledging that '[p]eople are increasingly concerned about how their personal information is being used by organisations in both the public and private sector, and the backlash will only increase for organisations that are not proactively addressing these concerns', it is recognition that there is a loss of trust among the very users of technology who expected to benefit from it.[159]

Without focussing on the technological implications, ranging from Block Chain to the Internet of Things, concern rests on the ability for corporations to have collected and used individual's

[156] Joanna Kulesza, 'Freedom of Information in the Global Information Society: The Question of the Internet Bill of Rights' (November 4, 2008). University of Warmia and Mazury in Olsztyn Law Review, Vol. 1, pp. 81-95, 2008. Available at SSRN: https://ssrn.com/abstract=1446771 last accessed 20 Nov 2020

[157] European Group on Ethics in Science and New Technologies (EGE) This is an independent, multi-disciplinary body which advises on all aspects of Commission policies where ethical, societal and fundamental rights issues intersect with the development of science and new technologies.

[158] 'Top Ten Strategic Developments Trend for 2019'; available at gartner.com

[159] In their consultancy work Gartners are now drawing to corporates' attention the need to re-establish that trust. It includes this statement in its review, "Any discussion on privacy must be grounded in the broader topic of digital ethics and the trust of your customers, constituents and employees. While privacy and security are foundational components in building trust, trust is actually about more than just these components. Trust is the acceptance of the truth of a statement without evidence or investigation. Ultimately an organization's position on privacy must be driven by its broader position on ethics and trust. Shifting from privacy to ethics moves the conversation beyond 'are we compliant' toward 'are we doing the right thing".

data without informing them of the how, why, and what they actually do with such data. There is mention of 'strategic obfuscation', a blurring of data transactions so that such data may be used for purposes of which can only be guessed. At the very least this represents a true diminishing of autonomy as well as the recurring themes of loss of privacy, data protection and individual control. Where the right to be forgotten comes into play is to provide an ability to remove information or links to information which is no longer pertinent to an individual at such time. Potentially, this can provide a missing element of informational self-determination within a right to be forgotten to ensure that, despite the lack of transparency, control can remain with an individual on how such information is used to portray themselves.

Emphasis has also been given in the EDPS strategy plan[160] as part of its revised focus stated under the second objective of the strategy for the years 2015 to 2019 as, '[f]orging global partnership… developing an ethical dimension to data protection'.[161] This has followed a publication in 2018 of the Ethics Advisory Group Report[162]. Attention was truly placed at the International Conference of Data Protection and Privacy Commissioners, dubbed '*the Olympic Games of Data Protection'* by EDPS Giovanni Buttarelli.[163] In this conference there was a clear change of approach with leaders of various tech giants presenting amidst seasoned data protection and privacy representatives. Announcements of all forms of new initiatives to improve the use of data and to increase privacy protection were made at this highly publicised event that really launched the discussion on digital ethics onto the international agenda. Buttarelli referred several times to 2018 as being the year of Data Protection, concentrating on implementation of the GDPR but with future movement to bring this concept more into line with fundamental protections and the new world of 'Digital Ethics'. This type of movement will be essential in forging paths to greater application of the right to be forgotten

[160] EDPS Strategy Plan available at; http://informationaccountability.org/wp-content/uploads/EDPSStrategy20152019EN.pdf

[161] Information available at https://edps.europa.eu/sites/edp/files/publication/ar2018_en.pdf

[162] Available at https://edps.europa.eu/data-protection/our-work/publications/ethical-framework/ethics-advisory-group-report-2018_en As part of the EDPS 2015-2019 strategy, the Ethics Advisory Group is set up with the mandate to explore the relationships between human rights, technology, markets and business models in the 21st century. Last accessed 3 Dec 2020

[163] 40th International Conference of Data Protection and Privacy Commissioners, October, 'Debating Ethics, Dignity and Respect in Data Driven Life'2018 https://www.privacyconference2018.org/en/40th-international-conference-data-protection-privacy-commissioners.html Last accessed 25 Feb 2021

and acceptance of not only the need to exercise human rights on the Internet but the opportunity to recognise new ones.

6.6.2 Next steps

In one of the first moves towards formal recognition of the drive towards ultimately lifting the power of the tech giants, apart from the work being carried out in individual cases by France and Germany when using other tools such as anti-competition fines to rein in such bodies, the UK published a consultation paper of internet regulation. Following the launch of the so called 'Digital Charter' in January 2018, it echoed the intent of the UK Government to make the UK 'the safest place to be online and the best place to start and grow a digital business looking at an agreed programme of 'norms and rules'. The Online Harms White Paper published aims to be at the forefront of building a new regulatory framework for online activity.[164] Although often intent on the harms arising from harmful content, such as porn or violence, it examined various approaches such as categorizing online platforms as publishers or imposing a duty of care on these entities. The on-line harms consultation paper ran from 8th April to the 1st July 2018, with the intent to look into key issues arising from the widespread use of the Internet.[165] Implicit in this and in the views of the minister at the time, Jeremy Wright, was the indication was that the UK Government should act and that the era of little interference in a free flowing Internet was at an end.[166] It was made clear in the review that online platforms would also to be expected to self-regulate, moderate, and remove content. This view was, however, challenged by the finding that there has been a failure to address issues and a general view that self-regulation might not be enough.[167] The response to the consultation was published in December 2020.[168] The outcome of the consultation has been

[164] The Online Harms White Paper 8 April, 2019 available at available at https://www.gov.uk/government/consultations/online-harms-white-paper see col 55 last accessed 20 Nov 2020

[165] ibid, the Online Harms White Paper sets out the government's plans for a world-leading package of online safety measures that also supports innovation and a thriving digital economy.

[166] ibid, the Online Harms White Paper 8 April, 2019, note the consultation is now closed.

[167] House of Lords Communications Committee, Regulation in a Digital World, 9 March, 2019. HL Paper 299 of session 2017-19, p 49

[168] Consultation Outcome Online Harms White Paper: Full government response to the consultation Updated 15 December 2020. 'The government's response to online harms is a key part of our plans to usher in a new age of accountability for tech companies, which is commensurate with the role they play in our daily lives. Our ambition is to build public trust in the technologies that so many of us rely on' available at https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response last accessed 24 Feb 2021 This has now resulted in publication of a Draft

accepted and is now proceeding through to parliament as a draft bill. In this there is clear recognition of the obligations of internet service providers to users' rights of expression and privacy as shown in the Explanatory Notes to the bill.[169] This has been joined by the announcement that the Competition and Markets Authority (CMA) has indicated that a new regulator is needed to police the growing power of the digital platforms, including Google and Facebook.[170] Following the Digital Markets revised strategy published in February 2021,[171] a Digital Markets Unit (DMU) within the CMA was announced with the intention of promoting pro competition and protecting consumers and businesses from unfair practises. Although focused on curbing the asymmetries of power and the impact on competition, this is a clear first step towards restraints on the activities of the tech giants. The DMU will oversee a new regulatory regime for the most powerful digital firms, promoting greater competition and innovation in these markets and protecting consumers and businesses from unfair practices and activities. The impact of this on the application of the right to be forgotten now resting largely with search engines remains to be debated, but it leaves doubt as to the ability for this process to be continued without clearer supervision. However, the trend towards more expressed concern, even condemnation, towards the Internet giants continues with new steps being taken to look at the impact on individuals' personal lives.[172]

Further input also came from UCL Constitution Unit's Independent Commission on Referendums. This echoed arguments that making social media companies liable for content requires them to make judgments on information or material created by a range of contributors, not merely journalists or staff. There was concern that making decisions on content would impact the ability for freedom of expression and this could be unfettered. 'It

Online Safety Bill, 12 May 2021 available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

[169] Available at; https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985031/Explanatory_Notes_Accessible.pdf

[170] The Times, Thursday 4th July 2019

[171] Available at https://www.gov.uk/government/publications/competition-and-markets-authoritys-digital-markets-strategy

[172] Incidentally in an attempt to regain public support after many instances of concern over the detrimental material contained on it, Facebook has recently announced a change of name to Meta (October 2021) to reflect its new focus on meta data rather than personal data.

would mean outsourcing to private companies delicate decisions about how best to balance important freedoms'.[173] Mention was also made of the imposition of creating a clear 'duty of care'. This however reflects the reality of the decision making in the right to be forgotten applications where this rests solely on ISPs.

Ideas were expanded upon by the work for the Carnegie UK Trust carried out by Lorna Woods and William Perrin which, although looking at the steps a company could take, i.e. reasonable measures to prevent harm, saw that there was still a need for the exercise of reasonableness to be subject to oversight by some form of regulator with recourse to the courts in the case of dispute. Generally, it was considered that a regulator would be responsible for establishing, amongst other duties, a transparency, trust, and accountability framework. This proposal was supported by the Lords Communications Committee, confirming a need to create a culture of risk management in the provision of internet services. [174] However, it is unlikely such a view would be accepted by jurisdictions such as the US who are opposed to introducing more regulation. So, whilst the idea is generally growing in acceptance and voiced as being necessary, even by such entities as Google, Facebook, and Amazon, there is a lack of consensus of approach. Whilst this continues to be debated, the enforcement of human rights continues to be exercised in the right to be forgotten by commercial entities seen to be acting as quasi-regulators whilst potentially occupying a monopolistic position. It is hard to see how this can meet any increasing concerns as to who determines which information is available that may impact how a person is perceived, who decides what is remembered, and what is forgotten. [175]

[173] Independent Commission on Referendums Report for the Independent Commission on Referendums July 2018 p183

[174] Additional viewpoints considered were those of the London School of Economics Truth Trust and Technology which also supported a body to monitor and inform digital activities by the online service providers.

[175], Patricia Sánchez Abril, Jacqueline D Lipton, (2014) "The Right to be Forgotten: Who Decides What the World Forgets?" Kentucky Law Journal: Vol. 103: Iss. 3, Article 4. Available at: https://uknowledge.uky.edu/klj/vol103/iss3/4

6.6.3 Could a form of industry self-regulation meet the need for an ethical approach to, and observance of, the right to be forgotten?

The idea of self-regulation is not a new one and can be seen in similar initiatives such as the EU Code of conduct on Hate Speech, [176] the Code of Practice on Disinformation[177] reflecting the new issues of the Internet as well as attempts to self-regulate industries through for example Ofcom for broadcast media as well as IPSO and IMPRESS[178] for newspapers and magazines. Indeed, it may also be considered that self-regulation has taken shape in the ability of the Law Society to enforce breach of its regulations. However, it is becoming apparent that the tech industry is still considering ways to regulate itself, i.e., they would prefer to choose the path rather than have it imposed upon them through legislation or regulation. Proposals from the founder of the Internet, Tim Berners Lee, intend to create a new organization, 'Solid,'[179] which could potentially be a movement towards the industry creating its own regulation.

In addition, in its calls for regulation of its own industry Facebook has highlighted the change of approach, drawing attention to the fact that usually such businesses try to avoid any restrictions whether self-imposed or otherwise. The Times newspaper's commentary, after noting the calls for more regulation, has argued that such 'players to the field' have realized that established regulation could be their friend, potentially adding legitimacy and that this 'maintains status quo conferring respectability'.[180] Such regulation could, however, add further barriers to trade in line with monopolies by increasing the price driven entry requirements with onerous compliance costs. Facebook's new global spokesperson, Nick Clegg, has spoken positively of a world that requires new rules, but to many this could largely be considered a defensive move to set off increased calls for the break-up of Facebook.[181]

[176] Available at https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en
[177] Available at https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
[178] Independent Press Standards Office (IPSO) and Independent Monitor for the Press (IMPRESS)replaced the Press Complaints Commission only IPSO is recognized as an approved regulator.
[179] Solid, https://solid.inrupt.com / last accessed 17 Feb 2021
[180] https://www.thetimes.co.uk/article/tech-giants-must-no-longer-be-left-to-police-themselves-argue-mps-dtd8bv5m6 last accessed 10 November 2020
[181] See https://www.theguardian.com/us-news/2019/oct/19/elizabeth-warren-facebook-break-up . Here Elizabeth Warren the US senator raised the issue of potential regulation of tech platforms wanting to regulate tech platforms that earn $25 bn or more in global annual revenue. 'Today's big tech companies,' she said,

The challenges facing any such form of industry-imposed regulation are immense as these need to cover very different approaches taken by other states and jurisdictions. For example, the decision by Australia to make media companies legally responsible for comments posted on a Facebook page[182] has raised the issue effectively resulting in a climbdown by Facebook after threats to withdraw from hosting journalistic content.[183] From a very different viewpoint China blocks access to much of the Internet and censors what content can be viewed and by whom.[184] The ability to introduce forms of regulation which are globally accepted show the difficulties in also enforcing human rights and, particularly, the exercise of a balancing of them within the internet's environment. Even where acceptance exists of a right to be forgotten, this would take a different form in many jurisdictions lacking an overall regulator with the ultimate decision-maker remaining Google.

6.6.4 How can the right to be forgotten be enforced and policed in the light of this change of approach?

The possibility of progression to accepting digital rights or a bill of Internet rights may not seem probable in the immediate future despite early steps being taken both in the EU and in the UK.[185] It is clear that the virtual monopolistic approach of the Internet giants can erode the significance of the Google Spain case and the full implementation of the provisions of Article 17 of the GDPR. The so called burden of processing and enforcing the right to be forgotten has fallen onto the very entities whose behaviour has been challenged. The

announcing her policy, 'have too much power – too much power over our economy, our society and our democracy.' last accessed 19 Nov 2020

[182] The Australian Competition and Consumer Commission's (ACC) 'News media and digital platforms mandatory bargaining code'; Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020 available at https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2021a/21bd048

Bills Digest No. 48, 2020–21. This now provides a mandatory code under which the ACC will oversee the actions of digital platforms and Australian news businesses to address the bargaining power imbalance and negotiate in good faith appropriate renumeration for the use and copying of news content.

[183] see 'Facebook reverses ban on news pages in Australia, available at https://www.bbc.co.uk/news/world-australia-56165015 last accessed 25 Feb 2021

[184] In China there are lists available of banned sites which includes the Google suite as well as Facebook, YouTube, Instagram, Vimeo, Spotify, Snapchat, and Tumblr. Details available at https://www.techradar.com/vpn/which-websites-and-online-services-are-banned-in-china

[185] The proposed Online Safety Bill is now due to be effected by the UK government following its earlier publication of the White Paper on Online Harms, see; https://techcrunch.com/2020/12/14/uk-online-harms-bill-coming-next-year-will-propose-fines-of-up-to-10-of-annual-turnover-for-breaching-duty-of-care-rules / last accessed 15 Dec 2020

question then posed by Abril and Lipton concerns'…. whether such procedures with little or no government or judicial oversight are now the most appropriate and socially desirable method for protecting privacy'.[186] By analogy such question also applies to the protection of other rights included within the scope of the right to be forgotten, such as dignity and reputation. Generally, this is seen as less than optimal with the determining of whether a right to be forgotten exists under individual applications resting on commercial organizations whose focus must clearly be on making profits and ensuring the 'product' is capable of generating the maximum income irrespective of opposition or quasi rights. Is the right to be forgotten then confined to being a balance between the control of a monopolistic 'super power' and the ability of an individual to exercise their right to informational self-determination? The ability to ensure that digital identity should not subject to the capricious nature of such enterprises must surely be compromised in such scenarios.

If the answer to such question is no, then recognition of the right to be forgotten and its ability to provide informational self-determination as part of a fundamental right could require increased state intervention to ensure its valid and consistent use. The use of the GDPR to regulate the behaviour of non-state entities involved in the application of the right to be forgotten through not only Article 17 but through its general principles of safeguards and fairness may yet prove to be insufficient. Concentrating on responsibility the regulation does not necessarily impose direct liability relying instead on controllers to put into effect the controls necessary.

6.7 Conclusion

Whilst the right to be forgotten is not yet capable of being seen as a universal right or formally recognized as a human right within existing conventions, it offers a new ability for a person to not only control data in line with the EU's holding of data protection as a fundamental right, and to protect privacy, but also to find a way of ensuring portrayal of the self by maintaining a relevant online identity. Shown primarily through the Internet with the increasing and everlasting access to searches and social media whether directly or via links

[186] Patricia Sanchez Abril, Jacqueline D Lipton, 'The Right to be Forgotten: Who decides what the world forgets?' (2014) Kentucky Law Journal Vol 103 2014 to 2015 p 366

(URLS) a person's ability to ensure that they are depicted as they would wish is at risk. The need for protection is consistent with the need for dignity and reputation and potentially to ultimately provide for rehabilitation. This meets the requirements of societal order with time allowed for memories of past events to fade and for matters that would be detrimental if forming part of such perpetual digital identity to be made less available. The launch of increased data protection in the EU, the new approach to the value of privacy and the recognition of the need to observe human dignity through autonomy, can all be provided for through the use of a wider form of the right to be forgotten. Focus on the right to be forgotten as being a limited recourse has been argued by Artemi Rallo to be considered as purely a reaction to technology providing endless access to personal data, but he also expressed concern as to the scope of the right believing this needs to be recognized as a wider right exercisable in other contexts not just against search engines as was found in Google Spain or against data controllers under Article 17.[187] Where the right to be forgotten can be considered as evoking wider scope, it is clear that for an online based society, it has additional and valuable impact to ensure other human rights are also respected. Indeed he reiterates that 'forgetting is intrinsic to the protection of human dignity'.[188]

There are of course counter arguments to the acceptance of the right to be forgotten in its widest form. Whether arguing that it cannot be seen as a potential fundamental right based on it not being considered truly essential nor universal as a right, or that it is merely a process created by Google or other search engines, or even merely a procedural requirement under the implementation of Article 17 of the GDPR, the right to be forgotten stands for a much needed global data deletion principle. [189] Rallo, has contrasted proposals offered by Benjamin Keele,[190] in favour of the maintenance of freedom of expression with explanations of the extent of the right by Jef Ausloos.[191] Overall these arguments provide that the right of erasure as specifically set out under Article 17 now supersedes previous debates in an attempt to

[187] Artemi Rollo 'The Right to be Forgotten on the Internet; Google v Spain' (Information Center 2018) p44
[188] ibid Artemi Rollo p 13
[189] ibid Artemi Rollo p 20
[190] Benjamin J Keele 'Privacy by deletion; the need for a global data deletion principal' (2009)Indiana Journal of Global Legal Studies. 16-1 pp. 363- 384
[191] Jef Ausloos. 'The Right to be forgotten - Worth Remembering?' (2012) Computer Law and Security review vol 28 143-152 p 147. 'Enabling a more effective control by the individual the introduction of a (well defined) "right to be forgotten" therefore seems appropriate at first sight.'

define the limits of the scope of the right when looking at how data protection can provide resolution. Such protection despite being based on two fundamental rights, only operates on a balancing premise, in his opinion, in a similar way to how the right to be forgotten can be exercised. This then argues that increased status for the right to be forgotten is not required. Ausloos claimed for a right of erasure merely as a practical response to the availability of non-essential information in an attempt to reduce the scope of a right to be forgotten which he believed should be limited.[192] More recently he has argued that clarity is required to meet the challenges of data protection which can involve 'defining power' so not just the balancing of rights but addressing the balance of the knowledge and information held by controllers 'versus data subjects'. This also involves the capacity to manipulate personal data to achieve data autonomy or what he agrees can be termed informational self -determination. Ausloos advises of the risks where 'protecting the data subject's autonomy in the face of power asymmetries, may impact others as well' which he considers evident in the Google Spain case.[193] This view becomes supportive of a right to be forgotten or a right of erasure being required to ensure effective data control, to empower individuals against what he refers to as 'the architectures of control erected by the information society services'[194]

However, in light of the potential ability of the right to be forgotten to provide wider recourse for informational self-determination, the right could be considered to merit an equal place as obtaining a new level of control outside data protection and privacy. To be viewed as a fundamental right is for there to be acknowledgement that the requisitions of data protection and privacy may not always be sufficient to offer the individual the autonomy they require to present to society the person they wish to be seen as. The intervention of the Internet and particularly the continual access has changed the boundaries of privacy, which if not dead is certainly changing and the procedural requirements of the GDPR could be argued to not offer the fluidity required to be able to apply informational self-determination. For this to occur, recognition of its status is required, whether by formal convention or through the jurisprudence of the ECtHR, as does the position of the implementor of the right to be forgotten, which rests primarily in the hands of ISPs, particularly search engines.

[192] seen n191 Jef Ausloos p 150
[193] Jef Ausloos, *The right to erasure in EU Data Protection Law* , (OUP 2020) 424
[194] ibid p 423

If the right to be forgotten is viewed as a timely response to the growth of the tech giants arising from the perceived economic need to provide both commerce and individuals with more and more information, its future still remains in the hands of those it is designed to protect individuals from. From the initial impact of Google Spain where the right was applied towards search engines to the provisions of Article 17 where the right of erasure provides an obligation on all data controllers, its application is now widened to cover the activities of internet service providers (ISPs) . The impact of such empires whose products are primarily based on obtaining data could potentially be compromised with the ability of a data subject being further increased to enable them to determine the control of the availability and accessibility of their data. With the restriction on smaller companies entering the same markets which the tech giants dominate due to cost of meeting not only regulatory requirements but also fulfilling the desire for new products by consumers, it is those larger entities that will be the providers of the decisions as to what should be forgotten. A lack of certainty, and therefore a lack of clarity, as to the scope and status of the right to be forgotten cannot help meet the need for the free flow of data balanced with the depth of benefits now required to maintain dignity. This is shown in the lack of clear guidance on how the balancing of rights should take place and what constant criteria are applied not just in respect of ISPs but across all those operating in the same field. In addition, with new awareness of the value of not only privacy but data control, the placement of such responsibilities on a commercial entity who now needs to fund and source this right seems not only unfair but unwise.

If regulation based on a form of digital ethics proves to be too complex to be put in place, and if direct responsibility should not be placed at the feet of such entities as search engines then the right to ask for the removal of links and the effectiveness of the right to be forgotten is compromised. In addition, its ability to offer sought after informational self-determination is jeopardized. It is essential that to meet the new demands of data subjects, who wish to use the services provided by the ISPs, that the position of these entities is clarified and appropriate resources put in place. There is a need to ensure that the commercial practices of these entities cannot negate the needs discussed in this chapter, that their monopolistic positions are heeded, and that formal protection for a wider right to provide informational self-determination can be guaranteed.

Chapter 7 Conclusion

As has been seen past decades have bought unimaginable changes to the way we as humans conduct our lives. The Internet has created not only the opportunity for innovation in the way business is conducted but other benefits such as education and the supply of information through data accessibility and data exchange as well as providing for social interaction. The use of social media has arguably completely changed the way society now functions and not always necessarily for the good. Some would claim that the price paid for this includes both the loss of privacy and control over personal data. In addition, there can be significant damage experienced through the creation of a form of eternal digital memory which no longer permits the human ability to allow memories to fade over time.[1] The intrusion of the past increases as more information becomes accessible, impacting not only human rights of privacy but an individual's dignity and reputation. Details of previous events and personal information no longer deemed relevant keeps the individual rooted in their past not the present. As has been shown, such information can portray a person in the least desired form leaving them with little recourse or control as to how society perceives them.[2]

This thesis considered whether the right to be forgotten can provide for an individual to be able to determine how to portray themselves online. It has examined the foundations the scope and extent of the right to be forgotten with the intention of arguing that such right is not only a right to have information forgotten or erased now under Article 17 of the General Data Protection Regulation (the GDPR) and particularly through the de-linking process established by Google but one that grants informational self -determination. This provides a step beyond the control of data or the protection of privacy leading to an ability to instantly restrict access to information about you. Such an ability would influence how you, as an individual, are portrayed through access to such personal data namely online. This would give additional rights potentially against the power of the tech giants meaning that an individual could potentially reduce the use and availability of personal data. The impact of such a right however must not be reserved only for the wealthy or powerful but needs to be made more

[1] See in particular; Viktor Mayer-Schönberger, *Delete*: *The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2011) at 2.
[2] Ibid See ch 5 and the PJS case

readily and consistently available so that it can be exercised with ease and transparency against such entities. This is an issue which is gradually being more widely debated with the rise of companies that specialise in dealing with such matters on behalf of their clients. The literature and focus to date have primarily been on evaluating the right to be forgotten from the aspect of delinking of search results or the removal of personal information through data protection to provide for safeguarding of privacy. This has necessitated the balancing of the right to be forgotten with the right of freedom of expression. The use of data protection regulation and particularly the finding of search engines as data controllers has arisen to ensure the required level of control. However, this thesis has deliberated that there is a wider impact when the right is exercised, arguing that it can be interpreted on a broader basis in line with original ideas of rights based on ideas of personhood and autonomy focused on the 'forgetting' of prejudicial information underlying the right. This subsequently provides for an individual to have informational self-determination. Based on original ideas put forward by the *Bundesverfassungsgericht*[3] and considered by many to be the foundation of data protection within Germany, such concept provides an individual with further recourse within a right to be forgotten to determine how they are portrayed in their society and specifically online. An interpretation of the right to provide such benefit can be more constructive, providing for more than limited aspects of data protection and privacy. This helps the right to provide an ability to exercise autonomy, maintain reputation as well as dignity and ultimately to effect rehabilitation.

To provide an understanding of the origins of the human rights forming the basis of the right to be forgotten, Chapter 2 looked at the beginnings of such rights and specifically at privacy. This included consideration of privacy's connections to underlying rights of freedom and dignity. Within an examination of the emergence of ideas of basic entitlements, which underlay human existence and provide for potentially universal rights, it was shown that there is recognition of privacy as a right that enhances such human attributes such as dignity, autonomy and reputation. Under the scope of privacy there is a natural desire to be in control of information pertaining to us and to restrict the result of it being made available to others

[3] The German Federal Constitutional Court in the case of 1983 Population Census Decision, 15 Dec 1983 BvR 209/83, *BVerfG* 65 1

irrespective of whether we wish it to be so available or not. Where particular personal information is made readily obtainable indefinitely and where it impacts a person's ability to portray themselves, a right that could afford more control with the opportunity to allow such information to be forgotten before it adversely affects an individual's ability to lead the life they aspire to, has become increasingly important.

The development and acceptance of human rights can be seen in the examination of various theories as to how they are formed and utilized. These are often subject to cultural influences which has been the subject of keen debate over the establishment of certain rights. Although it can be accepted that not all rights bear the same importance, data protection and privacy, often considered the basis of the right to be forgotten are now widely recognized and can be seen to have the same roots essentially providing for individual autonomy. This also accepts the importance of the foundation right of dignity with the protection of reputation to ensure an individual's position in society. Such established rights are now vital to ensure that an individual obtains the level of control and protection that the flow and accessibility of data now demands.

This chapter also considered the acceptance of data protection as a fundamental right whether considered as a subset of privacy or as provided for in the EU's Charter of Fundamental Rights (the Charter)[4] and how acceptance of such status has been steadily growing shaped by the new challenges brought about by information technology. Personal information now has the potential to be retained permanently in digital form as opposed to the natural function of the human mind. It can be seen to be collected from various activities, enhanced by the use of artificial intelligence and retained through the development of databases to be accessed indefinitely through on -line activities such as searches. This creates the opportunity for not only privacy to be prejudiced but also dignity and reputation highlighting the need to evaluate and understand the potential scope of the right to be forgotten and what remedy it can offer. With acceptance that this right represents something fundamental to ensuring the protection of an individual's ability to conduct their life as they think fit, by retaining the ability to be autonomous and be able to portray themselves as they

[4] The Charter of Fundamental Rights of the European Union [2000] OJ C 364/1

desire, the right then becomes vital to ensuring a sense of self. Using the concept of informational self-determination which refers back to its original roots in Germany[5] evoked under the principles of the right to be forgotten, such right can be established as a right developing from dignity through the quest for autonomy and identity to offer such protection.

In chapter 2 whilst looking at the building and acceptance of relevant human rights, it could be seen that application of concepts of freedom in the sense of autonomy as expressed by Sen or in personhood proposed by Griffin, are being acknowledged within many jurisdictions particularly where the idea of identity or persona is more established. It becomes clearer that the right must not only protect an individual's aspirations but meet society's expectations so such individual can be assured of maintaining reputation within society and even rehabilitation. The right to be forgotten despite the need for wider scope still remains a limited right to be balanced by the right to freedom of expression and any social contract made between state and citizens to enforce this protection. In an era of formidably accessible information the right to portray yourself in public, whilst retaining privacy around information that you do not believe should define you for eternity, is however vital.

Within Chapter 3 a detailed analysis of the recognition of how data protection had become a fundamental right in the EU was shown. This also demonstrated why it warranted the increase in formal protection provided by the final implementation of the GDPR[6]. Such analysis then examined the emergence of the right to be forgotten through not only the balancing of rights of privacy and freedom of expression but through rights of rectification and removal of data provided under the Data Protection Directive (DPD).[7] The emergence and acceptance of the right formed part of the drive towards a new data regime. The decision in Google Spain[8] may

[5] Right of informational self-determination was argued to have originated in the case, 1983 Population Census Decision, 15 Dec 1983 BvR 209/83, *BVerfG* 65 1 see also Orla Lynskey *The Foundations of EU Data Protection*, (OUP 2015) ch 4, 94

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[7] The Data Protection Directive, 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31

[8] Case C- 131/12 Google Spain Sl Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González, [2014] ECLI: EU:C:2014:317 (Google Spain)

be considered to have pre-empted the finalization of the GDPR but it is clear that the right to be forgotten, as now accepted, was seen to be necessary to provide a valid recourse for those wishing to maintain their privacy as well as potentially reputation by controlling the availability of personal data accessible through the Internet. The 'right of erasure' now in the form of Article 17 of the GDPR,[9] can be seen to support autonomy and potentially the ability to shape one's identity in a digitalized world.[10] Such rights form part of the fundamental standards necessary to provide each human with tools to protect their individuality and sense of self although balanced with rights of freedom of expression as well as the public's right to receive information. Direct opposition to the right to be forgotten and any extension of its application, particularly in the US with its emphasis on liberty and freedom to express opinions, highlights the need to define more clearly where the right can and should be used. Although freedom of expression must be respected, it needs to be balanced with other human rights to provide for a rounded approach to the control of personal information particularly within the environment of the Internet.

Chapter 3 further identifies how recognition of the new right to be forgotten has faced many challenges by those disputing the necessity for it.[11] The idea of the Internet as a conduit for information exchange with the ability to be able to freely express views, often controversial and increasingly discordant, was still seen as being diminished by the right to remove past events or history resulting in further controversy in the overall acceptance of the right to be forgotten being necessary. With the evolution of data protection despite the constraint of the balancing of rights, the movement within the EU member states finally saw the foundations laid for such a right in the Google Spain decision. Final recognition of the right of erasure, also termed the right to be forgotten, was subsequently implemented through the GDPR.

[9] GDPR, Art 17, Right of Erasure ('right to be forgotten') available at https://gdpr-info.eu/art-17-gdpr/

[10] EU, Complete guide to GDPR compliance, July 2019; 'The right to be forgotten dovetails with people's right to access their personal information in Art 15**.** The right to control one's data is meaningless if people cannot take action when they no longer consent to processing, when there are significant errors within the data, or if they believe information is being stored unnecessarily. In these cases, an individual can request that the data be erased. But this is not an absolute right. If it were, the critics who argue that the right to be forgotten amounts to nothing more than a rewriting of history would be correct. Thus, the GDPR walks a fine line on data erasure.' available at https://gdpr.eu/right-to-be-forgotten last accessed 25 Feb 2021

[11] see Christiana Markou , '*The Right to be Forgotten' : Ten Reasons why it should be forgotten*: in (eds) Serge Gutwirth, Ronald Leenes, Paul de Hert *Reforming European Data Protection Law* (Springer 2015)

In Chapter 4, the ground-breaking precedent of the Google Spain case[12] and the subsequent debate as to the extent and scope of the right as set out in the decision was examined to understand more fully how the case arose and the influence of its principles. Here the decision of the CJEU and the part it played in finding the existence of a right to be forgotten was unprecedented. It clearly accepted the emerging concept of the right to be forgotten albeit without clear definition of the right's scope or extent of its application. With its immediate and most relevant impact on the liabilities of search engines, specifically Google itself, it also challenged the level of protection provided to such entities and to wider ISPs. The case was not without controversy initially specifically in going against the opinion of the AG Jääskinen [13] and this outcome was to many, instrumental in the finalization of the provisions of the GDPR and specifically Article 17 to prevent the need for judge made decisions to shape the new path data protection was taking.

The direct focus on search engines was debated hotly as not only going against previous protections and attitudes towards such entities but in the acceptance that any such companies had some form of control over the contents revealed. New principles relating to the 'erasure' of data considered under the DPD as well as the balancing act of competing human rights of privacy and freedom of expression under the Charter would now be applicable to other entities engaged in data driven activities if found to be data controllers. This chapter also examined the jurisprudence and legal commentaries in relation to the Google Spain case which created a more detailed understanding of how the right could be applied whilst waiting for decisions to be made under the GDPR, formalized two years after the decision and implemented as late as 2018. From such analysis, it has become clearer that the scope of the right to be forgotten can be expanded to provide a wider form of control of personal information through ideas of informational self-determination. It is still unknown how the application of the GDPR's right under Article 17 will be applied but whilst waiting for this, there is now greater recognition of how the right is taking shape and gaining acceptance

[12] n8 Google Spain

[13] Case C-131/12, Google Spain Sl Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González, [2013] ECLI: EU:C:2014:317, Opinion of Advocate General Jääskinen

on a more international basis with growing interest in the ability to control personal information being made constantly available through digital memory.

The tension of the balancing act between the right of privacy and freedom of expression has increased focus on Google Spain's decision which cannot be underestimated in terms of its new approach and influence. This has highlighted privacy and also reputational concerns as to how information is presented and retained through digital memory with the attendant risks to personal freedom. Despite not being as detailed as many commentors would have wished, the scope of the precedent established under Google remains as valid and essential to the application of the right as at the time the case was determined

In chapter 5, the question of how the right as it is now being applied and potentially being interpreted to provide for informational self -determination was considered. Despite claims from the internet giants to say that the price of freedom of access to information available globally 24/7 is the accepted loss of privacy or the reshaping of expectations of privacy,[14] it can be seen that such availability of data has become increasingly intrusive and the impact on individuals much greater. The ability to use vital tools such as the Internet seems to have come at the expense not only of privacy but of wider loss of control of autonomy over how you are portrayed. Looking at applications of the ability to hide or forget information within Europe, this examination showed how the right to be forgotten could protect both dignity and reputation by providing an ability for an individual to ensure that their portrayal online reflects the person they are, unhindered by irrelevant past information however valid. Potentially this would also support ideas of rehabilitation within society. This results from acceptance that the disruption caused by a digital memory and its consequences may prevent a enable a person from leading a good life within the constraints of society. If past mistakes are bought constantly to viewers' attention even to legally 'forgotten' events such as bankruptcy orders as was the issue at the heart of the Google Spain case or criminal convictions, there is no way of escaping the damage such information does. These revelations even when referring to spent convictions i.e., the convictions that society or societies have

[14] Bobbie Johnson, 'Privacy is No Longer a Social Norm says Facebook Founder' The Guardian available at http://www.theguardian.com/technology/2010/jan/11/facebook-privacy last accessed 18 November 2020

deemed not significant enough to be remembered forever, can be still available and damaging to both dignity and reputation further blocking the ability to be rehabilitated. To add to the debate, it is clear that data protection in itself, as largely a passive function, has no active life unless enforceable action is provided through the data industry or under regulations or laws. An individual can only look to protect or control their data by activating such laws or regulations that exist rather than increasing the responsibilities of those who oversee such activities. The CJEU's decision in the Google Spain case, intended to provide protection for EU citizens but without sufficient clarification as to how when and where. The provisions of Article 17 may well add clarity and to provide a clearer response.

In this chapter, how the right to be forgotten interacts with other rights and where its principles can be expanded to supply wider recourse, specifically slanted towards accessibility of information on or through the Internet was examined. By the drawing together of ISPs and particularly search engines onto territory where journalistic protection does not apply, the ability for the right to provide new solutions in areas involving the provision of personal information and data is key to maintaining wider rights such as dignity and autonomy.

An extension of the scope of the right to be forgotten can therefore offer the potential for providing a more appropriate profile on the Internet and of assuming control of your portrayal of self or what can also be referred to as a form of digital identity. The extent that this may be provided may become clearer as more cases gradually emerge. An understanding of both the potential or limitations of Article 17 will also help with the realization of informational self-determination. The more structured and mechanical nature of Article 17 of the GDPR building on existing remedies under the Data Protection Directive may be sufficient to provide for the deletion of inaccurate, out of data or data no longer required as a minimum with the balancing of rights creating further scope.

The cases examined in this chapter highlighted the different approaches taken by various member states to determine how much information should continue to be made available to the public. Questions of the public's right to receive information formed a key part in deciding what if any removal of information or links to information could take place. However, whilst

balancing privacy, its protection and the misuse of data with freedom of expression, despite claims opposing the right, there may not be as many opportunities to 'rewrite' history as suggested. It is clear that the public's right to receive information must be a factor in the extent in which self -determination can take place but is part of the balancing act that needs to take place. The impact of decisions based on assessing the harm experienced by an individual and the way they could conduct their lives in light of the availability of such information may prevent significant obstruction to the removal of information where the public interest is paramount.

The range of cases showed the opportunities where recognition of the need for privacy has evolved bringing in wider rights over personal information leading to how an individual is portrayed online. These bring emphasis on the importance of taking your place in society and where the availability of information, in particular through the Internet, can be the cause of a person being adversely affected whether by loss of autonomy or dignity, by loss of reputation or just by irrelevant information whether accurate or not. A desire to be able to apply informational self-determination to leave the individual in control of not only their private life but their ability to maintain dignity reputation and as was shown, take advantage of any opportunities for rehabilitation into society is a natural development of the right. This is also reflected in recent developments within the technology industry. In a response to changing views, Google has recently decided to automatically to delete user history quoting its concerns as to users' privacy and control of data as important to its business.[15] In addition Facebook, another ISP, has provided means of removing access to certain pieces of information through its users' settings. Intuitively people are claiming rights of privacy and data protection to control how much data is collected, processed and made available and how this can portray them. In doing so they also claim the right to determine how they are represented as persons through such data. When decisions seem to lack consistency in

[15] Google CEO, Sundar Pichai, announced the new changes in blog post, emphasizing the company's commitment to security, privacy and user choice. Pichai emphasized the company's commitment to privacy, security, and user choice." As we design our products, we focus on three important principles: keeping your information safe, treating it responsibly, and putting you in control," available at https://www.theverge.com/2020/6/24/21301718/google-auto-delete-location-search-history-default-myactivity or https://www.computing.co.uk/news/4016956/google-automatically-delete-users-search-location-history-months last accessed 5th Dec 2020

approach or transparency in how such decisions are made, the need to argue this right as informational self -determination becomes clearer. It may also be that as a result of this reclaiming of autonomy that the tech giants should no longer be considered the decision makers in applying the right.

This change in approach to recognizing the rights of internet users specifically, led to an examination in Chapter 6, which not only looks at the difficulties in defining the right to be forgotten as a fundamental right but also how the 'power' held by such entities impacts on the exercise of the right to be forgotten with regard to informational self-determination. From this, concerns over the power held by 'data opolies' represents a new approach to ensuring protection for individuals whether considered consumers or data subjects through the operation of the right to be forgotten. This emphasizes the realization that privacy together with other individual rights need to be secured and not overridden by increasing lucrative commercial practices. The chapter also challenges the ability of a commercial entity to provide effective enforcement of the right or a form of regulation sufficient to ensure that the interests of data subjects who are also users of that enterprise's services are met.

From the research the right to be forgotten or right of erasure now under Article 17 of the GDPR does provide for a person to control personal data with regard to erasing information or links to information and through this informational self -determination. Using the right to be forgotten to shape how one appears through the Internet, by access to searches and through social media whether by links or directly, provides further control over how such individual is portrayed and ensures the element of choice in respect of personal data being made available. The individual can therefore be in control through managing the accessibility to their data which can impact their life. This is in line with the original arguments expressed by such writers as Meyer Schonberger, for allowing memories of past events to fade and for such information that would be detrimental if forming part of an eternal digital identity, to be made less available. Ideas attached to the value of privacy, such as the need to observe human dignity through autonomy can provide additional protection for reputation through use of a wider form of the right to be forgotten. As a limited recourse, as argued by Artemi Rallo, the right could be considered; 'purely a right in the face of technology providing endless

access to personal data.' However, he further comments, 'the debate on the right to eb forgotten has everything to do with the future risks of the Internet for reputation, privacy, liberty and human dignity' echoing here the words of Solove.'[16] Can it be the case that it must be applied through a wider approach. The scope of the right to be forgotten may not just be limited to mere deletion or erasure but to allow the ability to select how you can be viewed to protect other rights.

The result of this wider right is not merely the ability to access data and the loss of control or loss of privacy but the ability to control how you as an individual can be perceived by society and the subsequent consequence on the way you lead your life. The outcome of the cases discussed show that where there has been claims made under the new right, the concern has largely been not to just have information forgotten by a delinking exercise or now 'erased' under Article 17 but to ensure that there is not prejudice towards the person through the instant access and continuous availability of information. Such information in pre internet era would not have remained so instantly accessible nor had the detrimental impact now being seen. A wider interpretation can be argued to merely return the person concerned to a pre internet status where past events are allowed to remain in the past.

Where the right to be forgotten evokes much wider scope, for individuals taking part in an online based society, it can have additional and valuable impact providing protection against the onslaught of new technology. Through the process created by Google and followed by other search engines, and as now required under the implementation of Article 17 of the GDPR, the right establishes a global data deletion principle [17] In the words of Jef Ausloos 'It formalizes, by laying down a legal infrastructure—subject to safeguards taking into account other rights, freedoms, and interests—to empower data subjects. Embedded in a broader legal infrastructure, it puts the tools in data subjects' hands.'[18] Superseding previous debates trying to limit of the scope of the right, the right to be forgotten can be considered to take an equal place in obtaining a new level of control outside data protection and privacy. With its

[16] Artemi Rallo *The Right to be Forgotten on the Internet: Google v Spain*, (Electronic Privacy Information Center 2018) p16
[17] ibid Artemi Rallo p20
[18] Jef Ausloos *The Right to Erasure in EU Data Protection Law*, (OUP 2020) Part III Section 4 p 442

scope based initially on the principles of Google Spain and now the procedural requirements of the GDPR, the ability to use it fully is potentially curtailed by the entities that implement the right. To be able to exercise the right is a timely response to meet the increasing power of the tech giants respecting a new awareness of privacy with demands for further control by individuals. However, whilst the decision-making rests with such entities the extent of the right to provide informational self -determination to enable control over how you are portrayed online may remain limited.

Other than where there is a need for the information to remain accessible for public benefit, the importance of personal information no longer being available as determined by the individual concerned impacting how an individual is portrayed and ultimately their reputation is vital. This prioritizes not only a full and comprehensive understanding of the full extent of the right but the need for effective enforcement. In the words of Meyer Schonberger 'We live in a global village where "forgetting has become exception and remembering default"[19] This enhances the potential damage of an everlasting digital memory. This builds on the necessity for an individual's ability to be able to use informational self-determination to ensure how they are portrayed online. This however brings huge challenges with regard to the power of such commercial organizations in providing for application of the right[20]. Although this thesis has concentrated on Google as the pragmatist in the Google case and the author of the removal process, the right to be forgotten must also be exercisable within other scenarios and against other bodies.[21] Restrictions potentially through digital ethics may be too complex to be enforced as was debated in chapter 6. However, if direct responsibility cannot be placed at the feet of such entities as search engines by way of self-regulation to manage the availability of information and the right to ask for the removal of links, the effectiveness of the right to be forgotten is compromised and its ability to offer sought after individual self -determination could be jeopardized. It can be questioned as to whether fines become

[19] Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2011)

[20] n18 In this Jef Ausloos conducted a study of responses from 66 Internet service suppliers in 2017. This culminated in his opinion with not one response being fully satisfactory in that all required further communication with the data controller. see Part III Section 3.2 p433

[21] In fact it can be seen in the Google Transparency report that the highest number of requests for removal under the right to be forgotten process relates to posts on Facebook available at https://transparencyreport.google.com/eu-privacy/overview?hl=en_GB last accessed 18 Feb 2021

meaningless against the might of the entities effectively controlling the Internet.[22] Whereas ideas of self-regulation are often seen as the simplest route, it is clear that this ensures that the relevant commercial organisations drive the response and set out how the right can be administered. It is equally clear that this does not necessarily provide the result sought by individuals nor potentially work within the legal rights set out within Article 17. Despite the intension seen at both the EU and UK level as discussed in Chapter 6 not only has a form of self-regulation not yet been effected, it is by far not universally agreed. With a lack of acceptance of such need by the companies creating potential data-opolies, the course of agreeing the perimeters and liabilities through such self-regulation looks turbulent. A simple step froward would be to build upon the Google Spain process introduced by Google, yet such process has not been adopted by other search engines and the likelihood of it being so seems remote. [23] So the right to apply the protection afforded not only through the decision in Google Spain but now enacted within the GDPR remains with the corporate entities who now need to support the regulation as well as potentially apply the balancing of fundamental rights.

With the capacity to manage the forgetting of the past as it or events within it are no longer relevant, who makes that decision which might have ever lasting consequences is key. Is it the commercial organization intent on maximizing the values obtained from the free flow and free access to data or is it the society that through legal recourse establishes the boundaries to the ability to retain and never 'forget' such information? The constant delicate balance between freedom of speech/ expression and privacy continues to grow with examples almost daily of movements towards claiming back privacy, certainly by the rich and famous with more to lose but also by those not so famous wanting to restrict forages into their past as was

[22] When John Perry Barlow wrote the Declaration of Cyberspace, he envisaged a new space free from the restrictions of the real world with its politics and laws, however this approach relied on the benevolence of the tech giants rather than ensuring a form of meaningful control. This creates an issue in providing effective self - regulation without interference.

[23] An example can be seen in the European Commission's report on "Assessment of the Code of Practise on Disinformation- Achievements and areas for further improvement' 2020 available at https://s3.eu-central-1.amazonaws.com/euobs-media/b29cdd11fe0160c7f01ad68779305b51.pdf where Vera Jourová indicated that the code of conduct had shown that online platforms and advertising sector could do a lot to counter disinformation but the time had come to go beyond self-regulatory measures. Although in a different field an analogy could be drawn here.

seen with Senor Gonzales. In the case of Sir Cliff Richards [24] despite media opposition towards what could be seen as a major fetter on the freedom of journalistic investigations the 'public' saw this has unwarranted abuse of such abilities to an innocent man, albeit in the public eye, previously un-convicted 74 year old man. The development of a theme of morality particularly with regard to the extent of how rehabilitation can be established reflects the level of concern as to the impact of reputation on personal freedom. It also brings into question how the power of large corporate entities enables them to act in breach of such rights without any form of comeback.

The new right if considered a fundamental right linked to privacy and in line with it being created by regulation as part of a fundamental right to data protection grants an individual agency to not only control the availability of data which can be protected under more prosaic laws, to utilize autonomy, to protect not just privacy but reputation as well as the ability to be rehabilitated into society. Here the balance between privacy and freedom of expression can be used a gauge to protect and maintain that person's place in society. Not just to redefine themselves to present the best image of self but to become as if a new member of society, to have a value and to be capable of continuing to take a useful part in society. The extent of the availability of links to past occurrences needs therefore to be considered in light of developing social requirements. However, this will always be balanced against the desire that history is not being rewritten nor freedom of expression compromised. However, as technologies grow and bring further changes to society so human rights transform to reflect the times they are being exercised in. Basic freedoms may be accepted and largely unchallenged in many developed states, but new frontiers are being faced. Here the question arises as to how the state should potentially intervene to protect its citizens whether through deeper regulation of the internet service providers or by providing independent bodies to oversee the decision making.[25] Through the challenges faced by implementation of the right through the ISPs, the ability to refer to the appropriate data protection authorities and ultimately the courts the way ahead seems to long drawn out. However with the increase in

[24] Sir Cliff Richard OBE v (1) The British Broadcasting Corporation (2) Chief Constable of South Yorkshire Police [2018] EWHC 1837 (Ch))

[25] See Carnegie report in the UK where an independent regulator in the form of OfCom to oversee the activities of internet platforms was proposed. available at https://www.carnegieuktrust.org.uk/publications/internet-harm-reduction/ last accessed 24 Feb 2021

interest in regulation of the ISPS and the development of new ideas as to how the EU member states can tackle such issues[26] it may well be that new avenues to obtain the protection needed are being prepared.

It has been seen that the challenge may be how to promote the right whilst restricting abuse of other rights. There is no doubt that as the right to be forgotten represents a new key fundamental right which allows the past to be hidden where required by an individual seeking to control access to personal information to protect the way they are portrayed. Ease of availability on an unprecedented scale is curtailed under such right preserving the ability for an individual to be able to exercise a right of informational self determination to protect the way they are viewed and limit accessibility to their personal data. Even to benefit from rehabilitation. Current times with modern future needs demand rights that can clearly exist and be defined as such.

As George Orwell stated in the book '1984' where life was controlled by 'Big Brother' a seeming forecast of the future ahead, 'He who controls the past controls the future'[27] This phase is the motto of the controlling Party who rewrites history on a daily basis to meet the current needs or aims of the Party. This is what sums up the negative approach to the right to be forgotten and currently prevents it being viewed more widely as a fundamental right to provide not only the right to have information forgotten but to ensure informational self-determination despite increasing interest in the need for such protection on a global basis. Once an understanding of the right is recognised as not giving a blanket freedom to re-write history, then its true value in ensuring an accurate reflection of a person in 'real' time will be accepted.

[26] In Feb 2019 France announced its intention to provide for a new law to tax internet and technology giants on their internet sales in France. see https://www.euractiv.com/section/digital/news/france-set-to-introduce-new-tax-on-internet-giants/ last accessed 13 Feb 2021. In addition, more recently Germany has proposed further legislation. On January 12, 2021, the German Ministry for the Economy and Energy released a new draft Law on Data Protection and the Protection of Privacy in Telecommunications and Telemedia (TTDSG). see https://www.insideprivacy.com/data-privacy/germany-publishes-new-draft-rules-for-cookies-and-similar-technologies/ last accessed 22 Feb 2021

[27] George Orwell, '*1984*', (Originally published by Secker & Warburg 1949, reprinted Penguin Modern Classics 2008) Ch II p 44.

In the meantime, the challenge will remain as to how such right can be exercised to provide the maximum protection. As seen, it cannot be the case that the main decision maker is the protagonist in Google. With the extensive interest in its 'products' and the increasing monopoly for daily way of life, this form of individual protection should not also rest in such hands. The counter argument must be that to preserve freedom of expression, should it be up to an individual to determine how much of the past they can erase in order to preserve how they see themselves and how they maintain their reputation and dignity as well as privacy. The next step is to consider whether there should be a regulatory review for such decisions and here whether the state in its various forms must take over 'policing' this right or place in it the hands of a non profit making organization, not a commercial one.

The provisions of Article 17 which now shape formal recognition of the right under the GDPR should ultimately mean that the overall regulator that can challenge decisions would be the appropriate state Data Protection Authority. However, a freedom of information request[28] has revealed that the amount of referrals made to the UK DPA following a decision made by Google, have certainly been very limited in view of the number of applications made direct to Google[29]. Although there is information concerning the volume a lack of transparency is evident as there is not information that expands upon the reasons the applications were made nor the reasoning behind the decisions.

This emphasises the difficulty around trying to identify the scope and the extent of the right to be forgotten and how it can be effectively applied. The water has been further muddied by the recent case in respect of Facebook, a prominent tech giant, which has also endured difficult privacy and data protection issues as was seen in the Cambridge Analytics scandal. The case of Glawischnig-Piesczek v Facebook [30] also heard in the CJEU was reported by the

[28] Freedom of Information Request, UK ICO (Case Reference Number IRQ0856742, Aug 2019),this noted ; There have been 102 requests received (25 May 2018 – 9 July 2019) under the provisions of Article 17 (GDPR) the right of erasure also known as the right to be forgotten. Data subjects are advised that they have the right to apply to a court if they believe there has been a contravention of their rights under data protection legislation. We are not aware of any applications to the Court in respect of decisions in regard to the right of erasure or the right to be forgotten (Article 17, GDPR) by the ICO.'

[29] In the UK 218,540 URLs were not delisted by Google representing 46.6% of the applications made. see Google Transparency report, https://transparencyreport.google.com/eu- last accessed 19 Feb

[30] Case C-18/18, Eva *Glawischnig-Piesczek* v Facebook [2019] ECLI:EU:C:2019:821 See also Press release 'EU law does not preclude a host provider such as Facebook from being ordered to remove identical and, in certain circumstances, equivalent comments previously declared to be illegal' available at

EU Press Office as concluding that 'EU law does not preclude a host provider such as Facebook from being ordered to remove identical and, in certain circumstances, equivalent comments previously declared to be illegal.'[31] This case widening the ability to force removal of information damaging to reputation[32] whilst bought under the Directive on Electronic Commerce[33] showed clearly the concern that there needs to be clarity for worldwide solutions albeit arguing here on under private international law.

Part of the immense contribution made by the Google Spain decision has been the confirmation of a search engine, an Internet service provider, as a data controller with the additional responsibilities placed on Google in this instance to also administer the right as determined in the case. It can however be noted that the tech giants have superior technical and organizational skills as well as resources to address requests under the right to be forgotten more quickly than state funded regulators. The role of the search engine has been the focus, and as such has increased awareness, of the process with recent calls for the benefit of such process to be made available to all users of search engines.[34] Concerns have been raised as to whether such companies operating on the Internet should 'serve as guardians of the world citizens' rights online.'[35] Others have expressed concern that such internet entities become the judge and the jury in such decision making.[36] If the question of whose laws should be applied is also involved, this heightens the tensions. However, this also brings into account the role of such a commercial entity as a potential quasi regulator amidst claims of such entity being in a too powerful position generally. There is however a changing approach briefly discussed in Chapter 6 where the recent actions against the monopolistic character of the

https://www.euractiv.com/wp-content/uploads/sites/2/2019/10/CP190128EN.pdf last accessed 28 Feb 2021

[31] ibid https://www.euractiv.com/wp-content/uploads/sites/2/2019/10/CP190128EN.pdf

[32] In this case the comments published by the user were found by the Austrian court to be harmful insulting and defamatory to the claimant.

[33] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ('Directive on electronic commerce') OJ 2000 L 178, p. 1)

[34] Rebecca Heilweil, 'How close is an American Right to be forgotten?' , March 4 2018, Forbes https://www.forbes.com/sites/rebeccaheilweil1/2018/03/04/how-close-is-an-american-right-to-be-forgotten/#466ab9f9626e see also Technology News Sept 24 https://www.reuters.com/article/us-eu-alphabet-privacy/you-have-the-right-to-be-forgotten-by-google-but-only-in-europe-idUSKBN1W90R5 last accessed 19 Dec 2020

[35] Giancarlo F Frosio, 'The Right to be forgotten: much ado about nothing' 2017 Colo Tech LJ vol 15.2 pp 307-315

[36] Mariarosaria Taddeo, Luciano Floridi, 'The debate on the moral responsibility of Online service Providers' 22 Sci & Engineering Ethics 2016 1575 1592 p 20

tech giants particularly the FAANGS have called into question the dominance of such entities. This is also reflected in the reaction of such entities to the increasing pressure on them. An example of this is the recent decision made by Google to remove information after a period of eighteen months. Although this is largely in relation to default settings on search and location history, this represents a huge move towards recognition of the digital memory and its consequences. As summarized by its CEO, Sundar Pichai 'As we design our products, we focus on three important principles: keeping your information safe, treating it responsibly, and putting you in control.' [37]

Regulators, the press and the public are increasingly vocal about what is seen as the negative side of technology. Following from an initial excitement and optimism doubt has set in resulting in an acceptance of more control of activities carried out digitally. This has accelerated into more scrutiny and built expectations that such entities should become accountable. With wider acceptance of the right to be forgotten as a fundamental right, and one that has broader scope, the way forward to ensure informational self -determination may be the appointment of independent regulators to perform a function outside of the data protection authority. This idea has been called a 'wild card' involving looking at initial steps to bring focus on board not just for data protection but for anti-competition or anti-trust initiatives.[38] This may provide more 'hands on' oversight and intervention. The path towards digital regulation in line with some of the views discussed in chapter 6 such as digital ethics or a bill of rights for the Internet would offer the opportunity for more independent review and consistency. With harmonization a long-term goal, despite the opposing stances taken by the EU and the US, there is more common ground based on acknowledgement of the power of the tech giants and a reluctance of power to be left in their hands. Concerns revolve around a lack of transparency or consistency not just with regard to data but to process and decision

[37] Press Release, 'Google is now to delete information after 18 months' available at https://www.computing.co.uk/news/4016956/google-automatically-delete-users-search-location-history-months last accessed 18 Dec 2020

[38] This is not however a new idea but more of a realization of the necessity of such a role. As early as Nov 2017 Buttarelli then European Data Protection Supervisor stated that 'I'm not saying we will need a European FTC (US Federal Trade Commission), but we will need a Digital EU Regulator.' Further adding that the posiiton would have the powers to also look into competition and consumer protection issues raised by processing of personal data (so, therefore, in addition to data protection issues). see https://fpf.org/blog/a-conversation-with-giovanni-buttarelli-about-the-future-of-data-protection-setting-the-stage-for-an-eu-digital-regulator/ last accessed 22 Feb 2021

making and the use of artificial intelligence. Here the roll out of the GDPR with its impact of securing rights for European citizens impacted by the activities of non-EU based companies has perhaps led the way to greater acceptance even within the US. Buttarelli called not only for 'friends of privacy but for more than that, a coalition to preserve and advance the dignity of real people'.[39] If further regulation is not possible and it is accepted that this task would be a massive one, then perhaps as a minimum to ensure transparency to grant the right to provide the informational self-determination, a Code of Good practice. This could set out the agreed principles to provide the transparency in relation to decisions under the right to be forgotten necessary to ensure consistency. However, it must be recognized that the challenge of ensuring the right to be forgotten is exercised is still being met where possible by the DPAs. As recently as November 2020 the Swedish DPA fined Google the sum of 75 million Kroner for not complying with requests for delinking in two cases.[40] In addition on the 27th November 2020 the UK announced that a new UK regulator would be created in an attempt to ensure that the power of entities such as Google and Facebook and other ISPs would be curbed.[41] Under a dedicated Digital Markets Authority a new code of practice would be prepared to enforce a new code of practice which limits to certain effect the dominance of the technology companies whilst ensuring what is referred to as 'acceptable' behaviour. Although targeted at curbing such anti-competitive activities, this represents a very important step in how the tech giants are being perceived and how they can be bought under control. Voiced as an intention to avoid negative impact on people by the activities of commercial entities, it may be the first step in an emergence of acceptance of the need to rein in such bodies to ensure individual rights are protected under the right to be forgotten and that the use of the Internet does not diminish them. Despite Google's vehement

[39] Giovanni Buttarelli, 'Privacy Matters: updating human rights for the digital society' Health Technol., 2017, 7:325-328

[40] 'The Swedish Data Protection Authority imposes administrative fine on Google', https://www.datainspektionen.se/nyheter/the-swedish-data-protection-authority-imposes-administrative-fine-on-google/?utm_source=POLITICO.EU&utm_campaign=528b156d70-EMAIL_CAMPAIGN_2020_03_11_10_52&utm_medium=email&utm_term=0_10959edeb5-528b156d70-189713005 last accessed 11 Jan 2021

[41] The Competition and Markets Authority will create a Digital Markets Unit which will oversee the introduction of a new code of practise for technology companies affecting those companies deemed to have' strategic market status' as yet undefined see 'New UK tech regulator to limit power of Google and Facebook available at; https://www.theguardian.com/technology/2020/nov/27/new-uk-tech-regulator-to-limit-power-of-google-and-facebook last accessed 8 Jan 2021

protestations and intention to appeal, this is the next stage in recognizing that individuals right must take precedence over commercial interests and that to achieve this in the absence of being able to enforce human rights through the national courts and the European Court of Human Rights, state appointed regulators must now move forward.

Although the need for enforcement is clearly vital to establishing the validity of the right of erasure under Article 17, its potential use to provided informational self-determination is supported by it being recognized as a wider right, by the cases not only determined by the CJEU and national law however limited to date but to some extent by the approach gradually developing through the European Court of Human Rights. With the change of approach towards to protection required for privacy and data protection to one which brings with it rights over dignity and reputation, the ability for an individual to control how they are portrayed online is now being met providing the ultimate power to enable a person to take part in society irrespective of past events or occurrences. As such it must be welcomed and applied.

BIBLIOGRAPHY

PRIMARY SOURCES

Legislation

*Codice civile*no, 262 of 16 March 1942 (Italy)

The Universal Declaration on Human Rights, 1948

American Declaration of the Rights and Duties of Man, 1948

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 134 November 1950, ETS 5

International Covenant on Civil and Political Rights, 1966

International Covenant on Economic, Social and Cultural Rights, 1966

Communication Decency Act 1966`47 USC s 230

International Covenant on Civil and Political Rights, 16 December 1966, United Nations,

International Covenant on Economic Social and Cultural Rights, 16 December 1966, United Nations,

The Second Chance Act (HR 1593) US 1968

American Convention on Human Rights, Nov 22 1969, No. 17955

Rehabilitation of Offenders Act, 1974 c 53

Restatement (Second) of Torts 652D (1977)

German Federal Data Protection Act (*Bundesdatenschutzgesetz* [BDSG] 1977

Information Technologies Data Files and Civil Liberties Act, n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (Amended by the Act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data) (France)

African Convention of Human and Peoples Rights, (the Banjul Charter) June 1981

Council of Europe Convention No. 108 on Data Protection, Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.01.1981).

Dutch Data Protectuion 1989 (*Wet Persoonsregistraties privé-levenssfeer, persoonlijkleven,privé-sfeer, persoonlijke levenssfeer, persoonlijke vrijheid, privé-leven*7) (The Netherlands)

Treaty on European Union, 1992 OJ C 191, pp. 1-112

Data Protection Directive, 1995 95/46/EC

Communications Decency Act of the United States of America 1996 47 USC s 230 (contained in title 47 of the United States code) available at http://uscode.house.gov/browse/prelim@title47

Data Protection Act 1998 c 29 (UK)

The Charter of Fundamental Rights of the European Union, [2000] OJ C 326

Communications Decency Act 1996, 47 USC. amended by S 230 (2000). (US)

Council Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

Treaty of Nice, Amending the Treaty on European Union, the Treaties Establishing the European Communities and Certain Related Acts, 11 December 2000, Official Journal C 80 of 10 March 2001; 2001/C 80/01,

Directive on privacy and electronic communications) 2002/58/EC 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector **(**ePrivacy Directive)

The Federal Trade Commission Act (15 U.S.C. SS41-58) 2006 (US)

The Second Chance Act 2007 (HR 1593) (US)

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community 2007 C306/01

Council Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws OJ L 337, 2009

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the

free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 (Ireland)

Data Protection Act 2018, c1 Ch 3 para 47 (UK)

California Consumer Privacy Act no 1798.100 AB-375, 2018 (US)

Personal Data Protection Bill, 2019 (India)

California Privacy Rights Act 2020 which modifies and expands on the California Consumer Privacy Act of 2018.

Draft Online Safety Bill May 2021 available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

Other documents issued by the European Commission

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) final - 2012/0011(COD)

European Communication; Communication from the Commission to the European Parliament, the Council the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World, A European Data Framework for the 21st Century Brussels 25.1.2012 Com (2012) 9 final

Conclusions of European Council Brussels re new EU data protection and cyber security framework-Oct 2013, available at
https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf

Factsheet on the 'Right to be Forgotten' ruling (C 131/12) issued 03-06-2014 http://ec.europa.eu/justice/dataprotection/files/factsheets/factsheet_data_protection_en.pdf

Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines 4 April 2008 00737/EN WP 148

Article 29 Data Protection Working Party, 'Statement of the WP29 on the impact of the development of Big Data on the protection of individuals with regard to the processing of their personal data in the EU', Sept 2014

Article 29 Data Protection Working Party 'Statement on the role of a risk-based approach in data protection legal frameworks' 30 May 2014

Article 29 Data Protection Working Party –'Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, 2014 '

Article 29 Working Party Opinion 01/2016 on the EU –U.S. Privacy Shield draft Adequacy decision

Factsheet, The EU Data Protection Reform and Big Data, Vera Jourova,. Jan 2016 http://ec.europa.eu/justice/data-protection/reform/index_en.htm

Letter from Article 29 Working Party to Redding re Privacy Shield 10 April 2016 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf

Other documents

United Nations Drafting Commission Report (Secretariat Outline) June 1947 available at http://research.un.org/en/undhr/draftingcommittee/1

The Younger Committee's Report (UK) Hansard L Deb, 06 June 1973 vol 343 cc104-78 available at https://api.parliament.uk/historic-hansard/lords/1973/jun/06/privacy-younger-committees-report

Report of the Committee on Data Protection, cmnd 7341 (the Lindop Report) Dec 1978

OECD 1980, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Hansard, House of Lords (UK) 5th series, vol 585, col 436, Jan 1998

The House of Commons (UK), The Right to be forgotten, Standard Note SN/HA/6983 11 Sept 2014

EDPS; Opinion 5/2019 on the Interplay between the ePrivacy Directive & the GDPR in particular regarding the competence, tasks and powers of data protection authorities 12 March 2019 EDPB available at https://edpb.europa.eu/sites /edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

Proposal for 'Right to be Forgotten' Act 2019, see Senate File 2236 available at legis.iowa.gov

Cases

Prince Albert v Strange (1849) 1 Mac & G 25,

Melvin v Read ,1931, 112 Cal. App.285, 297 (US)

Duke of Argyll v Duchess of Argyll HL, 1962 SC (HL) 88)

Pangrazi and Silvetti v Comitato Referendum, Pretura Roma 6-5-1964 (Italy)

Duchess of Argyll v Duke of Argyll [1967] ch 302

Katz v United States 389 U.S. 347 (1967) (US)

Roe v Wade, US Supreme Court (1973) No 70-18 (US)

United States v Miller (1976) 425 US 435 (US)

Nixon v Administrator of General Services 433 US 425 (1977) (US)

Smith v Maryland (1979) 442 US 735 (US)

Population Census Decision, Germany, 15 Dec 1983 BvR 209/83, BVerf G 65 1 (Germany)

Malone v. The United Kingdom - 8691/79 [1984] ECHR 10 (2 August 1984)

Rees v UK, [1986] ECHR Application no. 9532/81

Bowers *v.* Hardwick, U.S. Supreme Court, [1986] 478 U.S. 186. (US)

Leander v Sweden ECHR [1987] 9 EHRR 433, 9248/81

Birindwa & Tshisekedi v Zaire Com No 241/1987 and 242/1987 [1989] Human Rights Committee (United Nations)

Coeriel & Aurik v The Netherlands, Com no 453/1991 [1995] Human Rights Committee (United Nations)

Hurley v Irish American Gay Lesbian and Bisexual Group of Boston, [1995] Case no 515 U.S. at 574 (US)

Jones v New Haven Register, Inc, 46 Conn. Supp 634, 640 A 2d. 1097 1100 [2000] (US)

Rotaru v Romania 28341/95, [2000] ECHR 192, (2000) 8 BHRC 449

Douglas v Hello! [2001] QB 967 2005 EWCA Civ 595 (UK)

R (Pearson) v DVLA [2002]UK EWHC 2482

Case C-101/01 Bodil Lindquist v *Aklagarkammaren i Jonkoping*,[2003] ECLI:EU:C:2003:596

Campbell v MGN [2004] UKHL 22

Chauvy v France (2004) 41 EHRR 610 at 70

Cumpana v Romania (2004) 41 EHRR 200 at 91

Beckham & Another v News Group Newspapers Ltd [2005] EWHC 2252 (QB)

France & Ors v France [2005] 40 EHRR 706

Jameel (Yousef) v Dow Jones& Co Inc [2005] EWCA Civ 75

A v Norway, [2006] ECHR Application no. 28070/06

Bunt v Tilley [2007] 1WLR 1242

Johnson v Medical Defence Union Limited (No. 2) [2007] EWCA Civ 262 Bus LR 503

White v Sweden [2007] EMLR 1 at 21

Mosley v News Group Newspaper [2008] EWHC 1777 (QB)

OBG Ltd v Allen [2007] UKHL 21 [2008] 1AC1

Stacey Synder v Millersville University, et al. United States District Court for the Eastern District of Pennsylvania, [2008] case 2:07-cv-01660-pd (US)

The Times Newspaper Ltd (Nos 1 and 2) v The United Kingdom, ECtHR, [2009] Application nos. 3002/03 and 23676/03; [2009] EMLR 14 s.27

Juzgado de Primera Instancia [1a Inst.] [Court of First Instance], 29/7/2009, Da Cunha, Virginia v Yahoo de Argentina s/ Daños y Perjuicos, (Resulta, I, para. 3) (Arg.)

Metropolitan International Schools Limited (t/a SkillsTrain and/or Train2Game) claimant- and -(1) Designtechnica corporation (t/a digital trends) (2) Google UK Limited (3) Google Inc [2009] EWHC 1765 (QB) [2009] EMLR 27

Case C- 301/06 Ireland v Parliament and Council (10 Feb 2009) ECLI:EU:C:2009:68

Joined cases C-92/09 & C -93/09 Volker and Markus Schecke GbR v Land Hessen 2010 ECR 1 - 11063

M.X v Google & Eric Schmidt, Tribunal de grande instance de Paris 2010 available at http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2985

Terry (previously 'LNS') v Persons Unknown [2010] EWHC 119

AB v Google, Tribunale Ordinario di Milano, 24 March 2011 (Italy)

Ferdinand v MGN [2011] EWHC 2454 (QB)

Karakó v Hungary (2011) 52EHRR 36 [23]

Thornton v Telegraph Media Group Ltd 2011 1 WLR 1985

United States v Jones (2012) 565 US 400 (US)

Case C-457/10P, AstraZeneca AB and AstraZeneca plc v European Commission [2012] ECLI:EU:C:2012:770

C-293/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland, the Attorney General, Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl & Others (2012) (C-594/12) (Joined Cases C-293/12 and C-594/12) OJ C 175, 10.6.2014, p. 6–7

re Southern Pacific Personal Loans Ltd; Oakley Smith and another v Information Commissioner [2013] EWHC 2485 (Ch); [2013] WLR (D) 336

RocknRoll v News Group Newspapers Ltd: [2013] EWHC 24 (Ch)

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

Jameda case, Judgment of the VI. Civil Senate of September 23, 2014 -BGH VI ZR 358/13 – available at https://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=69297&pos=0&anz=1

Zoekresultaat - inzien (document available in Dutch) [2014] :NL:RBAMS:2014:6118

Khoroshenko v Russia, ECtHR, Grand Chamber, Application No. 41418/04, [2015] available at https://hudoc.echr.coe.int/fre#{"itemid":["001-156006"]}

Mosley v Google [2015] EWHC 59 (QB); [2015] 2 C.M.L.R. 22; [2015] E.M.L.R. 11; [2015] F.S.R. 24

Vidal Hall v Gore [2015] 3 W.L.R. 409 [2015] C.P. Rep. 28[2015] 1 C.L.C. 526[2015] 3 C.M.L.R. 2[2015] E.M.L.R. 15[2015] F.S.R. 25

Case 362/14 Maximillian Schrems v Data Protection Commissioner Joined Party, Digital Rights Ireland Ltd [2015] ECLI:EU:C:2015:650 (Schrems 1)

Weller v Associated Newspapers Ltd Court of Appeal (Civil Division) [2015] EWCA Civ 1176;

Google v Judith Vidal-Hall, Robert Haan, Marc Bradshaw [2015] EWCA Civ 311

Olivier G v Le Soir n° C.15.0052.F, [29 April 2016] The Belgian Court of Cassation

PJS v News Group Newspapers Ltd [2016] EWCA Civ 393 [2016] UKSC 26

Olivier G v Le Soir, The Belgian Court of Cassation, [29 April 2016] n° C.15.0052.F, ,

Fürst-Pfeifer v. Austria (Applications nos. 33677/10 and 52340/10) Strasbourg, [Aug 2016]

Google Inc. v. Equustek Solutions Inc. (fka Equustek v. Jacko) Ruling Supreme Court of Canada, (2017) SCC 34

Case C-398/15, Camera di Commercio Industria Artigianato e Agricoltura de Lecce v Salvatore Manni, 9 March 2017, EWHC 119 Para 149 ii

Townsend v Google Inc & Anor, 2017 NIQB 81

Google Inc. v. Equustek Solutions Inc, SCC 34, [2017] 1 SCR 824,

Phil v Sweden, EctHR ,No. 74742/14, February 7, 2017

Vasunathan v The Registrar General, High Court of Karnataka (2017) SCC OnLine Kar 424);

C-18/18, Eva Glawischnig-Piesczek v Facebook, available at https://www.euractiv.com/wp-content/uploads/sites/2/2019/10/CP190128EN.pdf

ABC v Google Inc [2018] EWHC 137 (QB)

ML & WW v Germany [2018] ECHR 554

NTI v Google LLC [2018] EWHC 67 QB

NT1 & NT 2 v Google LLC [2018] EWHC 799 (QB)

Sir Cliff Richard OBE v (1) The British Broadcasting Corporation (2) Chief Constable of South Yorkshire Police [2018] EWHC 1837 (Ch)

Re Mr A, Korkein Hallinto- Oikeus Högsta Förvaltningstomstolen (The Supreme Administrative Court of Finland) 2018: ECLI:FI:KHO:2018:112 available at

https://www.kho.fi/fi/index/paatoksia/vuosikirjapaatokset/vuosikirjapaatos/1534308651626.html

Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, [2018] ECLI:EU:C:2020:559

Savage v Data Protection Commissioner & anor [2018] IEHC 122

C-136/17, GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL), interveners: Premier ministre, Google LLC, successor to Google Inc. 2019] ECLI EU:C:2019:773

Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) [2019] ECLI EU:C:2019:772

BVerfG, Order of the First Senate of 6 November 2019 - 1 BvR 16/13 -, paras. 1-157,ECLI:DE:BVerfG:2019:rs20191106.1bvr001613

Zulfiqar Ahman Khan vs. Quintillion Business Media Pvt. Ltd. and Ors (2019) 175 DRJ 660.

HRH the Duchess of Sussex v Associated Newspapers Ltd. [2021] EWHC 273 (ch)

Opinions of the Advocate General

Case C -131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, [2013] ECLI: EU:C:2014:317, Opinion of Advocate General Jääskinen

Case C-136/17 GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL), [2019] ECLI:EU:C:2019:14 Opinion of Advocate General Szpunar

Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), [2019] ECLI:EU:C:2019:15, Opinion of Advocate General Szpunar

SECONDARY SOURCES

Books

Adams J T, *The Epic of America,* (Boston Little Brown and Co. 1931)

Adams J & Haden D., *Social Effects of Computer Use and Misuse* (Wiley 1976)

Agre P E, Rotenberg M, (eds) *Technology and Privacy- The new landscape,* (Cambridge MIT Press 1997)

Alston P, Goodman R, *International Human Rights* (OUP 2013)

Andrade N N G de, *Right to personal Identity: The Challenges of Ambient Intelligence and the need for a new Legal Conceptualization*, in (eds), Serge Gutwirth, Yves Poullet, Paul De Hert, Ronald Leenes *Computers, Privacy and Data Protection an Element of Choice*, (Springer 2011)

Ausloos J, *The Right to Erasure in EU Data Protection Law*, (OUP 2020)

Baldwin T, *Alt Control Delete: How Politics and Media crashed our democracy*, (C Hurst and Co 2018)

Bentham J, *Utilitarianism*, 1789 re published by Broadview Press (2000)

Bernal P, *Internet Privacy Rights –Rights to Protect Automony,* (CUP 2014.

Bernal P, '*Privacy, autonomy and the internet*'. in *Internet Privacy Rights: Rights to Protect Autonomy (*Cambridge Intellectual Property and Information Law 2014), pp. 24-52)

Blackstone W, *Commentaries on the Laws of England,* Vol 4 (originally published by the Clarendon Press 1765–1770.) available at https://avalon.law.yale.edu/subject_menus/blackstone.asp

Blanchette J-F, *The noise in the Archive: Oblivion in the Age of Total Recall,* in Gutwirth S, Poullet Y, De Hert P, Leenes R, (eds) *Computers, Privacy and Data Protection: an Element of Choice* (Springer 2010)

Giovanni Bognetti, 'The Concept of Human Dignity in European and U.S. Constitutionalism', in G. Nolte (ed.), European and US Constitutionalism, Science and Technique of Democracy No. 37 (2005), at 75, 79.

Brock G, *The right to be forgotten- Privacy and Media in the Digital Age*, (IB Tauris 2016)

Brkan M, Psychogiopoulou E, (eds) *Courts, Privacy and Data Protection in the Digital Environment* (Edward Elgar Publishing 2017).

Brownsword R, *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality* in (eds) Gutwirth S, Poullet Y, De Hert P, de Terwangne C, Nouwt S. *Reinventing Data Protection?* (Springer, 2009).

Bygrave LA, *Data Privacy Law; An International Perspective*, (OUP 2014)

Bygrave LA , *Data Privacy Law and the Internet: Policy Challenges* in (eds) Norman Witzleb, David Lindsay, Moira Paterson, & Sharon Rodrick. *Emerging Challenges in Privacy Law: Comparative Perspectives*. (CUP 2014) Ch 12, 259-289

Carpanelli E, Lazzerini N (eds) *Use and Misuse of New Technologies Contemporary Challenges in International and European Law* (Springer 2018)

Casanas, A E, *The Constitutional Court of Spain: From system balancer to polarizing centralist.* In Aroney N, Kinkaid J, (eds) *Courts in Federal Countries: Federalists or Unitarists?* (University of Toronto Press. 2017)

Castells M, *The power of identity*, (Wiley-Blackwell 2nd ed 2010)

Cheer U, *Divining the Dignity Torts*, in (ed) Andrew Kenyon, *Comparative Defamation and Privacy Law*. (CUP 2018)

Clapham A, *Human Rights: A Very Short Introduction,* (Very Short Introductions: OUP; 2nd edn 2015)

Cofone I N, (ed) *The Right to be Forgotten; A Canadian and comparative Perspective*, (Routledge Focus, 2020)

Colvin M (ed) *Developing Key Privacy Rights* (Hart Publishing, 2002)

Cruft R, Liao S M & Renzo M, eds., *Philosophical Foundations of Human Rights,* (OUP, 2015)

De Hert P , Gutwirth S – *Data Protection in the case law of Strasbourg and Luxembourg; Constitutionalism in practice* -in (eds) Gutwirth S, Poullet Y, De Hert P, de Terwangne C, Nouwt S, *Reinventing Data Protection, (*Springer 2009)

De Zwart M, *Privacy for the weak transparency for the powerful* , in Kenyon AT (ed) *Comparative Defamation and Privacy Law*, (CUP 2016)

Donelly J, *Universal Human Rights in Theory and Practice,* (Cornell University Press 3ed. 2013)

Ezrachi A, Stucke M. E, *Virtual Competition; The promise and Perils of the Algorithm- Driven Economy*, (First Harvard University Press 2019)

Foucault M. *Discipline & Punish Panopticism III: The Birth of the Prison* 1975 (NY: Vintage Books 1995)

Gewirth A, '*Are there any Absolute Rights*?' in Waldron J *(*ed*), Theories of Right* (OUP 1984)*,*

González Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. (Springer, 2014)

Griffin J, *On Human Rights,* OUP, reprinted 2013

Ghezzi A, Pereira AG, Vesnic-Alujevic L, (eds) *The ethics of memory in a digital age, interrogating the right to be forgotten,* (Palgrave MacMillan 2014)

Gunnarsson L, Mürbe, U*,* Weiss N, (eds) *The Human Right to a Dignified Existence in an International Context -legal and Philosophical Perspectives* (Hart Publishing 2019)

Gutwirth, S, *Privacy and the Information Age* (Rowmans & Littlefield Publishers, 2002)

Gutwirth S, Poullet Y, De Hert, (eds) *Data Protection in a Profiled World,(* Springer 2010)

Gutwirth S, Poullet Y, De Hert P, Leenes R, (eds) *Computers, Privacy and Data Protection: an Element of Choice* (Springer 2011)

Gutwirth S, Leenes R, De Hert P, (eds) *Reforming European Data Protection Law*, (Springer 2015)

Gutwirth S, De Hert P, Leenes R, (eds) *Reloading Data Protection Multidisciplinary Insights and Contemporary Challenges*, (Springer 2014)

Gutwirth S, Poullet Y, De Hert P, de Terwangne C, Nouwt S, (eds) *Reinventing Data Protection, (*Springer 2009)

Gutwirth S, *Privacy and the Information Age*, (Rowmans & Littlefield Publishers, 2002)

Haga Y, *Right to be Forgotten: A New Privacy Right in the Era of Internet,* in Corrales M, Fenwick M, Forgo N (eds) *New Technology Big Data and the Law* (Springer Publishing 2017)

Henkin L, *The Age of Rights*, (Columbia University Press 1990)

Hobbes T, *"Leviathan; or the Matter, Form, and Power of a Commonwealth, Ecclesiastical and Civil,"* (1651)

Holvast J, *The History of Privacy*, (Springer 2008)

Hunt L, *Inventing Human Rights, (*WW Norton & Co. 2007)

Ishay M, *The History of Human Rights,* (University of California Press, 2nd ed 2008)

Jones M Leta, *Ctrl +Z; The Right to be Forgotten*, (New York University Press 2016)

Kalin W, Kunzli J, *The Law of International Human Rights Protection* (2nd ed OUP 2019)

Keown D, *Are There Human Rights in Buddhism*, in (eds) D Prebish, C Husted, *Buddhism and Human Rights,* (Curzon Press London 1998)

Kenyon A T, (ed) *Comparative Defamation and Privacy Law* (CUP 2016)

Klang M, Murray A, (eds) *Human Rights in the Digital Age*, (The Glasshouse Press 2005)

Lane J, Stodden V, Bender S, Nissenbaum H, (eds) *Privacy, Big Data and the Public Good Frameworks for Engagement* (CUP 2014)

Leenes R, van Brakel R, Gutwirth S, l De Hert P, (eds) *Data Protection and Privacy: (In)visibilities and Infrastructure* (Springer 2017)

Levmore S, Nussbaum, M C (eds) '*The Offensive Internet- Speech Privacy and Reputation* (Harvard University Press 2010)

Lindsay D F, '*The 'right to be forgotten' by search engines under data privacy law: A legal and policy analysis of the Costeja decision'* in A. T. Kenyon (ed), *Comparative Defamation and Privacy Law* (Cambridge Intellectual Property and Information Law, CUP 2016).

Locke J, *The Second Treatise of Government* ,1690 (reprinted New York MacMillan 1986)

Lynskey O, *The Foundations of EU Data Protection Law*, (OUP 2015)

McNamara L, *Reputation and Defamation*, (OUP2007)

Markou C, *The Right to be Forgotten' : Ten Reasons why it should be forgotten*, in Serge Gutwirth, Ronald Leenes, Paul de Hert , (eds) *Reforming European Data Protection Law*: (Springer 2015)

Marsden C C, *Net Neutrality: Towards a Co Regulatory Solution*, (Bloomsbury Academic 2010)

Marx K, *On the Jewish Question*, in *Deutsch-Französische Jahrbücher,* (1844)

Mayer-Schönberger V, '*delete' The Virtue of Forgetting in the Digital Age,* (Princeton University Press 2009)

Mendel T. et al (eds) *Global Survey on Internet Privacy and Freedom of Expression* (Unesco Series on Internet Freedom) (UNESCO Publishing 2012)

Meyer-Schönberger V, Cukier K, *Big Data*, (John Murray Publishers 2013)

Miglio A, *Enforcing the Right to Be Forgotten beyond EU Borders, Use and Misuse of New Technologies*, in Carpanelli E, Lazzerini N (eds*) Contemporary Challenges in International and European Law*, (Springer 2019)

Moeckli D, Shah S, Sivakumaran S, *International Human Rights Law* (OUP 2010)

Mowbray A, *Cases, Materials and Commentary on the European Convention on Human Rights* (3rd ed OUP 2012)

Murray A, *Information Technology Law* (2nd ed. OUP 2013)
Murray A, *Information Technology Law*; *The Law and Society* (3rd ed OUP 2016)
Murray A, *Information Technology Law* (4nd Ed OUP)

Newton M T, Donaghy P J, *Institutions of modern Spain: a political and economic guide.* (CUP. 1997)

Nissenbaum H, *Privacy in Context: Technology, Policy and the integrity of Social Life,* (Stanford University Press 2009)

O'Callaghan P, *'The Right to Be Forgotten in Ireland*' in F. Werro (ed) *The Right to be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas and Asia* (Springer 2018),

Orwell G, '*1984*' , (Originally published by Secker & Warburg 1949, reprinted Penguin Modern Classics 2008)

Othman N, *Grounding Human Rights Arguments in Non Western Culture sharia and the citizenship and rights of women in a modern Islamic state,* in (eds) Joanne R Bauer, Daniel A Bell, *East Asian Challenge for Human Rights*, (CUP 1999)

Paine T, *Rights of Man,* 1791, (new ed Penguin Classics 1984)

Pino G, *The Right to Personal Identity*, in Van Hoeke M, Ost F (eds) *Italian Private Law, Constitutional Interpretation and Judge Made Laws, The Harmonization of Private Law in Europe* (Oxford, Hart Publishing 2000)

Rallo A, *The Right to be Forgotten on the Internet: Google v Spain, (* Electronic Privacy Information Center, 2018)

Raz J, *Morality of Freedom*, (Clarendon Press 1986)

Rousseau J J, *The Social Contract or Principles of Political Right*, 1791 (translated with intro by GD H Cole, JM Dents & Sons available at https://oll.libertyfund.org/title/cole-thesocial-ccontract-and-discourses)

Sheeran S, Rodley N, (eds) *Routledge Handbook of International Human Rights Law*, (Routledge 2013)

Rouvroy A, Poulet, Y, *The Right to Information Self determination and the value of self-development , Reassessing the importance of privacy for democracy*, in Serge Gutwirth et al (eds) *Reinventing Data Protection (*Springer 2009)

Sen A, *The Development of Freedom,* (OUP 1999)

Solove D J, *A Brief History of Information Privacy Law* in (ed) Mathews K J, *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, (PLI 2006)

Solove D.J, *Nothing to Hide: the false tradeoff between privacy and securit*y, (Yale University Press 2011)

Solove D.J, *Speech, Privacy and Reputation on the Internet*, in Levmore S, Nussbaum M. C (eds) *The Offensive Internet* (Harvard University Press 2010)

Solove DJ, *The Future of Reputation: gossip, rumor, and privacy on the Internet* (Yale University Press 2007)

Solove D.J , *Understanding Privacy*, (Harvard University Press, 2018)

Stucke M E, Grunes A P, *Big Data and Competition Policy*, (OUP 2016)

Tzanov M, *The Fundamental Right to Data Protection*, (Hart Publishing 2019)

Vermeulen G, *The Paper Shield - on the degree of protection of the EU-US Privacy Shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement agencies* in (eds) Berker D, Sventesson J, Kloza D, *Transatlantic Data Privacy Relationships as a Challenge for Democracy* (Intersentia 2016)

Volio F, *Legal personality, privacy and the family* in Henkin L (ed) *The International Bill of Rights,* (Columbia University Press, 1981)

Voss G, Woodcock K H, *Navigating EU Privacy and Data Protection Laws* (American Bar Association 2016)

Waller D, Younger R, *The Reputation Game, The art of changing how people see you*, (OneWorld Publications 2017)

Waldron J, *Is Dignity the Foundation of Human Rights?* in (eds) Cruft R, Liao, S. M Massimo Renzo, *Philosophical Foundations of Human Rights* (OUP 2015)

Westin A, *Freedom and Privacy*, (Atheneum, 1967)

Witzleb N, Lindsay D, Patterson M & Rodrick S, '*Emerging Challenges of Privacy Law, Comparative Perspectives*' (eds) (CUP 2014)

Articles

Abril P S, Lipton J D. 'The Right to be Forgotten: Who Decides What the World Forgets?' (2014) Kentucky Law Journal: Vol. 103, Iss. 3, Article 4 available at: https://uknowledge.uky.edu/klj/vol103/iss3/4

Adams A, Murata J, Orito Y, 'The Development of Japanese Data Protection,' (2010) Meiji University Policy and Internet , Vol 2 Iss 2 Art 5 available at www.psocommons.org/policyandinternet

Abril P S, Moreno E P, 'Lux In Arcana: Decoding the Right to be Forgotten in Digital Archives,' (2016) MDPI, Open Access Journal, vol. 5(3), available at www.mdpi.com/journal/laws

Abril P S, Moreno E P, Adam, J, Contemporary Practical Alternatives to a 'Right To Be Forgotten' in the United States [2019] Latin American Law Review no 02 23-60, available at https://doi.org/10.29263/lar02.2019.02

Ambrose M Leta, Ausloos J, ' The Right to be Forgotten across the pond' [2013] Journal of Information Policy, 3 1-23

Apa E , Pollicino O, Modelling the LIiability of Internet Service Providers: Google v Vivi Down (Egea 2013)

Aplin T, 'The Development of the Action for Breach of Confidence in a Post-HRA Era' (2007). Intellectual Property Quarterly, Vol. 1, p. 19 - 59, 2007. Available at SSRN: https://ssrn.com/abstract=2437014

Aplin T F, Bosland J J, 'The Uncertain Landscape of Article 8 of the ECHR: The Protection of Reputation as a Fundamental Human Right?' in (ed) A. Kenyon, Comparative Defamation and Privacy Law (CUP, 2016), ch 13.

Aplin T F & Mohamed S (2019) 'The concept of "reputation" in the moral right of Integrity,' Journal of Intellectual Property Law and Practice, 14 (4), 268-277

Ausloos J, 'The Right to be forgotten - Worth Remembering?' (2012) Computer Law and Security review, vol 28, p. 147.

Austin L M, 'Privacy and the Question of Technology', [2003] Law & Philosophy 22: 119-166

Barendt E, 'What is the point of libel law *?*' (1999) Current Legal Problems, Vol 52, Issue 1, Pages 110–125,

Barendt E, 'Balancing Freedom of Expression and Privacy: The Jurisprudence of the Strasbourg Court,' [2009] Journal of Media Law, 1:1, 49-72,

Bergkamp L, 'The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy' [2002] Computer Law and Security Report 18(1)

Berman S P, 'GDPR in the US : Be careful what you wish for,' [2018] Government Technology, available at http://www.govtech.com/analysis/GDPR-in -the- US-Be careful= What- You – wish for.html

Bernal PA, 'A right to Delete', (2011) European Journal of Law and Technology Vol 2 Iss 2 p 2

Blackman J, 'Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image over the Internet', [2009] 49 Santa Clara L Rev 31

Blanke J M, 'Privacy and Outrage' (2018) 9 Case W. Res. J.L. Tech. & Internet [1] (3rd)

Boban M, 'Digital Single Market and EU Data Protection Reform with regard to the processing of personal data as the challenge to the modern world', [2016] Proceedings of 16th International Scientific Conference ESD: The legal challenges of modern world 1-2 , 191-201 University of Split, Croatia; available at https://www.bib.irb.hr/904724

Boizard M, 'The right to respect for private life: an effective tool in the right to be forgotten?' (2015) 1 Montesquieu Law Review issue 2,

Bolton III R. L, 'The Right to Be Forgotten: Forced Amnesia in a Technological Age' [2014,] John Marshall Journal of Computer & Information Law,

Bond R, 'Data Ownership in social networks – a very personal thing', (2010) Privacy and Data Protection, Vol 11/Issue 1,

Borgesius F J Z**,** Steenbruggen Dr W, 'The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust Laws of confidentiality exercised in Europe'**,** (2019**)** Theoretical Inquiries in Law**,** Vol 20: Iss 1

Bougiakiotis E, 'The Enforcement of the Google Spain ruling'. [2016] International Journal of Law and Information Technology, 0,1-32

Boyd D, 'The Future of Privacy: how privacy norms can inform regulation'. [2010] 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem, 29 October 2010 available at ;
http://www.danah.org/papers/talks/2010/PrivacyGenerations.html

Brkan M, 'Data Protection and Conflicts of Laws, A challenging relationship' [2016] European Data Protection Law Review, 2(3), 324-341.

Brown C,'Universal human rights: a critique', 1997 Int Journal of Human Rights Vol 1 Iss 2 pp 41-65

Bunn A, 'The curious case of the right to be forgotten', (2015) Computer Law and Security Review Vol 31, Iss 3, Pages 336-350

Buttarelli G, 'Privacy Matters: updating human rights for the digital society' [2017] Health Technol. 7: 325-328

Buttarelli G, 'Strange Bedfollows: Data Protection, Privacy and Competition', [2017] The Computer & Internet Lawyer, Vol 34 No 12

Byrum K, 'The European right to be forgotten: A challenge to the United States Constitution's First Amendment and to professional public relations ethics'. [2016] Public Relations Review available at http://dx.doi.org/10.1016/j.pubrev.2016.10.01

Carter E L, 'Argentina's Right To Be Forgotten', (2013) Emory International Law Review Vol 27

Castellano, P S, 'The Right to be Forgotten under European Law, a Constitutional Debate', (2012) Lex Electronica, Vol 16.1 4

Chenou J-M, Radu R, 'The 'Right to Be Forgotten': Negotiating Public and Private Ordering in the European Union, (2017), Business & Society vol 58 issue 1, pp 74-102

Corda A, Lageson S E, 'Disordered Punishment: Workaround Technologies of Criminal Records Disclosure and the Rise of a New Penal Entrepreneurialism' (2019) British Journal of Criminology,

Cohen J E, 'Turning Privacy Inside Out' (2018) Theoretical Inquiries in Law, 20.1 available at SSRN: https://ssrn.com/abstract=3162178

Cofone I, ‘Google v Spain: A Right to be Forgotten’ (2015). Chicago-Kent Journal of International and Comparative Law, Vol. 15, No. 1, 2015,

Cunha, M V de Azevedo, Marin L, Sarto G, ‘Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web’ (2012) International Data Privacy Law Vol 2 iss 2

Davola A, Stracqualursi E, ‘Eclipsing the Web: Online Data Protection and Liability of Search Engines in the Google Spain Case’, [2015] 23 Dig.: Nat'l Italian Am. B. Ass'n L.J. 65

Determann L, ‘Adequacy of Data Protection in the USA: myths and facts’ (2016) International Data Privacy Law Advance, Vol 6 Iss 3 p244-250

Diggelmann O, Cleis MN, ‘How the Right to Privacy Became a Human Right’, [2014] Human Rights Law Review 14, pp 441-458

Dixon T, ‘Valuing Privacy: An overview and Introduction’, [2001] UNSW LawJl 1; 24(1) p

Docksey C, ‘Four Fundamental Rights: finding the balance’, (2016) International Data Privacy Law; Oxford Vol. 6, Iss. 3, pp 195 - 209.

Donnelly J, ‘Human Rights and Human Dignity: An Analytic Critique of Non-Western Conceptions of Human Rights’, (1982) The American Political Science Review Vol 76 No 2 p 303-316,

Edwards L, Veale, M, ‘Slave to the Algorithm? Why a ‘Right to Explanation is Probably not the Remedy You Are Looking for’ [2017] 16 Duke L & Tech Rev., 80 pp 18-81

Erdos D, ‘EU Internet Enforcement after Google Spain, Report of Proceedings’ [2015] Centre for European Legal Studies Faculty of Law Conference, Session 3 University of Cambridge, available at;

https://www.cels.law.cam.ac.uk/sites/www.law.cam.ac.uk/files/images/www.cels.law.cam.ac.uk/documents/google_spain_conference_report_-_16.12.2015.pdf

Fazlioglu M, 'Forget me not, the clash of the right to be forgotten and freedom of expression on the Internet', (2013) International Data Privacy Law, Vol 3, Iss 3, pp 149–157

Foster S, 'Balancing Sexual Privacy with the Public Right to know: The decision in Moseley v MGM', [2008] Criminal Law and Justice Weekly 172 JPN p 627

Fried C, 'Privacy', [1968] Yale LJ p475 available at http://www.jstor.org/stable/pdf/794941.pdf?refreqid=search%3Aa8f896894d0271a6c5f713b3148c1804

Frosio G F, 'The Right to be forgotten: much ado about nothing'. (2017) Colo Tech LJ vol 15.2 pp 307-315

Garstka K K, Erdos D, 'Hiding in Plain Sight? The 'Right to Be Forgotten' and Search Engines in the Context of International Data Protection Frameworks' (2017) available at SSRN: https://ssrn.com/abstract=3043870

Gidron T, Volovelsky U, The Right to be Forgotten: The Israeli Version, [2018] Computer Law & Security Review 34 pp 824-829

Goffman E, 'The presentation of self in everyday Life' [1959] Edinburgh University Social Sciences Research Centre accessed at; https://monoskop.org/images/1/19/Goffman_Erving_The_Presentation_of_Self_in_Everyday_Life.pdf

Graef I, Clifford D, Valcke P, 'Fairness and enforcement: bridging competition, data protection and consumer law', (2018) International Data Privacy Law, , Vol 8, No 3 p 200-223

Grafanaki S, 'Autonomy Challenges in the Age of Big Data', [2017] 27 Fordham Intell. Prop. Media & Ent. L. J. 803

Graham C, 'Data Protection Reforms must target crooks not business', The Register 6 Feb 2013

Graux H, Ausloos J, Valcke P, 'The Right to be Forgotten in the Internet Era' [2012]. ICRI Research Paper No. 11. Available at SSRN: https://ssrn.com/abstract=2174896

Grest L , Surguy M, 'Bexit Brainstorming; data privacy'. [2015] 166 NLJ 7702, p17

Grinffiel J A , 'Don't Shoot the Messenger: Civil Liability for ISPs after Virginia da Cunha v Yahoo – Argentina & Google Inc' [2011] 17 Law & Business Review Am 111

Grunes A P, 'Another Look at Privacy' [2013] 20 Geo Mason L Rev p 1107,

Gumbis, Jaunius; Randakeviciute, Jurgita; Bacianskaite, Vytaute Do Human Rights Guarantee Autonomy? 2008 Cuadernos constitucionales de la Cátedra Fadrique Furió Ceriol, ISSN 1135-0679, Nº 62-63, 2008, pp 77-93

Habermas J, 'The concept of Human Dignity and the Realistic Utopia of Human Right, The crisis of the European Union: A Response', (2010) Wiley online, Metaphilospohy Vol 41 Iss 4, July 2010 pp 464-480

Hargreaves S, 'The Trouble with using Search Engines as a Primary Vector of Exercising the Right to be Forgotten', [2016] Pandora's Box 83-106
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2873391

Henkin L, 'Privacy and Autonomy', [1974] Columbia Law Review 1410

Hoffinan D, Bruening P, Carter S, 'The right to obscurity: how we can implement the Google Spain decision ?' (2016) North Carolina Journal of Law & Technology, vol 17, iss 3: March 2016

Hörnle J, 'Google's Algorithms, Search Results and Relevancy under Data Protection Law: Whose Data Quality*?*' [2014] 25 (6) Entertainment Law Journal p 209;

Houser K A., Voss W G, 'GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy*?*' [2018] 25 Rich. J.L. & Tech. no. 1

Iglezakis I, 'The Right to Be Forgotten in the Google Spain Case (Case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet?', [2014] available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472323

Jacobs J.B, Larrauri E, 'Are Criminal Convictions a Public Matter? The USA and Spain' (2012) 14(1) Punishment & Society 3.

Kahn J D, 'What's in a Name? Law's Identity Under the Tort of Appropriation' (2001). Temple Law Review, Vol. 74, p. 263

Käll JA, 'Posthumann Data Subject ? The Right to be Forgotten and Beyond,' (2017) German Law Journal Vol 18 no 05 pp 1145-1162

Karapapa S, Borghi M, 'Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm' [2015] Int J Law Info Tech 23 (3): pp 261-289

Keele B J, 'Privacy by deletion; the need for a global data deletion principal' (2009) Indiana Journal of Global Legal Studies 16-1, pp 363- 384

Kelly M J , Satola D, 'The Right to Be Forgotten' (2017) University of Illinois Law Review, 2017 Vol. 1, available at SSRN: https://ssrn.com/abstract=2965685

Kirkup A, Evans T, 'The Myth of Western Opposition to Economic, Social and Cultural Rights A Reply to Whelan and Donnelly' [2009] HRQ 31 221-238 The John Hopkins University Press

Koops B-J, 'Forgetting Footprints, Shunning Shadows; A critical Analysis of the Right to be Forgotten in Big Data Practice', [2012] Tilburg Law School Legal Studies Research Paper series No 8/2012

Koops B-J, 'On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy'. [2014] Politica e Società 3: 247–264.

Koops B-J, 'The Trouble with European Data Protection Law', [2014] International Data Privacy Law 4(4):250-261

Koops B-J, Clayton Newell B, Timan T, Škorvánek I, Chokrevski T, Galic Mˇ. 'A Typology of Privacy.' [2017] University of Pennsylvania Journal of International Law 38: 483–575.

Korenhof P, 'Timing the Right to Be Forgotten: A Study into 'Time' as a Factor in Deciding About Retention or Erasure of Data', [2014] available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436436

Kulesza J, 'Freedom of Information in the Global Information Society: The Question of the Internet Bill of Rights' (2008) University of Warmia and Mazury in Olsztyn Law Review, Vol. 1, pp. 81-95, available at SSRN: https://ssrn.com/abstract=1446771

Kulk S, Borgesius Zuiderveen FJ, 'Freedom of Expression and Right to Be Forgotten Cases in the Netherlands after Google Spain', [2015] EDPL 15 -2 p 113

Kuner C, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law' [2012] Bloomsberg BNA Privacy and Security Law Report, Feb 2012, pp1-15

Kuzma J, ‘Empirical Study of Privacy Issues among Social Networking Sites’ [2011] Journal of International Commercial Law & Technology 6(2), pp.74-84

Lai A, ‘The Right to be Forgotten and What the Laws Should/Can/Will be : Comparing the United States and Canada’, [2017] Global Journal of Comparative Law 6 77-104 available at brill.com/gjcl

Laidlaw E, ‘Private Powers, Public Interest: An examination into search engine accountability’, (2009) International Journal of Law and Information Technology Vol. 17, Issue 1, pp 113-145

Lavelle J J, ‘Search Query: Can America Accept a Right to Be Forgotten as a Publicity Right?’ [2018] 83 Brook.L.Rev Iss 3

Lee J ‘SB 568*:* Does California’s Online Eraser Button Protect the Privacy of Minors’, (2015) UC Davis Law Review, vol 48, 1173-1205,

Levin A & Abril P S, ‘Two Notions of Privacy Online’ [2009.] Vanderbilt Journal of Entertainment & Technology Law, 11(4), pp.1001–1051.

Lindsay D, ‘The 'Right to be Forgotten' by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling’ [2014] Journal of Media Law 6(2) pp 159-179

Loh A, ‘Google v. Equustek: United States Federal Court Declares Canadian Court Order Unenforceable’, [2017] Jolt Digest, available at https://jolt.law.harvard.edu/digest/google-v-equustek-united-states-federal-court-declares-canadian- court-order-unenforceable.

Lynskey O, ‘Time to Forget the “Right to be Forgotten”?, Advocate General Jãaskinen’s Opinion in C-131/12 Google Spain v AEPD’, European Law Blog, 13 July 2013

Lynskey O, ‘Deconstructing Data Protection: the added-value of a right to data protection in the EU legal order’ [2014] The International and Comparative Law Quarterly; Oxford 63. (3) pp 569-597

Lynskey O, ‘Control over Personal Data in a Digital Age: Google Spain V AEPD and Mario Costeja Gonzalez’ [2015] 78 (3) MLR 522 -548

Lynskey O, ‘Grappling with “Data Power” Normative Nudges from Data Protection and Privacy’, [2019] 20 Theoretical Inquires L 189

Lynskey O, ‘Delivering Data Protection: The Next Chapter’, [2020] German Law Journal 21 pp 80-84

Lytras C, ‘Right to be Forgotten: Europe's Cutting Edge Weapon to fight Google?’ (2015) European Public Law: EU eJournal Vol 12, Issue 106, available at SSRN: https://ssrn.com/abstract=2668479

McNealy J E, The Emerging Conflict between Newsworthiness and the Right to Be Forgotten (2012). Northern Kentucky Law Review, Vol. 39, No. 2, 119-135

Mantelero A, ‘The EU Proposal for a General Data Protection Regulation and the roots of the right to be forgotten’, [2013] Computer Law & Security Review 29 no 3 para 1-3.

Marshall P, ‘European Courts set Privacy Standards’, [2016] Technology and Business Ethics, available at http:// business researcher.sagepub.com/sbr-1775-98200-2717800/20160215/short-article-european-courts-set-privacy-standards

Mai J-E, ‘Big Data privacy: the datafication of personal information’, [2016] The Information Society 32(3) pp 192-199

Martin K, ‘Diminished or Just Different? A factorial vignette study of privacy as a social contract’. (2012) Journal of Business Ethics, 111(4), pp.519–539.

McNealy J E, ‘The Emerging Conflict between Newsworthiness and the Right to be Forgotten’, (2012) Northern Kentucky Law Review Vol 39.2 pp 119-135

McIntyre T J, O’Donnell I, ‘Criminals, Data Protection and the Right to a Second Chance’ (2017) 58 Irish Jurist (ns) 27

McGoldrick D, ‘Developments in the Right to be Forgotten’ [2013] Human Rights Law Review 13(4), pp 761-776.

Meijer S, ‘Rehabilitation as a Positive Obligation’, (2017) European Journal of Crime, Criminal Law and Criminal Justice, Vol 25, Iss 2

Miglio A, ‘Setting Borders to Forgetfulness: AG Suggests limiting the Scope of the Search Engine Operators’ Obligations to Dereference Personal Data’, [2019] EDPL Case Notes 1/2019

Mo Jojo Y C ,‘Privacy and Publicly Available Information –an analysis of the Common Law and Statuary Protection in Hong Kong’ Statute Law Review (2019) Vol 40, Iss 2, pp 188–205,

Moreham N A ‘Unpacking the reasonable expectation of privacy test’, LQR 2018 651

Neville A, ‘Is it a human right to be forgotten?, Conceptualising the World view’, Santa Clara Journal of Int Law [2017] vol 15 Iss 2 p 157- 172

Nissenbaum, H, ‘Protecting Privacy in Public, The problem of Privacy in the Information Age’ (1998) 17 Law and Philosophy, p 559

O'Hara K, ‘The right to be forgotten: The good, the bad, and the ugly’, [2015] IEEE Internet Computing 19(4) 73-79

O'Hara K, Shadbolt N, Hull W, 'A Pragmatic Approach to the Right to be Forgotten', [2016] Global Commission on Internet Governance, Paper Series No 26

Pettrachin A, 'Towards a universal declaration on internet rights and freedoms?' [2018] The International Communications Gazette, 0 1-17

Pollicino O, De Gregorio G, 'Privacy or Transparency? A new Balancing of Interests for the 'Right to be Forgotten' of Personal Data Published in Public Registers', [2017] The Italian Law Journal vol.03-no 02

Pound R, 'Interests of Personality' (1915) 28 Harvard Law Review 343 p47

Powles J, 'The case that won't be forgotten' (2015) 47 Loyola University of Chicago Law Journal, p 583 available at;
http://luc.edu/media/lucedu/law/students/publications/llj/pdfs/vol47/issue2/Powles.pdf

Rauhofer J, 'Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle', [2015] EDPL 1/2015

Raz J, 'Human Rights Without Foundations', (2007). Oxford Legal Studies Research Paper No. 14/2007, Available at SSRN: https://ssrn.com/abstract=999874

Redecker D, Gill L, Gasser U, 'Towards digital constitutionalism ? Mapping attempts to craft an Internet Bill of Rights,' [2018] The International Communication Gazette 2018 0 1-18

Revina SN, Zaharov AL 'The Transformation of Human Rights in the Information Society Connected with the Foundation of the Right to be Forgotten by the European Court of Justice' (2015) Mediterranean Journal of Social Sciences Vol 6 No 6 supplement 3

Robertson V H.S.E, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data' (2019). Available at SSRN: https://ssrn.com/abstract=3408971

Riccardi J Lee, 'The German Federal Data Protection Act of 1977: Protecting the Right to Privacy', [1983] B.C.Int'l & Comp. L. Rev. 243 available at http://lawdigitalcommons.bc.edu/iclr/vol6/iss1/8

Rengger, N (2011), 'The World Turned Upside Down? Human Rights and International Relations after 25 Years', International Affairs, Vol. 87, No 5, pp 1159–1178

Rosen J, 'Symposium Issue; The Right To Be Forgotten' (2012) 64 Stanford Law Review Online Vol. 64 p 88 available at: https://review.law.stanford.edu/wp-content/uploads/sites/3/2012/02/64-SLRO-88.pdf

Rouvroy A, '*Reinventer L'art d'oublier et de se Faire Oublier dans la Societe de l'information*' Version Augmentee (2008) (ed) Lacour S, L'Harmattan, 249-278. Available at: http://1libertaire.free.fr/ARouvroy03.html

Sator G, 'The right to be forgotten: balancing interests in the flux of time', [2016] International Journal of Law & Information Technology 24 (1) pp72-98

Schoor E Adams, 'Narrowing the Rights to be Forgotten: Why the European Union needs to amend the proposed Data Protection Legislation', [2014] 39 Brook Journal of International Law

Schweda S, 'European Parliament's Legal Service Presents Opinion on **CJEU** Data Retention Ruling, as Commission Discusses Next Steps' , (2015), EDPL Review Vol 1 Iss 1 Pp 52 - 54

Silvestre GF, Borges CB, Benevides NS, 'The Procedural Protection of Data De-indexing in Internet Search Engines: The Effectiveness in Brazil of the So called Right to be Forgotten against media companies', (2019) Revista Juridica Vol 01No 54 Curitiba pp 25-50

Smart U, 'The three Rs: remorse, rehabilitation, right to be forgotten: how de-listing is left up to the courts in NT1 & NT2 and AR V Chief Constable of Greater Manchester' [2017], 40 E.I.P.R. 2018, pp. 804-811

Solove DJ, Hartzog W, 'The FTC and the New Common Law of Privacy'. [2014] Columbia Law Review 114(3) pp.583–676.

Solove DJ, 'The Origins and Growth of Information' (2003) Privacy Law PLI/PAT, Vol. 748, p. 29, available at SSRN: https://ssrn.com/abstract=445181

Spahiu I, 'Between the right to know and the right to forget: looking beyond the Google case,' (2015) EJLT Vol 6, No 2,

Spoor E, 'Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation', (2014) Brooklyn Journal of International Law, Vol. 39, No. 1,

Stamatopoulo E, 'Cultural Rights in International Law' (2007) EJIL Vol 21 Iss 4 pp 1111-1115

Sterling G, 'Report: 2 years in, 75% Percent of Right to be Forgotten Asks Denied by Google'. [2016] Search Engine Land, available at https://searchengineland.com/report-2-years-75-percent-right-forgotten-asks-denied-google-249424

Stucke M E, 'Should we be concerned about Data-opolies?' (2018) As:2 Geo.L.Tech.Rev.p 275 available at;
https://www.georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-Stucke-pp-275-324.pdf

Stucke M E, Ezrachi A, ‘When Competition fails to optimize Quality; A look at search Engines’ [2017] 18 Yale J of Law and Tech 70, p 86

Sun L ,‘Draw a Line between Freedom of Speech and Privacy of Public Figures’ Humanity, 2013 available at ; https://novaojs.newcastle.edu.au/hass/index.php/humanity/article/view/36/

Taddeo M, Floridi L, ‘The Debate on the moral Responsibility of Online Service Providers’, 22 Sc &Engineering Ethics 1575,1592 (2016)

Taylor M, ‘The EU’s human rights obligations in relation to data protection laws with exterritorial effect’, (2015) International Data Privacy Law, Vol 5, Iss 4 pp 246–256,

Tene O, Polonetsky J, ‘Symposium Issue - Privacy in the Age of Big Data: a time for big decisions’ [2012] Stanford Law Review vol 64 (63), pp.63 - 69

Townsend J, ‘Data Protection and the Right to be Forgotten in Practice: A UK perspective’ (2017) International Journal of Legal Information 45.1 pp 28-33

Tesón F R, ‘International Human Rights and Cultural Relativism’, 25 VA. J. INT'L L. (1985), pp 869- 898

Tzanou M, ‘The war against terror and transatlantic information sharing: Spillovers of privacy or Spillovers of security?’ (2015) 31 (80) Utrecht Journal of Int. & European Law 87

Uršič H, ‘In the Anticipation of the Right to be Forgotten’s 3rd Birthday- EU Courts In Search of Boundaries, Coherence and Balance’, [2018] The Interdisciplinary Internet Institute available at http://www.theiii.org/index.php/1901/in-the-anticipation-of-the-right-to-be-forgotten.

Veil W, 'The GDPR, The Emperor's new clothes. On the structural shortcomings of both the old and the new Data Protection Law' [2018] IAPP Resource Center available at http;//ssrn.com abstract =3305056

Verheij A J, 'The right to be forgotten – a Dutch perspective', [2016] International Review of Law, Computers & Technology, 30:1-2, pp 32 -41,

Voss W G, 'European Union Data Privacy Law Reform General Data Protection Regulation Privacy Shield and the Right to De listing' (2016) The Business Lawyer, Vol 72 Winter 2016-2017

Voss W G, 'After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy Law in a Time of Change', (2016) Toulouse Business School January 6, Business Lawyer, Vol. 71, No. 1, 2015/2016

Voss W G, 'Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation' [2018] La Revue Juridique Themis, Universite de Montreal, Faculte de Droit, , 50 (3), pp.783-820 available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3104800

Voss W G, 'Obstacles to Transatlantic Harmonisation of Data Privacy Law', (2019) University of Illinois, Journal of Law Technology & Policy, Vol 2019

Warren S D & Brandeis L D , 'The Right to Privacy', [1890].4 Harv .L. Rev. 193

Weber R H, 'The Right to be Forgotten More than a Pandora's box ?' [2011] JIPITEC 2 120

Wechsler S, 'The Right to Remember: The European Convention on Human Rights and the Right to be Forgotten', [2015] Columbia Journal of Law and Social Problems, 49.1.p 135 -165

Werro F, 'The Right to Inform v The Right to be Forgotten: A Transatlantic Clash', [2009] Research Paper No 2 available at htpp://ssrn/abstract=1401357

Whitman J Q, 'The two Western Cultures of Privacy : Dignity versus Liberty' [2004]Faculty Scholarship Series Paper 649 http://digitalcommons.law.yale.edu/fss_papers 649

Willis LE, 'Why Not Privacy by Default?' [2014] Berkeley Technology Law Journal 29(1), pp.61–134.

Witte DS, 'Privacy Deleted: Is it too late to protect our privacy online?' [2013] Journal of Internet Law, 17(7), pp.1–28.

Wright R G, 'The Right to Be Forgotten: Issuing a Voluntary Recall' [2015] Indiana University Robert H. McKinney School of Law Research Paper No. 2015-13. Available at SSRN: https://ssrn.com/abstract=2569237

Wright J Skell, 'Defamation Privacy and the Public's right to know: A national problem and a new approach,' [1968] Texas Law Review, 46

Youm KH, Park A, 'The right to be forgotten in European Union Law: Data Protection Balanced with Free Speech'. [2016] Journalism and Mass Communication Quarterly 1-23

Young SP, 'Politicians Privacy', [2018] Ramon Llull Journal of Applied Ethics, Iss 9 pp 191-210

Zalnieriute M, 'Google LLC v Commission Nationale De L'Informatique et Des Libertes (CNIL)', [2020] American Journal of International Law, Vol 114 (2)

Zanfir, G, 'Tracing the Right to be Forgotten in the Short History of Data Protection Law: The 'New Clothes' of an Old Right' [2013] presented at the Computers, Privacy and Data Protection Conference, Brussels, 22-34 January 2014. available at SSRN: https://ssrn.com/abstract=2501312

Press releases and Statements

Statement on Internet Search Engines, AEPD Madrid I Dec 2007 Director of AEPD to constitutional Commission of Congress Madrid , 28 Mob 2007

Press Release; European Commission, 'European Commission sets Out Strategy to Strengthen EU Data Protection Rules', IP/10/1462 Nov 4, 2010

Press release; Data protection reform: available at
https://ec.europa.eu/commission/presscorner/detail/en/MEMO_12_41
MEMO/12/41Brussels, 25 January 2012

Press Release; Viviane Reding, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age', Innovation Conference Digital, Life, Design Munich 22 Jan 2012 available at; https://europa.eu/rapid/press-release_SPEECH-12-26_en.htm

Press Release; EDPS: Enforcing EU data protection law essential for rebuilding trust between EU 21 Feb 2014 available at
https://ec.europa.eu/commission/presscorner/detail/en/EDPS_14_4

Press Release; Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, Adopted on 16 September 2014 available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

Press release; – Commission issues guidance on transatlantic data transfers and urges the swift establishment of a new framework following the ruling in the Schrems case
Brussels, 6 November 2015
'EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield' Feb 2016

https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216 last accessed 22 Feb 2021

Press release; European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows, 12 July 2016 Brussels
http://europa.eu/rapid/press-release_IP-16-2461_en.htm

The Conservative and Unionist party Manifesto 2017 available at; https://s3.eu-west-2.amazonaws.com/manifesto2017/Manifesto2017.pdf last accessed 25 May 2017

Press Release; European Court of Human Rights ECHR, 237 (2018) 28.06.2018 The public's right to access archived material online took precedence over the right of convicted persons to be forgotten

Consultation outcome -Online Harms White Paper: Full UK government response to the consultation 15 December 2020

Newspapers and Blogs

Brüß M, 'German FCJ: doctors can have their profile deleted from rating site - but can they?' February 23, 2018 available at https://ipkitten.blogspot.com/2018/02/german-fcj-doctors-can-have-their.html last accessed 27 Feb 2021

Giovanni Buttarelli 'Future of Privacy Forum Conversation with Giovanni Buttarelli ' (2018) see https://fpf.org/blog/a-conversation-with-giovanni-buttarelli-about-the-future-of-data-protection-setting-the-stage-for-an-eu-digital-regulator/ last accessed 22 Feb 2021

Corfield G, *Here is how Google handles Right To Be Forgotten requests*, The Register (May 2018)

Fleischer P, 'Foggy thinking about the right to Oblivion', (2011) available at;htpp://peterfleischer.blogspot.com.com/2011/03

Floridi L, 'Right to be forgotten poses more questions than answers', [2014] https://the guardian.com/technology/2014/nov/11/right to be forgotten

Fujikawa M, 'Google Japan Case Raises Issue of "Right to Be Forgotten,"' (Oct 2014) Wall Street Journal, available at http:// online.wsj.com/articles/google-japan-case-raises-privacy

Goni U, 'Can a soccer star block Google's searches', Time. (Nov 14 2008) available at http://world articles0,8599,1859329html

Greenwald G, 'why Privacy matters' Ted Global 2014 available at
http://www.ted.com/talks/glenn_greenwald_why_privacy_matters

Haynes D, 'Forget the Right to be Forgotten, Other Means Exist'. [2014] The Conversation at http://theconversation.com/forget-the-right-to-be-forgotten-other-means-exist-29117 243

Heilweil R, 'How close is an American right-to be-forgotten ?' Forbes, 4 Mar 2018
Cambridge Analytics https://www.theguardian.com/news/series/cambridge-analytica-files

Johnson B**,** 'Privacy is No Longer a Social Norm says Facebook Founder'. The Guardian [2010] Available at http://www.theguardian.com/technology/2010/j
an/11/facebook-privacy

Keene D R, 'When Does rehabilitation create a 'right to be forgotten' [2018] available at; https://ukhuman rights blog.com 2018/04/20 when-does- rehabilitation-create -a -right to -be -forgotten

Kiss J, ″Dear Google: open letter from 80 academics on 'right to *be forgotten*'″. The Guardian. https://www.theguardian.com/technology/2015/may/14/dear-google-open-letter-from-80-academics-on-right-to-be-forgotten

McCay L, 'The Internet never forgets; how to live in the 21st Century', June 30, 2012 https://www.huffingtonpost.com/dr-layla-mccay/the-internet-never forgets_b_1460110.html

Meichtry S, 'Italy says Google Trio violated Boy's privacy', (Feb 25 2010) Wall Street Journal available at https://www.wsj.com/articles/SB10001424052748704240004575084851798366446

Peltz-Steele R, 'The right to be forgotten is really a right to be forgiven,' Washington Post, Nov 21 2014

Powles J, 'Jimmy Wales is wrong: we do have a right to be forgotten'[2014] https://the guardian/technology/2014/aug/08/jimmy-wales

Rosen J, 'The Web means the End of Forgetting', [2010] The NY Times ,25 July 2010

Samonte M, europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/

Scott M, 'Google appeals French Privacy Ruling' The New York Times, https://www.nytimes.com/2016/05/20/technology/google-appeals-french-privacy-ruling.html?_r=0

Scott M, "French Court Refers Google Privacy Case to ECJ", *Politico*, July 19, 2017, https://www.politico.eu/article/french-court-refers-google-privacy- case-to-ecj/.

Selinger E, Hartzog W, 'Google can't forget you, but it should make you hard to find', [2014] "Wired", available at https://www.wired.com/2014/05/google-cant-forget-you-but-it-

should-make-you- hard-to-find/.

Smith E ,'The Tech lash against Amazon, Facebook and Google and what they can do', The Economist, 20 Jan 2018,

Toobin J, 'The Solace of Oblivion Annals of Law' [2014] available at www.newyorker.com/magazine/2014/09/29/solcae-oblivion

Tomlinson H, 'Article 8 and the "outside world": privacy, reputation and employment'[2019] available at https://inforrm.org/2019/01/10/article-8-and-the-outside-world-privacy-reputation-and-employment-hugh-tomlinson-qc/#more-41358

The BBC 'Facebook reverses ban on news pages in Australia', available at https://www.bbc.co.uk/news/world-australia-56165015 last accessed 25 Feb 2021

The Guardian, 'The Edward Snowden revelations', see https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

The Guardian, 'Privacy is No Longer a Social Norm says Facebook Founder', Available at https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

The Guardian, 'Effectively people will be able to airbrush history. In terms of using the law, this is entirely novel,'. https://www.theguardian.com/media/2018/feb/16/max-mosley-threatens-sue-papers-orgy-story-data-laws

The Independent, 'How France fell out of love with Mintel ' article about the Minitel Rose sex line scandal http://www.independent.co.uk/news/world/europe/how-france-fell-out-of-love-with-minitel-7831816.html last accessed 15 June 2019

The New York Times, 'Ordering Google to Forget', May 2014, https://www.nytimes.com/2014/05/14/ opinion/ordering-google-to-forget.html? r=0.

The New Statesman, 'How Quantum Computing will change the world' https://www.newstatesman.com/science-tech/technology/2017/12/how-quantum-computing-will-change-world, last accessed 9 Feb 2018

The Washington Post, 'Facebook updated its Manage Activity setting to allow the deletion of old posts in order to 'prevent stalkers, employers and the government from snooping on your past, too'. see https://www.washingtonpost.com/technology/2020/06/02/facebook-manage-activity/ last accessed December 2020

Other Sources

Thomas Jefferson, First Inaugural Address, 4th March 1801 available at; http://avalon.law.yale.edu/19th_century/jefinau1.asp last accessed 17 April 2017

Hansard, House of Lords 5th series, vol 585, col 436, Jan 1998.

Pew Research Center 'Teens, Social Media & Technology Overview 2015 'available at www.pewinternet.org/2015/04/09/teens-social-media-technology-2015, last accessed 18 Feb 2021

Online Reputation: What are they saying about me ? ' Discussion Paper prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada, available at https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/or_201601/

"Google v CNIL (CJEU)", *Reporters Committee for Freedom of the Press*, November 29, 2017, https://www.rcfp. org/browse-media-law-resources/briefs-comments/google-v-cnil-cjeu;

Regulating Online Privacy: Some Policy Guidelines, Including Guidelines for International Harmonization, Proceedings of the 51 St Hawaii International Conference on System Sciences 2018

Google, Requests to delist content under European privacy law, Transparency report: available at https://transparencyreport.google.com/eu-privacy/overview last accessed 15 Feb 2021

Search engine by country, available at http://returnonnow.com/internet-marketing-resources last accessed 18 Feb 2021

The Google Transparency Report https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en last accessed 24 Feb 2021

Debating Ethics, Dignity and Respect in Data Driven Life 40th International Conference of Data Protection and Privacy Commissioners, October 2018 https://www.privacyconference2018.org/en/40th-international-conference-data-protection-privacy-commissioners.html_

Freedom of Information Request, E P Kirkwood to UK ICO (Case Reference Number IRQ0856742 Aug 2019),

Winston Maxwell, 'Chronicle of Data Protection, Report on the French proposal'. Hogan Lovells, Nov 18 2009

Mason S, 'A Balanced View – Independent Assessment Safeguarding the public through the fair and proportionate use of accurate criminal record information', March 2010, https://webarchive.nationalarchives.gov.uk/20100408141053/http://police.homeoffice.gov.uk/publications/about-us/ind-review-crim/a-balanced-approach-12835.pdf?view=Binary