University of Vienna

European Master's Degree in Human Rights and Democratisation

A.Y. 2016/2017

TO BE OR NOT TO BE FORGOTTEN: A New Dimension of the Conflict between the Right to Privacy and Freedom of Expression

Author: Yuliya Moshkovska

Supervisor: Christina Binder

Abstract

Global nature of communication technologies has raised new issues concerning privacy and the extent to which freedom of expression could be exercised. *The right to be forgotten*, a rather new approach to privacy protection, has emerged in the heart of the conflict between the two fundamental rights. The European provision of a new right has sparked a global debate over possible dangers of the application of the right. Global censorship and erasure of historical records being some of them, the controversial right is claimed to threaten the freedom of the Internet. Supporters of the right to be forgotten disagree and see it as a tool to regain the effective control over our private data and thus protect our privacy rights in the online world. But does forgetting on the Internet pose such an imminent danger to freedom of expression or is it disregarded due to emotional responses based on misunderstanding of what is being proposed? The prospective scope of the right to be forgotten is being decided now. The direction of its development, as well as the scope and applicable jurisdiction are currently on the international agenda. The future of applying human rights in the online environment is at stake.

Acknowledgements

I would like to thank Manfred Nowak and the entire E.MA team for their enthusiasm and support, as well as my supervisor Christina Binder.

Special thank you to Natasha for being the best possible company in this journey. You made my second semester an incredible experience filled with humour and new discoveries.

I also have to acknowledge the valuable input of Steven in my research. I would like to express my warmest gratitude for your patience and timely support.

List of Abbreviations

ICCPR - the International Covenant on Civil and Political Rights

HRC - the United Nations Human Rights Committee

GDPR - The General Data Protection Regulation

UDHR - The Universal Declaration of Human Rights

ECHR - The European Convention on Human Rights

ACHR - The American Convention on Human Rights

ACHPR - The African Charter on Human and Peoples' Rights

EU - The European Union

OECD - The Organisation for Economic Cooperation and Development

AEPD - Agencia Española de Protección de Datos (Spanish Agency of Data Protection

CJEU - The Court of Justice of the European Union

URL - Uniform Resource Locator

ICCL - The Irish Council for Civil Liberties

ECtHR - The European Court of Human Rights

GCHQ - The Government Communications Headquarters

NSA - National Security Agency, USA

DPA - Data Protection Authorities

29WP - The Article 29 Working Party

APME - Associated Press Managing Editors, Canada

ECJ - The European Court of Justice

TGI - Tribunal de Grande Instance, France

DRM - Digital Rights Management

Table of Contents

Introduction

Surpassing merely human capabilities to remember information, digital era has introduced the reality of eidetic memory - a phenomena, which keeps intact every detail of every event and could instantly recall them with high precision. If human brain has limited possibilities to retrieve and store information, the complex system of computer networking has indeed no boundaries. The vast amount of collected data is being constantly shared by users of the World Wide Web, thus raising new challenges to protection and regulation of the private information. It is the global nature of the Internet that makes data from any corner of the world accessible in a click of a mouse. In the meantime, excessive quantity of data has made it harder to control how and with whom we want to share information. What enters the online world often stays there for an unlimited period of time and can be easily retrieved with the help of search engines. Humanity has faced a problem never seen before: the Internet never forgets.

Memory is a double edged sword. It accentuates the highs and underscores the lows. Warranted or not, our reputations have become a part of the common perception of our identity. It is because of memory that we pay a thousand times for the same sin. To remember a deed is to act it out in memory as it happened over and over again as long as the remembering continues, like a broken record. The robber will stay a robber. But when an individual does eventually falter, is it right for humanity to hold this error over his head for the rest of his days? The very reason pencils have erasers and keyboards have delete keys is behind the approach that no man should exempt from - to have a second chance.

The new reality of the digital age has brought the need to reclaim the effective control over our data. Do the individuals have the right to decide to which extent their personal information could be shared with the world? They surely do. But what happens when data has already entered the Web? The possibility of individuals making decisions to remove certain online content that relates to them would surely expand the notion of privacy. Nevertheless, such prospects would directly interfere with the fundamental human right to freedom of expression, undermining the characteristic purpose of the Internet - effective sharing of information on the global level.

These considerations reflect on the current international agenda. In 2014 the Court of Justice of the European Union has set a controversial precedent that has sparked debate all over the globe. Allowing

individuals to remove search results on the Internet when they are related to their private data, have raised the question of striking the balance between the two fundamental human rights: the right to privacy and freedom of expression. The decision has been met with conflicting reactions. Some argue that implementation of the new right to be forgotten will serve as a tool for global censorship and will directly affect the integrity of historical record. Others disagree, stating that the introduced right will merely harmonize the disproportionate relationship between data processing and individual's right to privacy.

"To be or not to be forgotten?" that is the question, that will have to answered by international community in the near future.

Research Questions.

Current research aims to answer the following question:

In the conflict between the right to privacy or freedom of expression, where does the right to be forgotten draw the line?

The existing practice will help to define where does the international community stand in the conflict between the right to privacy and freedom of expression and therefore what is the place of the right to be forgotten and its direction of the future development.

To answer this question the following subquestions will provide the context to draw the conclusions:

1. How did the right to be forgotten emerge and how is it currently regulated?
2. Which right prevails in this context according to the global practice: the right to privacy or freedom of expression?
3. What are the effects of the right to be forgotten on freedom of speech and information?
4. How far should the right to be forgotten reach? Should it become global?
5. Which information should be considered when applying the right to be forgotten?
6. Is it relevant what kind of individual is in question? Is the source of private information relevant?
7. When does the state interest overweight privacy? Or the other way around.
8. When does the public's right to override privacy? Or the other way around.

9. How does the commercial interest of tech giants reflect on the right to be forgotten and privacy? Should search engines be data controllers in that sense?
10. How does the right to be forgotten influence journalism?
11. How does the right to be forgotten reflect on human dignity and reputation?
12. According to current legal development and existing state practice on the issues of privacy and freedom of expression, what is the future of the right to be forgotten?
13. What are the challenges of the right to be forgotten?
14. What are the perspectives of the right to be forgotten development and its implications on online freedom?

Methodology

In order to answer the research question and subquestions a number of methods will be used. Historical analysis will be used to bring a new perspective to the right to be forgotten. Hence, different historical findings, legal documents and academic discourse will be used when establishing the basis of the right and its historical background. Subsequently, various national and international law doctrines will be used to provide a context on the conflict between the right to privacy and freedom of expression. The legal analysis of the provisions of international treaties, specific national regulations and respective law and soft law instruments of the European Union, will be performed to establish national, regional and international regulations of the aforementioned human rights. When analysing the tendencies of the prevalence of one right over the other in the framework of common-law and civil-law jurisdictions, existing case law on both national and international level will be an essential source.

Considering the digital aspect of the emerged right, the research will also use the sources of the current discourse on the right to be forgotten available on the Internet. This will include, but will not be limited to media response and reaction towards the implementation of the right, public statements made by search engines and their employees concerning the position of tech giants on the right to be forgotten, and statistical data provided by Google Transparency Report, featuring the details of the implementation of the right since 2014.

Relevant case law will support the arguments that relate to balancing privacy, public's opinion, freedom of expression and press. Notwithstanding, the findings, opinions and recommendations of academics, lawyers, politicians and tech professionals regarding the right to be forgotten will serve as a basis for establishing the scope of the right and its possible directions of development.

CHAPTER I. TOWARDS A NEW DIMENSION OF THE RIGHT TO PRIVACY: THE RIGHT TO BE FORGOTTEN

1.1. Emergence of the Concept of the Right to be Forgotten, Background.

Throughout the existence of mankind, transferring and storing information was the key to preserving and passing experience and knowledge from one generation to another; oral storytelling and written accounts were the previous methods of doing so. With every step of technological progress — from pigeon post to telegrams — new attempts to share information were developed in order to reach the wider public at greater distances. The emergence of computer technology and the Internet has undoubtedly facilitated the sharing of all forms of information on the unlimited territory and with an infinite public. Now information can be shared from any part of the world with the press of a button.

Together with limitless advantages in all spheres of human interaction and scientific development, the Internet has spawned unprecedented issues. While people continue sharing various forms of data online and digitising it for convenience and storage, it exposes the information to risks of surveillance and massive data harvesting.

This becomes particularly evident from the necessity of introduction of the right to be forgotten. If in the past forgetting was the norm for mankind and remembering was the exception, the emergence and rapid development of new technologies has reversed this ratio on a global scale. New opportunities to process and store information have made what was once a default forgetting to an automatic remembering. When data storage was limited to human memory forgetting was an inevitable part of processing information. Even physical records kept in libraries were only relevant so as long as the medium in which the information was stored was kept intact; books, articles, pictures, photographs and film that

existed until their erosion and/or destruction.[1] Even with the emergence of web pages on the World Wide Web the data was not preserved permanently. Each web page has a lifespan between 75[2] to 100 days and stores information until its expiration, unless archived.[3] A decade later, methods of Web preservation are still not able to permanently backlog data on the Web. Notwithstanding, various archives and data centers around the globe are able to store more than 600 billion gigabytes of data.[4]

Among the other factors of the discourse, the sources of collected data are of crucial importance. Today most aspects of our lives and interactions with others are recorded by various technologies. Our biometric data is collected by law enforcement authorities and stored in order to create a database to identify individuals. Doctors store medical records that contain highly personal information in a digital form.[5] Social media has become a platform where anyone can share personal information about themselves or any third party with an unlimited amount of users. Surfing the Internet also creates digital footprints and all data collected by cookies and search queries can tell more about us than we could possibly imagine: location data, our reading behaviour, that you were searching to buy a house in 2007, where you went for vacation the same year and by which airline, that in 2009 you searched for cancer specialists in your town and the next year you were looking for a divorce lawyer. This type of information does not only contribute to establishing certain trends according to demographics but also adds up into our extensive "*digital dossiers*".[6] Moreover, the means of communication, emails, text messages and even phone calls, collect a massive amount of data that is stored on various servers.

This towering amount of information is being constantly collected by governments and private companies. Just as new technologies allow us to share gigabytes of information and store it when needed, it also makes this data easily accessible to third parties. Anything that is being sent through the World Wide Web, be it a business email or a private photograph, can be traced and accessed with the help of respective technologies. Furthermore, mountains of information remain on the surface of the

[1] V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, Princeton and Oxford. 2011. Shared Memory.
[2] S. Lawrence and C.L. Giles, 'Accessibility of Information on the Web,' Nature, 8 July 1999, pp. 107-109.
[3] N. O. Finnemann, 'Internet - a Cultural Heritage of Our Time'. Forskning. 2001. p.3.
[4] J. Bruner, 'Where the World's Data Is Stored' (Forbes, 2011) <https://www.forbes.com/sites/jonbruner/2011/07/19/where-the-worlds-data-is-stored-infographic/#1341c51373af> accessed 13 July 2017.
[5] V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, Princeton and Oxford). 2011. Chapter I.
[6] J. Ausloos, 'The 'Right to Be Forgotten' - Worth Remembering?'. Computer Law & Security Review, Volume 28, Issue 2. 2001. pp. 143-152.

Internet due to global search engines. Any website or social media post can resurface from yesteryear by simply defining a couple of key words in search engines.

There is a common perception that in this age of the nearly perfect memory of the Internet nothing can be forgotten. And with this reality it is inevitable that at some point the question of "*Who should be a data controller?*" will become paramount in the rhetoric about appropriation, intrusion, false light and public disclosure of private information.

The idea of regaining the effective control over personal data has been present in the academic discourse way before the emergence of the Internet. In 1967 Alan Westin published his book "Privacy and Freedom" where the definition of privacy was "*the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"*.[7] A number of other authors had various ideas of what privacy should cover, but the majority agreed that there should be the right to erase certain information.[8] The concept of the right to be forgotten, or the right to oblivion,[9] has been explored in different legal contexts from rather diverse angles. In the opinion of Bert-Jaap Koops, there are three major approaches to the right to be forgotten in the literature: the right to have data deleted through expiration dates of the information, the right of a "clean slate", and the right to be judged only on present merits, rather than on their past.[10] The first interpretation focuses on individuals invoking the right to be forgotten against parties that are in possession of such information, thus erasing the data about their past, which such parties were intending to publish or make decisions about individuals based on this information. The objections to the existence of this data have to be justified. If information is no longer relevant, inaccurate or there is another objective justification, individuals may claim for their data to be removed by data controllers.[11] To enforce this right proves to be rather complicated, as the information might be possessed by multiple parties. Furthermore, certain parties may be authorised to obtain data under the law, which might make it difficult to demand such information to be erased. This form of the right to be forgotten may be

[7] A. Westin, *Privacy And Freedom*, Atheneum, 1967. p. 7.
[8] J. E. McNealy, 'The Emerging Conflict between Newsworthiness and the Right to Be Forgotten', Northern Kentucky Law Review, Vol. 39, No. 2 , 119-135. 2012, p. 121.
[9] The right to be forgotten is called "the right to oblivion" in Italy, Belgium and France.
[10] *Ibid.* p. 121.
[11] B.-J. Koops, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice', Tilburg Law School Research Paper No. 08/2012 229-256. 2011. pp. 229, 236.

applied in both cases, when the data has been released or published voluntarily by the individual, and when it has been made public by a third party.[12]

Jasmine McNealy asserts that the right to have a "*clean slate*" and the right to be connected only to present information are relatively similar. The two forms of the right to be forgotten share the notion that individuals change over time and it would be unreasonable to link them forever to their recorded past if it could be damaging to their present. A *clean slate* approach would thus allow individuals to mold their life on their own as opposed to being associated with the deeds from their past that remain in the memory of others.[13] An opportunity to have a fresh start on the Internet has also been regarded by Jonathan Zittrain, who introduced an approach of "*reputation bankruptcy*". This concept includes the erasure of all online data about an individual — text, photos and other information — in order to provide them a fresh start on the Web. According to Koops there are two clean slate perspectives that can be categorised as social and individual. Thus, social option regards than an individual should not be connected with outdated negative data and should have an opportunity to not be identified in relation to the past. Such approach had been already incorporated in the domestic law of plenty of states in the areas of juvenile criminal law, bankruptcy law and credit reporting.[14] For instance, Germany has a specific policy that aims to reintegrate convicted criminals back into society and prohibits the mentioning of their name in relation to the crime they committed after they have served their sentence.[15] Similarly, the individual perspective proposes that people should not be restricted in their right to speak and write openly out of fear that it may be used against them in the future. The alternative would not only undermine the basic principles of the democracy and freedom of expression, but also take away a "*fundamental human capacity — to live and act firmly in the present*".[16] Without any doubt, the right to be connected only to the current information is analogous to the clean slate approach. Meanwhile, it refers only to certain data about the past of the individual, that may bring damage, but not all data about the person available online.

---

[12] B.-J. Koops, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice', Tilburg Law School Research Paper No. 08/2012 229-256. 2011. pp. 238-39.
[13] J. E. McNealy , 'The Emerging Conflict between Newsworthiness and the Right to Be Forgotten', Northern Kentucky Law Review, Vol. 39, No. 2 , 119-135. 2012. p. 121.
[14] B.-J. Koops, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice', Tilburg Law School Research Paper No. 08/2012 229-256. 2011. pp. 229, 236.
[15] J. van Hoboken, *'The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Freedom of Expression Safeguards in a Converging Information Environment'*, European Commission, Amsterdam, 2013, p.3.
[16] V. Mayer-Schönberger V., *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, Princeton and Oxford). 2011. Chapter I.

There is a common misconception that the right to forget and the right to be forgotten are analogous or interlinked. In fact, the right to forget is directly connected to freedom of expression. According to Article 19 of the International Covenant on Civil and Political Rights (ICCPR, 1966), everyone has a right to hold and express opinions without interference.[17] Antoon De Baets has proposed a thought-provoking conclusion that since "opinion" also covers the memories of past events, it indicates that every human individual has a so-called right to memory. He states that since the United Nations Human Rights Committee (HRC), which is authorised to interpret the Covenant, specifically prohibits any coercion in the field of opinions, "*Any form of effort to coerce the holding or not holding of any opinion is prohibited. Freedom to express one's opinion necessarily includes freedom not to express one's opinion*",[18] then in line with the right to memory there is the right to forget. Therefore, no one should have an obligation to remember. From this perspective, both, the right to remember and the right to forget, are included in the right to free expression.[19]

Unlike the right to forget, the right to be forgotten derived from the right to privacy. The most recent definition of the right to be forgotten in the context of digital memory and data retention has been stipulated in the General Data Protection Regulation (GDPR), adopted by the European Parliament in April 2016. Article 17 of the Regulation provides the right to erasure, which obliges data controllers to erase publicly available information in their possession concerning the data subject, as well as to cease processing aforementioned information, when: such data is no longer necessary for the purposes it has been collected for; the data subject withdraws consent and there is no legal ground for processing; data subject objects to processing on grounds relating to his or her particular situation and there are no overriding legitimate grounds for processing or when data subject objects to their personal data being processed for direct marketing purposes; the personal data has been unlawfully processed; the personal data has to be erased for compliance with a legal obligation in European Union or Member State law to which the controller is subject; the personal data that is being processed is related to a child.[20]

[17] International Covenant on Civil and Political Rights, 1966. Art. 19.
[18] United Nations Human Rights Committee General comment No. 34: *Article 19: Freedoms of Opinion and Expression*. GE.11-45331. 2011.
[19] A. De Baets, 'A Historian'S View On The Right To Be Forgotten', International Review of Law, Computers & Technology. 2016. p.58.
[20] Regulation (EU) 2016/679 On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016.

Similar to the duty to remember being enforced on individuals, the right to be forgotten also involves the aspect of coercion. Although the application of this right protects privacy of the subject, it diminishes the right to information of others as well. In that case, the right to be forgotten influences freedom of expression. Taking into account the role of search giants in the online world, establishing the right to oblivion may also result in making Web search engines "*an indirect tool of censorship*".[21] In fact, there is an extensive discourse on whether this right would lead to re-writing history and affect not only life stories of certain individuals, but also bring a change to larger historical patterns.[22] Besides the argument that the right to be forgotten will affect the right to free expression in a negative way by limiting the right to know of others, some believe that on the contrary, it may support the people in freely expressing themselves considering that their opinions could be reversed.[23]

Nevertheless, the right to be forgotten will not be absolute, as there are certain circumstances that justify data being preserved. Viviane Reding, a former EU Justice Commissioner,[24] stated that, "*It is clear that the right to be forgotten cannot amount to a right of the total erasure of history…The new EU rules will include explicit provisions that ensure the respect of freedom of expression and information*".[25] At this point, the text of the Regulation remains unclear on how this right could be applied in practice from both aspects, enforcement and technological challenges, giving the states a broad window of interpretation.

1.2. The Ongoing Conflict Between the Right to Privacy and Freedom of Expression.

In our everyday life privacy and freedom of expression collide on a daily basis. Perhaps someone posted a picture of you that you don't appreciate on Facebook without your consent, or a company used a photograph of your child for advertising purposes and did not notify you, or your former boyfriend made a private video of you public, or maybe a journalist opened your correspondence and used the content for their next sensational article. The battle in establishing balance between freedom of expression and

[21] J. van Hoboken, *Search Engine Freedom. On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines*. Kluwer Law International 2012. p.34.
[22] A. De Baets, 'A Historian'S View On The Right To Be Forgotten', 10 International Review of Law, Computers & Technology. 2016. p.58.
[23] *Ibid*. p.64.
[24] Viviane Reding has been a Vice-President of the European Commission and European Commissioner for Justice, Fundamental Rights and Citizenship from 2010 to 2014. The post is now called "European Commissioner for Justice and Consumers" and is occupied by Vera Jourova.
[25] V. Reding, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age', Speech/12/26. Innovation Conference Digital, Life, Design, 2012.

the right to privacy has been a challenging issue throughout history and has become even more complicated with the emergence of modern technologies. Each of these rights happen to be opposite sides of the same coin, being closely interlinked on the level that both can be possible causes and consequences of the infringement of one another.[26] In order to exercise freedom of expression it is essential that an individual enjoys no interference with his or her right to hold and express opinions, as well as receiving and imparting information and ideas. Such interferences can be executed by the states that in any way through their policies or judgements restrict the right of the citizens to freely express themselves. Third parties also unlawfully interfere with privacy and cause possible damage and distress. At the same time, in certain cases, freedom of expression of one's opinions and impartment of information concerning other individuals may directly interfere with the right to privacy of others. In that case, the authorities and courts face the challenge of weighing the public interest against the protection of the private life of an individual, and establishing whether such interference has been or would be proportionate.

Both, the right to privacy and freedom of expression are protected on international, regional and domestic level. Those fundamental human rights are provided in the Universal Declaration of Human Rights (UDHR), Article 12 and Article 19.[27] Being non-legally binding, the UDHR is an instrument of customary international law that sets the standards in promotion of human rights. Hence, the International Covenant on Civil and Political Rights is currently the most effective international treaty when it comes to protection of freedom of expression and the right to privacy. Article 19 of the ICCPR guarantees freedom of opinion and expression, while Article 17 stipulates that no one should be subjected to arbitrary or unlawful interference with "*privacy, family, home or correspondence, nor to attacks upon his honour and reputation".*[28]

Freedom of expression is also imposed on the regional level through human rights treaties. In Europe it is regulated by Article 10 of the European Convention on Human Rights (ECHR) signed in 1950.[29] Article 13 of the American Convention on Human Rights (ACHR, 1969) protects freedom of expression

[26] C. Nyst, 'Two sides of the same coin – the right to privacy and freedom of expression' (2013) <https://www.privacyinternational.org/node/103> accessed 14 July 2017.
[27] Universal Declaration of Human Rights,1948.
[28] International Covenant on Civil and Political Rights 1966. Art. 17 and 19.
[29] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as Amended) (ECHR), 1950. Art.10.

in a number of countries in the Western hemisphere,[30] while Article 9 of the African Charter on Human and Peoples' Rights (ACHPR) secures this right on the African continent.[31] Likewise, the right to privacy has been also guaranteed by the ECHR, Article 8, promoting respect for private and family life, home and correspondence of individuals.[32] In the European Union (EU) privacy is protected by the EU Privacy Directive since 1995.[33] All EU states were required to revise their national legislation to conform with the Directive. Still, it appears to be often criticised for its inadequate enforcement by the states. Besides the EU initiative, other regional systems do not cover privacy as such. Instead, almost every country in the world has recognised the right to privacy directly in their Constitution. Both, right to privacy and freedom of expression, have been guaranteed by national legislation. States have incorporated the norms from international or regional treaties into their legal framework.

The two rights are indeed not absolute and may be restricted in justified circumstances in compliance with international human rights law. The right to privacy, Article 8, and freedom of expression, Article 10, stipulated in the ECHR, concern mainly the interference by public authorities, as it is evident from the text of the articles.[34] Nevertheless, the provisions also include positive obligations of the states, meaning that they have an obligation to protect the rights from interference of other parties.[35] Comparably, Articles 17 and 19 of the ICCPR have a much broader approach and do not specify the parties that could interfere with the rights.[36] Even though the above-mentioned articles don't include limitation clauses, unlike ECHR,[37] any "*unlawful or arbitrary*" interference with privacy are prohibited, while freedom of expression may be restricted only when it is "*provided by law"* or it is "*necessary*". According to Manfred Nowak, the definition "*arbitrary*" implies a violation specifically by state authorities. While "*unlawful*" interference is suggesting that for intrusion of privacy to be lawful, the purposes of such interference should be proportionate to the infringement of the right.[38] Likewise, the restrictions of the freedom of expression must meet certain conditions: be provided by law, have one of

[30] American Convention on Human Rights, 1969.
[31] African Charter on Human and Peoples', 1981.
[32] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as Amended) (ECHR), 1950. Art.8.
[33] Directive (EU) 95/46/EC On the protection of individuals with regard to the processing of personal data and on the free movement of such data of the European Parliament and of the Council. 1995.
[34] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as Amended) (ECHR), 1950. Art. 8. And 10.
[35] K. Reid, *A Practitioner's Guide to the European Convention on Human Rights*, Sweet & Maxwell, 915. 2011. p. 603.
[36] International Covenant on Civil and Political Rights 1966, Art. 17 and 19.
[37] M. Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary*, N.P. Engel. 1277. 2005. p. 381.
[38] *Ibid.* p. 383.

the foreseen purposes, and be necessary for accomplishing that purpose.[39] The justified purposes of interference with freedom of expression and information are acknowledged in ECHR and include public order (*ordre public*), public health and public morals[40], and respect of the right or reputations of others. As the reputation of others is protected by Article 8 of the Convention, this provision creates an evident conflict between the two rights.[41] National security is another justified purpose, which is often used in practice, as the states have a certain margin of appreciation in defining what could be considered as a threat, same as assessing whether the need for interference in general exists.

Courts all around the world are facing the ongoing dilemma of how to balance freedom of expression and the right to privacy on case-by-case basis. The approaches towards balancing of these rights vary depending on the jurisdiction. Nevertheless, there are clear tendencies of prevalence of one right over the other in court rulings of states with common-law and civil-law approaches.[42] Common-law jurisdictions, including the United States and the United Kingdom, regularly protect freedom of expression and press at the expense of interference with privacy of individuals.[43]

A number of cases ruled by the UK courts demonstrate reluctance over establishing the place for privacy in the case law.[44] The notorious *Coco v A N Clark*[45] case provides a rather limited notion of privacy. With the plaintiff arguing the "*breach of confidence*", the Court established that revelation of information obtained in confidence violated the obligations of confidence. The main objective of the Court was the protection of business secrets. Nevertheless, this test could also be applicable in situations when the information has been disclosed by an individual, with whom the affected side had a previous relationship (husband and wife etc.)[46] Hence, confidentiality would be "*based ultimately on conscience*" and the party being aware that an individual was sharing a specifically confidential information, leaving a room for improvement of privacy doctrine.[47]

[39] M. Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary*, N.P. Engel. 1277. 2005. p. 458.
[40] *Ibid.* pp. 465-466.
[41] *Ibid.* pp. 462.
[42] A. De Baets, 'A Historian'S View On The Right To Be Forgotten', International Review of Law, Computers & Technology. 2016. p. 59.
[43] *Ibid.* p. 59.
[44] L.Teacher, 'Invasion of Privacy is not an acknowledged Tort in the UK', (2013) <https://www.lawteacher.net/free-law-essays/constitutional-law/invasion-of-privacy-is-not-law-essays.php?cref=1 > accessed 13 July 2017.
[45] *Coco v AN Clark (Engineers) Ltd.* F.S.R. 415, The High Court of Justice (1968).
[46] Has been an issue in circumstances when a relationship was not proximate.
[47] A. Sachdeva and B. Hitchens , 'UK Supreme Court Confirms That There Can Be No Liability For Misuse Of Trade Secrets Unless And Until Confidential Information Is Acquired' (2013)

The subsequent case, *Peck v United Kingdom*[48], only sustained the UK provision of privacy. Geoffrey Peck has sued the Brentwood Borough Council for the violation of his private life. In August 1995 Mr. Peck attempted suicide in a public space, which was captured by the CCTV cameras and led to police saving the plaintiff. Further on, the Council provided the footage to local newspapers, TV channels and BBC UK to publish it as an example of the benefits of CCTV cameras in crime deterrence. The footage has been broadcasted to more than 9 million viewers and seriously affected Mr. Peck's private life. The attempt to protect his rights in the UK court system did not have a constructive result, as the courts did not consider whether Mr. Peck's privacy was violated or not, because the law in the UK lacks provisions of the distinct right to privacy. Instead, the High Court ruled that the actions of the Council were not "*irrational*" and dismissed the claims of the plaintiff.[49] The case reached the European Court of Human Rights, which has overruled the decision, stating that Council's actions were "*disproportionate and unjustified interference with his private life*" and constituted the violation of Article 8 of the European Convention of Human Rights. Further UK practice has a rather shifted opinion towards balancing privacy and freedom of expression. *Campbell v Mirror Group Newspapers*[50], *Mosley v News Group Newspapers*[51], *Prince of Wales v Associated Newspapers*[52], *Douglas v Hello!*[53] have weighed privacy over free speech and press, applying the principle of proportionality.

Meanwhile, the United States legal doctrine has the First Amendment in its focus, "*Congress shall make no law … abridging the freedom of speech, or of the press…*"[54], while right to privacy is not guaranteed by the Constitution or any of the following amendments, but rather is acknowledged in its framework by the US Supreme Court.[55] The emphasis on the protection of free expression and the press has a respective reflection on the practice of the courts. In the *Arne Svenson* case the plaintiff, Mr. Foster, was seeking damages for the alleged violation of his privacy. Mr. Svenson, being a photographer, used long

---

<http://www.mondaq.com/uk/x/251460/Trade+Secrets/UK+Supreme+Court+Confirms+That+There+Can+Be+No+Liability+For+Misuse+Of+Trade+Secrets+Unless+And+Until+Confidential+Information+Is+Acquired> accessed 14 July 2017.

[48] *Peck v United Kingdom,* 44647/98, ECHR (2003).

[49] C. Dyer, 'Suicide bid on CCTV may herald new privacy law ' (2003) <https://www.theguardian.com/media/2003/jan/29/pressandpublishing.broadcasting> accessed 13 July 2017.

[50] *Campbell v MGN Limited [n.d.]* UKHL 22, United Kingdom House of Lords (2004).

[51] *Mosley v News Group Newspapers Ltd.*, EWHC 1777, QB (2008).

[52] *His Royal Highness The Prince of Wales v Associated Newspapers,* EWCA Civ 1776, UK Court of Appeal (2006).

[53] *Michael Douglas, Catherine Zeta-Jones, Northern and Shell plc v Hello Ltd.,* WC2A 2LL, England and Wales Court of Appeal (2000).

[54] Constitution of the United States of America, Amendment I, 1789.

[55] B. Shmueli, and A. Blecher-Prigat, 'Privacy for children', Columbia Human Rights Law Review. 2011. pp.759-795.

zoom lenses to photograph people in the windows of the neighboring buildings from his balcony. His neighbors were not aware that Svenson was documenting private, and even intimate, moments of their life. Further on, the so-called fine art photographer, used the images as the part of his exhibition. Foster and the neighbors insisted that this technological home invasion exposed their private life, thus violating their statutory right to privacy. US Supreme Court has ruled that the actions of Mr. Svenson did not constitute the violation of the right to privacy of Foster and others, since taken images were considered "*the work of art*" (protected by the First Amendment) and fall under newsworthy and public concerns exception. Although the intrusive actions of the photographer could rightfully offend the citizens, they did not amount to unlawful surveillance penalised by the Penal Law.[56]

Similar approach has been taken in the ruling of the *Finger v. Omni Publications* case. Plaintiffs Joseph and Ida Finger, on the behalf of themselves and their six children, were seeking damages from Omni Publications International for the publication of their photograph in Omni Magazine jointly with an article concerning the research of caffeine-aided fertilisation. The Finger family claimed that there was "no real connection" between them and the article, as none of their children were conceived with the help of *in vitro* fertilisation, nor have any of them ever participated in this research conducted by the University of Pennsylvania, thus undermining the "*newsworthiness*" of the article and stating that their image was indeed used "*for advertising purposes, or for the purposes of trade*". [57] The NY Court of Appeals ruled that "*it cannot be said, as a matter of law, that there is no "real relationship" between the content of the article and the photograph of plaintiffs".* Therefore, the actions of Omni Publications fall under the exception of newsworthiness and do not violate the right to privacy of the Finger family.[58]

[56] *Foster v Svenson*, 651826/13 12998, US Supreme Court (2015).
[57] Civil Rights Law. Section 50, entitled "Right of privacy", states: "*A person, firm or corporation that uses for advertising purposes, or for the purposes of trade, the name, portrait or picture of any living person without first having obtained the written consent of such person, or if a minor of his or her parent or guardian, is guilty of a misdemeanor.*" Section 51 states, in part: "*Any person whose name * * * or picture is used within this state for advertising purposes or for the purposes of trade without the written consent first obtained as above provided may maintain an equitable action in the supreme court of this state against the person, firm or corporation so using his name * * * or picture, to prevent and restrain the use thereof; and may also sue and recover damages for any injuries sustained by reason of such use* and if the defendant shall have knowingly used such person's * * * picture in such manner as is forbidden or declared to be unlawful by section fifty of this article, the jury * * * may award exemplary damages*"* (emphasis supplied).
[58] *Finger v Omni Publications International, Ltd.*, 77 N.Y.2d 138, Court of Appeals of the State of New York (1990).

In comparison, civil-law jurisdictions, such as Germany, Switzerland, France and Italy, prioritise privacy over freedom of expression, according to the extensive legal practice.[59] A number of cases demonstrate that the right to privacy often outweighs public interest, and in those circumstances interferences are considered disproportionate. *Axel Springer v. Germany* provides an example how German courts balance the two rights. When a German tabloid newspaper published an article about a renowned TV actor in conjunction with his photographs, they made public the stories of his former arrest and conviction. The plaintiff claimed that the newspaper violated his right to privacy and damaged his honour and reputation. German courts supported his claims, restricting the right to free expression enjoyed by the newspaper. Further on, the case reached the European Court of Human Rights, where it has been overruled on the grounds that there was no proportionality in imposing restrictions on the tabloid and therefore their actions constituted the violation of Article 10 of the ECHR.

A similar dilemma arose in the *Julie Gayet v Closer* case at the tribunal de Nanterre in France. French actress sued Closer magazine for violating her right to privacy and image rights after the tabloid published a sensational article that revealed her relationship with the former president of France, Francois Hollande. Ms. Gayet claimed that she never desired to confirm nor make public the alleged relationship, and as a result of such publication she has been constantly harassed by journalists, thus being unable to maintain a private life. Although the tabloid argued that the content of the publication was in the public's interest, because it related to Mr. Holland and questioned his transparency and presidential security, the Tribunal ruled that Closer violated the right to privacy of Ms. Gayet, as the article related more to public curiosity rather than interest, and therefore awarded the plaintiff damages, together with an obligation of the magazine to publish a new statement.[60]

New technologies have brought a different dimension to the conflict between the right to privacy of individuals and freedom of expression and information, particularly on the Internet. In 2010 a court in Milan indicted three *Google Italy* employees to a suspended six-month jail sentence for a failure to comply with Italian Privacy Law.[61] The background of the case was based on the incident that happened in 2006 in one of the schools in Turin, when students filmed bullying of their disabled classmate and

[59] A. De Baets, 'A Historian'S View On The Right To Be Forgotten', International Review of Law, Computers & Technology. 2016. p. 59.
[60] *Julie Gayet v Closer,* Le tribunal de Nanterre (2014).
[61] *Italy v Drummond, De Los Reyes, Fleischer,* Arvind,14667/08, Milan Court of Appeals (2010).

uploaded it to the Google Videos platform. The video was removed after receiving an official complaint, when it has been already seen by more than 12,000 viewers.[62] The Court ruled that the company should be held liable for not blocking the video on the site in a timely manner, which sparked a much bigger controversy: should tech giants monitor the content that is being posted on their platform? Google reacted vigorously to the verdict, releasing a statement that this judgement undermines the freedom of the Internet and of expression of others. The company emphasised that "*European Union law was drafted specifically to give hosting providers a safe harbor from liability so long as they remove illegal content once they are notified of its existence*", and therefore the company employees should not be held liable for the video they have no connection with (as they were not the ones who filmed and uploaded it online).[63] From the perspective of the judgement, would the court sentence a mailman who delivered an envelope that contained hate speech? In 2012 the Italian Court of Appeals overruled the decision, confirming the presumption of Web platforms playing the role of the host for content that is generated by users, thus not having responsibility of an editor.[64]

Without a doubt, the ongoing conflict between the right to privacy and freedom of expression does not have a *panacea*. The collision of the two rights differs on a case-by-case basis, and therefore it would be impossible to find a common way in balancing the rights without the infringement of one of them. The approach towards defining the extent of the proportionate interference with the rights varies from jurisdiction to jurisdiction. Although freedom of expression and the right to privacy are fundamental human rights, they are not absolute and therefore could be restricted in justified circumstances. Yet, it is up to the courts to weigh all the facts of the case and arrive to a conclusion whether any interference with the rights is justified and according to the international human rights law. The digital era has definitely brought a new perspective to the dilemma of striking a balance in this conflict. With current possibilities of collecting and sharing information, new privacy issues arise on a daily basis, while it becomes harder to define to which extent can freedom of expression be enjoyed on the Web. "Where do we draw the line between the two rights?" is the question that doesn't seem to have an answer in the foreseeable future.

[62] J. Israely , ' Italy's Google Verdict Starts Debate on Web Freedom' (2010) <http://content.time.com/time/business/article/0,8599,1968123,00.html> accessed 13 July 2017.
[63] Official Google Blog, ' Serious threat to the web in Italy ' (2010) <http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379> accessed 13 July 2017.
[64] E. Pfanner , 'Italian Appeals Court Acquits 3 Google Executives in Privacy Case' (2012) <http://www.nytimes.com/2012/12/22/business/global/italian-appeals-court-acquits-3-google-executives-in-privacy-case.html> accessed 13 July 2017.

1.3. The Right to be Forgotten: New Level of Privacy Protection.

Putting privacy and freedom of expression in dispute, the right to be forgotten is the concept that deals with both, privacy of an individual in question and collection and processing of information. The idea of being able to erase information in certain circumstances or after the passage of a certain period of time, is connected with the emergence of the need to regain effective control over data. If previously humanity tended to forget over time, digital memory has forever changed data retention with its capability to impeccably archive. Subsequently, perfect memory has its consequences. Besides preserving our knowledge, experience and history, it links us to our memories forever.

The historical origins of the concept of the right to be forgotten have been first found in the French notion of a "*droit a l'oubli*" (the right to oblivion) and its Italian version "*diritto al' oblio*".[65] Both approaches were based on "*the right to silence on past events in life that are no longer occurring*".[66] The idea behind the concept suggested that individuals should not be judged on the basis of past events that are no longer relevant. For instance, once a person has been acquitted for a crime they should not be linked to it from then on.

The right to erasure has been first introduced in the European Union Directive 95/46/EC in 1995. The Directive, also known as Data Protection Directive, aimed to safeguard the rights of individuals concerning the processing of data and its free movement. The principles that lie in the core of the document have been incorporated from the general principles established by the Organisation for Economic Cooperation and Development (OECD) regarding the handling of personal data. During the symposium in Vienna in 1977, the OECD acknowledged the necessity of understanding the challenges of data protection in the fast-changing digital environment, and proposed a plethora of guiding principles.[67]

[65] P. A. Bernal, 'A Right To Delete?', European Journal of Law and Technology. 2011. p.2.
[66] A. Rainer , *The Convergence of the Fundamental Rights Protection in Europe,* Springer, 214. 2016. p.51.
[67] A. Rose and K. Ollerhead, 'Data Protection And The Right To Be Forgotten.' (*Uk.practicallaw.thomsonreuters.com*, 2017) <https://uk.practicallaw.thomsonreuters.com/9-518-8790?__lrTS=20170521111238152&transitionType=Default&contextData=%28sc.Default%29&firstPage=true&bhcp=1> accessed 14 July 2017.

The basic principles adopted by the OECD contained provisions that the collection of personal data should include the consent of the data subject, when it is possible, and must be acquired through "*lawful and fair means*". OECD emphasised that any personal data must be relevant for the purposes that it has been collected for and subsequently used. Moreover, the guidelines specify the exceptions of disclosure of personal data, providing that such data can be disclosed only with the consent of the data subject or when the disclosure is in accordance with law. It is quite striking that back in 1977 the organisation already recognised the risks to information that remain relevant today: "*loss, unauthorised access, destruction, use, modification or disclosure of data*".[68] Considering the growing importance of safeguarding data in the digital world, the guidelines also contained a broad scope of rights of individuals relating to their personal data. The aforementioned rights included the right to receive a confirmation from the data controller apropos any data that has been collected with respect to the individual and challenge that data. In case of a challenge being successful, an individual would have the right "*to have the data erased, rectified, completed or amended*".[69]

A number of principles stipulated in the OECD Guidelines have been an underpinning foundation of the right to erasure of data, which further expanded to the right to be forgotten, and could be followed through to the Data Protection Directive. In the meaning of the Directive, an individual has a right to request his personal data being deleted if that data is no longer necessary. Article 12 (b) of the Directive, "*Right to access*", includes the provision that every data subject has a right to demand from the data controller the rectification, erasure or deletion of data in accordance with the provisions of the Directive, specifically when the data is incomplete or inaccurate.[70] One of the most substantial principles concerning data collection and processing is the purpose limitation. Accordingly, Article 6 of the Directive suggests that personal data can be collected and processed only for "*specified, explicit and legitimate purposes*". In other words, once the collected data does not correspond to the purposes it has been collected for, it can no longer be processed. Limiting data processing to a previously established scope can in theory put a defined boundary to the harm that could be potentially done.[71] Nevertheless, constant personalisation of the Web continues changing our comprehension of what information is seen

[68] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).
[69] *Ibid.*
[70] Directive (EU) 95/46/EC On the protection of individuals with regard to the processing of personal data and on the free movement of such data of the European Parliament and of the Council. 1995.
[71] J. Ausloos , 'The 'Right to Be Forgotten' - mbering?' Computer Law & Security Review, Volume 28, Issue 2. 143-152. 2011. p.145

as "useful", therefore questioning the effectiveness of this principle. The Directive also covers the legitimate grounds of the processing of personal data in Article 7, that is usually viewed in conjunction with the Article 6, as the foundation principles of the right to erasure. The main goal of the Directive was to protect individual's personal data from both public and private parties. Recognising that in certain circumstances such data protection approach may infringe upon the freedom of expression from the perspective of public's interest in specific publications, the Directive included the exception for journalistic, artistic and literary works.[72] Not surprisingly, the Directive did not intend to regulate publications on the Internet since back in 1995 it was in its early stages of development and it seemed impossible to predict the growing importance of the World Wide Web in the near future. In fact, most advancements of the Internet that are now inseparable from our daily use did not exist at the time (Google was established in 1998, followed by other search engines).[73] Without a doubt, global impact of the Internet not only complicated the application of the Data Protection Directive, but brought the issue of balancing freedom of expression and the right to privacy to another level. Both rights are constantly being redefined in the online world and the states are attempting to follow up with respective standards and legal framework.

Since the 1995 Directive lays out current data protection rules, it has been interpreted and applied in practice in numerous cases. Without a doubt the most outstanding case that changed the way we perceive the right to erasure and introduced the right to be forgotten, is *Google Spain v AEPD and Mario Costeja Gonzalez (2014).*[74] In 2009 a Spanish citizen Mario Costeja filed a complaint to the local newspaper that published an article about the auction of property that was being sold due to social security debts. Since one of the repossessed properties belonged to him, every time someone searched for his name on Google Search the article from 1998 appeared as the first entry. Costeja argued that the sale of his house occurred years ago and that the issue had already been resolved for a long period of time, therefore that information was no longer relevant. In the meantime, the presence of the article and its association with him infringed his right to privacy and continued damaging his reputation. The newspaper refused to remove the publication, justifying it with the fact that as the article was published

[72] Directive (EU) 95/46/EC On the protection of individuals with regard to the processing of personal data and on the free movement of such data of the European Parliament and of the Council. 1995.
[73] G. Vassall-Adams, 'Case comment: Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos, Mario Costeja González' (2014) <https://eutopialaw.com/2014/05/16/case-comment-google-spain-sl-google-inc-v-agencia-espanola-de-proteccion-de-datos-mario-costeja-gonzalez/> accessed 13 July 2017.
[74] *Google Spain SL, Google Inc. v AEPD and Mario Costeja Gonzalez,* C - 131 /12, CJEU (2014).

on the order of the Spanish Ministry of Labour and Social Affairs, its removal was not possible. The following year Costeja contacted Google Spain with a request to delete the link to the publication. The company referred the complaint to the head office, Google Inc., which was responsible for the search engine. Following the dispute with Google, Costeja filed a complaint to the Spanish Agency of Data Protection (Agencia Española de Protección de Datos, AEPD), requesting the removal or alteration of the article in the La Vanguardia newspaper and removal or concealing of his personal data from Google Spain and Google Inc. The AEPD rejected the complaint concerning La Vanguardia, which benefitted from the journalistic exception under the Directive, and ruled that Google Spain and Google Inc. must remove or block search results in respect of Costeja. Both companies initiated legal action in National High Court (Audiencia Nacional), which subsequently reached the Court of Justice of the European Union (CJEU).

The main questions that were set out before the Court considered: whether the EU Data Protection Directive applied to Google and other search engines (since the company was based in the United States, but had a subsidiary in Spain, it was necessary to establish the territorial scope of the Directive); whether EU data protection laws apply to search engines and what responsibilities do they have as data controllers; whether "*the right to be forgotten*" exists under the current Directive.[75] The Court ruling was unexpected for most tech giants and set a precedent for the future application of the right to oblivion. The CJEU decision reasoned that although physical servers of Google Spain were not located in Europe, EU laws are applicable to search engine operators in cases when they have a subsidiary or a branch located in one of the Member States, as long as their advertising space is inseparably linked with the one on a global level.[76] Moreover, since Google is a data controller, it maintains the responsibilities under the 1995 Directive. Respectively, besides the EU data protection law, the right to be forgotten is also applicable.[77] Regarding the right to oblivion, the Court rules that under certain conditions individuals have the right to request search engines to remove links to pages containing their personal data. This right could be applied when such data is "*inaccurate, inadequate, irrelevant or excessive*"[78] for the

[75] 'Factsheet On The "Right To Be Forgotten" Ruling (C-131/12)' (2017) <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf> accessed 14 July 2017.
[76] G. Vassall-Adams, 'Case comment: Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos, Mario Costeja González' (2014) <https://eutopialaw.com/2014/05/16/case-comment-google-spain-sl-google-inc-v-agencia-espanola-de-proteccion-de-datos-mario-costeja-gonzalez/> accessed 13 July 2017.
[77] 'Factsheet On The "Right To Be Forgotten" Ruling (C-131/12)' (2017) <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf> accessed 14 July 2017.
[78] *Google Spain SL, Google Inc. v AEPD and Mario Costeja Gonzalez,* C - 131 /12, CJEU (2014). Para 93.

purposes of processing.[79] In the case of Mario Costeja, the Court recognised his right to the erasure of the links referring to information and ruled that Google and other search engines were obliged to remove links to personal data when the subject of this data filed a justified request. This landmark ruling had confirmed the existence of the right to be forgotten and applied it in practice. Nevertheless, the Court clarified that the right to be forgotten is not absolute and will always have to be considered on a case-by-case basis due to the balancing of the freedom of expression with other human rights.[80]

Recognising the importance of updating current legal framework, the European Commission, the Council of the European Union and the European Parliament initiated the General Data Protection Regulation, which is indeed the most important change in the data protection field in the last 20 years. The document not only aimed to modernise the EU data protection rules, it also clarified certain provisions of the EU Data Protection Directive that could be interpreted broadly and therefore provide a number of loopholes. One of the provisions was the right to erasure, which after the *Costeja* case needed to be updated for the digital age. Therefore, the proposed data protection regulation did not introduce the right to be forgotten but rather clarified the concept that had already existed. The new GDPR had various proposals before it was adopted by the European Parliament in 2016 (the Regulation comes into force in May 2018). The right to be forgotten, primarily proposed by the Commission in Article 17 of the GDPR, brings a new perspective to the existing right to erasure.[81] Since the application of the right in practice appears to be problematic for individuals, the proposed regulation reverses the burden of proof. Thus, instead of an individual having the responsibility to provide proof that their personal data should be removed, the companies are required to prove that such data cannot be deleted due to its necessity or relevance.[82] Similarly to the Data Protection Directive, the GDPR provides data controllers with an obligation to take all *reasonable steps* to notify third parties that data subjects want their information to be erased. Moreover, the controller is obliged to guarantee the data erasure. If the 1995 Directive was not specific regarding the application of the right to erasure to non-European companies and search engines, Article 3 of the GDPR sheds light on the issue with *extraterritorial applicability:*

[79] 'Factsheet On The "Right To Be Forgotten" Ruling (C-131/12)' (2017) <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf> accessed 14 July 2017.
[80] 'Factsheet On The "Right To Be Forgotten" Ruling (C-131/12)' (2017) <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf> accessed 14 July 2017.
[81] Regulation (EU) 2016/679 On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016. p.119/43-44.
[82] 'Factsheet On The "Right To Be Forgotten" Ruling (C-131/12)' (2017) <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf> accessed 14 July 2017.

whenever companies outside of Europe provide their services to consumers within the EU, European laws are applied.[83] Nevertheless, acknowledging the conflict between the fundamental rights of privacy and freedom of expression, the draftsmen emphasised that the right to be forgotten, when applied, should always balance the rights of the data subject against the "*the public interest in the availability of the data*".[84] According to the GDPR, an individual has a right to erase personal data when certain conditions are met: the data is no longer relevant in respect to the purposes it has been collected for or further processed, or the data subject withdraws the consent.

Three years after the Court of Justice of the European Union established the right to be forgotten to be legally binding in all EU states, most Member States have unanimously expressed their approval. However, the United Kingdom has repeatedly condemned this data protection policy. Even though the House of Lords committee referred to the right to be forgotten as "unreasonable, unworkable and wrong"[85], their position had little to no influence in the United Kingdom or EU. After the historical *Costeja* decision, thousands of individuals across Europe claimed their rights and requested search engines to remove links to their private information (up to July 2017 Google alone received more than *586,926* requests).[86] With less than a half of the total number of requests being satisfied[87], the right to be forgotten proves to be particularly complicated to apply in practice. Existing regulation of the right appears to be remarkably vague, thus posing a challenge to data subjects, who wish their personal data to be removed. Meanwhile, the growing amount of case law and requests to search engines in Europe and all around the world demonstrate the relevance of the right to be forgotten strengthening the rights of data subjects in protection of their information. Besides numerous requests in the European Union, where the right is applicable, the right to be forgotten started a forest fire of debates reaching countries all across the globe. States like Argentina, India, South Korea, and South Africa have already had court decisions ruling in support of the right to be forgotten in uncharacteristic cases. Naturally, there are alternative views contradicting the regulation and implementation of the right to oblivion. While the

[83] Regulation (EU) 2016/679 p.119/32-33.
[84] GDPR Portal, 'GDPR Key Changes' (n.d.) <http://www.eugdpr.org/key-changes.html> accessed 13 July 2017.
[85] J. Temperton, 'Unelected peers: EU right to be forgotten is 'unreasonable, unworkable and wrong'' (2014) <http://www.expertreviews.co.uk/software/internet-security/1400843/unelected-peers-eu-right-to-be-forgotten-is-unreasonable> accessed 13 July 2017.
[86] 'Transparency Report. European privacy requests for search removals ' (2017) <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en-US> accessed 13 July 2017.
[87] Some resources suggest that in 2016 75% of request of the right to be forgotten have been denied by Google. G. Sterling , 'Report: 2 years in, 75 percent of Right to Be Forgotten asks denied by Google' (2016) <http://searchengineland.com/report-2-years-75-percent-right-forgotten-asks-denied-google-249424> accessed 13 July 2017.

United States believes that the concept is a pitfall for the freedom of expression and media and is simply a new tool of censorship, China has a different data protection regime that is incompatible with the right. The Supreme Court of Japan has made a statement in one of its decisions, that, in comparison to the European data protection rules, "*any decision to delete information from search results should prioritise the public's right to information*"**,**[88] thus seeing the right to erasure from another perspective.

CHAPTER II. THE REACH OF THE RIGHT TO BE FORGOTTEN

2.1. Types of Information Applicable. Sensitive Information, Public and Criminal Records.

Considering that the main objective of the right to oblivion is to protect data subjects' privacy through removal of links to certain information in the Web search under specific conditions, the type of aforementioned data is of a crucial importance to the matter. Both current and proposed legal frameworks (1995 Directive and GDPR) provide that individuals have a right to request their personal data to be removed when it is *inaccurate, inadequate, irrelevant or excessive.*[89] But what kind of personal data could be desired to be removed once it satisfies those criteria? The records of hundreds of thousands of requests of removal filed to search engines, companies, media platforms, domestic and supranational courts suggest that the array of the sensitive personal data that has been made public is greatly diverse.

The definition of "*sensitive personal information*" varies among the legal systems, but generally includes personally identifiable information that could be associated with an individual: name, date and place of birth, address or any form of contact information, government-issued identification number or other identity documents, medical records, biometric data, political affiliation, religious views, bank account numbers, employment history, sexual life and criminal records.[90] As the CJEU stated, all cases have to be assessed on the case-by-case basis, therefore in each instance the decision-making bodies will have to take into account the relevance, accuracy, adequacy of information and proportionality between

[88] Reuters, 'Japanese court rejects demand to remove web search result - media' (2017) <http://www.reuters.com/article/google-japan-privacy-idUSL4N1FM24D> accessed 13 July 2017.
[89] *Google Spain SL, Google Inc. v AEPD and Mario Costeja Gonzalez,* C - 131 /12, CJEU (2014). Para 93.
[90] G. Stevens, '*Data Security Breach Notification Laws', Congressional Research Service,* 2012. 23. p.6.

the erasure of information and public interest that it poses. In addition, special attention should be drawn to data, the processing of which is necessary for archival and statistical research[91] and journalistic purposes, as well as the one that constitutes the works of art or literary accomplishments.[92]

Statistically, besides the usual requests to erase data that does not have any impact on anyone besides the individual (personal pictures etc.), the requests to remove nonconsensual pornography, or so-called revenge porn, are being consistently satisfied.[93] Tech corporations, such as Google, Facebook and Twitter are highly responsive to such vulgar and slandering practices.[94] The companies tend to assume larger roles in the issue and de-list the links once they are reported by users.

Particular types of information appear to be considerably controversial. Data that has been obtained in accordance with the law by public authorities for specific purposes, such as various public records, is often argued to be that of public interest, making the possibility of its removal more complicated (excluding the exceptions when there are legal or personal safety deliberations). For instance, information obtained in order to engage in trade or business activity is collected by respective authorities and generally published on official websites of the institution. Then the available data could be republished an infinite amount of times by intermediary websites that are visible on search engines years after the information assumingly loses its relevance. *Manni* case, the latest judgement by the CJEU on the right to be forgotten, raised a question whether the right to oblivion should be limited in respect to public records. The plaintiff, Salvatore Manni, initiated legal action against the Lecce Chamber of Commerce, demanding that records of the company, which he unsuccessfully led in 1992, be erased from an official register. Manni claimed that his current business activity had been facing difficulties as his clients performed background checks through a private company that extracted information from the public Companies Register which then resulted in their deterrence from dealing with him. Since the company in question that Mr. Manni was administrating went bankrupt more than ten years before the

[91] Bird&Bird, 'Individual rights | Right to erasure and right to restriction of processing' (2013) <https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/34--guide-to-the-gdpr--right-to-erasure-and-right-to-restriction-of-processing.pdf?la=en> accessed 14 July 2017

[92] Directive (EU) 95/46/EC On the protection of individuals with regard to the processing of personal data and on the free movement of such data of the European Parliament and of the Council. 1995.

[93] A. Truong, 'Google Is Giving Revenge Porn Victims The Right To Be Forgotten' (*Quartz*, 2015) <https://qz.com/432939/google-is-giving-revenge-porn-victims-the-right-to-be-forgotten/> accessed 14 July 2017.

[94] L. Edwards, 'Revenge porn: why the right to be forgotten is the right remedy' (2014) <https://www.theguardian.com/technology/2014/jul/29/revenge-porn-right-to-be-forgotten-house-of-lords> accessed 13 July 2017.

beginning of the proceedings, he argued that this data was no longer relevant for the purposes it had been collected for and therefore should be removed following his request. Although the Tribunale di Lecce ruled that the Chamber must anonymise the data concerning Mr. Manni and cover the damages he had suffered, when the case reached CJEU the Court had a contrasting opinion.[95] The Court emphasised the role of the public nature of company registers, noting that their main purpose is to safeguard the legal assurance among companies and third parties, as commonly it is their assets that are the only type of certainty that limited liability companies and joint stock companies provide.[96] Subsequently, the Court found that the limitation of access of the third parties that have a legitimate interest in obtaining such information would not be justified in this particular case, and thus the interference with the private data of Mr. Manni was not disproportionate, taking into account the nature of the register and the limited amount of personal data that was present in the Companies Register.[97] Therefore, the Court created a precedent, imposing limitations to the right to be forgotten when personal data is a part of public records.

Another highly controversial type of personal data are criminal records: arrests, spent and amnestied convictions. In numerous states' practices the rehabilitation of convicted individuals who have served their sentence is a policy that deserves special attention. In the era of new technology no criminal conviction can remain private no matter how trivial. It is common that once a convict's sentence is served and legal rehabilitation is received they face stigmas and discrimination in many fields of society: education, employment, traveling, participating in civil society and even obtaining insurance.[98] Although existing state policies attempt to integrate convicted persons back into society, the main problems they face cannot be dealt with so easily. The so-called "*Google effect*" leads to information regarding criminal offences being easily accessible to Internet users for many years. Unofficially, 75% of employers Google search their applicants and discriminate on the basis of a criminal record.[99] Even though the conviction has been rehabilitated in the eyes of the law for many years, convicted individuals will face its consequences as long as this information is public. In 1986 an incident of this nature caused

[95] Press Release. (EU) 27/17 Court of Justice of the European Union. 2017.
[96] *Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni,* C-398/15, CJEU (2017). Para 50 and 60.
[97] Press Release. (EU) 27/17 Court of Justice of the European Union. 2017.
[98] C. Stacey, 'The Google effect – Criminal records and the 'right to be forgotten'' (2015) <https://www.ejiltalk.org/extraterritohttps://www.linkedin.com/pulse/google-effect-criminal-records-right-forgotten-stacey-llb-llmriality-and-the-fundamental-right-to-data-protection/> accessed 13 July 2017.
[99] *Ibid.*.

Juan Matamoros to suffer a subsequent life of distress, social stigma and missed employment opportunities. More than 30 years ago Matamoros was driving home from a soiree with the friends in Florida, USA. The intense need to use the bathroom forced him to stop on the side of the road, which led him to being arrested by the officer for public urination and sentenced to jail, being labeled as a sex offender. Decades after serving his sentence, Matamoros and his family have been ordered to move out of their house due to its proximity to three city parks and one child-care facility (being registered as a sex offender, he violated an ordinance approved by the local city officials).[100] Now, applying the Google effect, Juan Matamoros will be a victim of this conviction for the rest of his life. Naturally, it could be considered justified for convicted criminals to be able to request the removal of this data from mass media and Google search under certain circumstances.

Nevertheless, some criminal cases are more sensitive and require special attention, taking both, the rehabilitation of the offender and personal safety of former or possible victims, into account. For instance, positions that are exposed to interactions or close proximity to the vulnerable groups or children, have a reason of making the disclosure of past convictions obligatory, even if the individual has served the penalty according to the law. Unofficial records suggest that approximately 12% of all right to be forgotten requests are related to child molestation and pornography, while 20% are based on past convictions and arrests and 30% associated with fraud activity.[101] In cases when a person was wrongfully convicted or it has been a minor offence, the public accessibility of information concerning the arrest or conviction of the individual might not be considered relevant after a certain period of time, and individuals could enjoy starting their life from a clean slate. But what if convicted criminals, who committed violent crimes or molested children, were allowed to completely clean up their records and past atrocities on the Web? Imagine a convicted child abuser starting a job in a day care or moving in a house next door to a children's playground? Do the parents have a right to know? As has been established by the Court, every case should balance the rights of an individual against the public right to know or public interest. People change and justice systems around the world regard that everyone deserves a second chance to rehabilitate. Nevertheless, safety and wellbeing of others will have to be taken into account as well. In 2016, a Japanese court ruled a first ever case on the right to be forgotten,

[100] D. Balona and R. Mahoney, 'Long-ago charge to cost man his home' (2007) <http://articles.orlandosentinel.com/2007-03-21/news/VOFFENDER21_1_matamoros-deltona-incident> accessed 13 July 2017.
[101] B. Robinson, 'Is this the end of the internet as we know it? Thousands rush to apply for their 'right to be forgotten' by having details of their past erased from Google ' (2014) <http://www.dailymail.co.uk/news/article-2644578/Thousands-paedophiles-apply-Google-right-forgotten.html> accessed 14 July 2017.

ordering Google to remove search results connected to three year old articles about a man who has been arrested in relation to child pornography and prostitution charges.[102] The Court stated that the plaintiff deserved to restore his life and enjoy an "*unhindered*" rehabilitation.[103] The controversial case sparked numerous debates on how erasing information on the Internet is potentially dangerous and damaging for individuals and society as a whole. Mass media has been speculating over the possibility that the CJEU ruling opened the doors to history alteration and provided an opportunity to individuals to cover up their "dirty" past. With businesses hiding previous fraud scandals, doctors erasing unflattering revues about their practices and pedophiles removing information about child abuse, the world would be become a much more risky and hazardous place to live. Notwithstanding, the society has to understand that the right to be forgotten is indeed not absolute or an automatic removal of content. Each request is being examined on a case-by-case basis, taking all factors of particular situations into account and applying the proportionality principle. The main objective of the concept is to forget information when it is no longer relevant and necessary and its public accessibility is violating the rights of individuals. The European Commission assures that "*the right to be forgotten is certainly not about making prominent people less prominent or making criminals less criminal*".[104]

2.2. Groups of Individuals. From the Masses to Public Figures.

It is without a doubt that the application and consequences of the right to be forgotten vary depending on the group of individuals the data subject is attributed to. In particular, the application of the right may differ on the grounds of the level of privacy a person may reasonably expect. Hence, there is a considerable distinction between the extent of privacy enjoyed by public and private figures. Moreover, the consequences of erasure of information about certain groups of individuals, that are of a public interest, could be more influential and damaging when it comes to preserving historical record and controlling the perceptions of the public.

[102] The decision has been further appealed by Google.
[103] J. McCurry , 'Japan recognises 'right to be forgotten' of man convicted of child sex offences ' (2016) <https://www.theguardian.com/technology/2016/mar/01/japan-recognises-right-to-be-forgotten-of-man-convicted-of-child-sex-offences> accessed 13 July 2017.
[104] 'Factsheet On The "Right To Be Forgotten" Ruling (C-131/12)' (2017) <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf> accessed 14 July 2017.

Most jurisdictions provide characteristical distinction between "*public figure doctrine*", also referred as "*figures of contemporary history*" in German-speaking jurisdictions, and private figures. Antoon De Baets suggests that it is helpful to subdivide the first type into absolute and relative public figures. Such distinction could be performed with an evaluation of the person's position in society, level of public interest he/she represents and the scope of personal rights the figure enjoys.[105] *Absolute public figures* are individuals, who "*stand out from the masses due to their exceptional behaviour or particular roles*".[106] These types of public figures are well-known outside of any kind of context or particular event as a result of their status, pertinence or role played in the society.[107] For instance, heads of states, royal families and celebrities all fall under this category. When it comes to the protection of privacy of absolute public figures, the matter happens to be more complicated due to defining the extent of privacy they enjoy. The courts around the world have justified that in certain circumstances public figures waiver their privacy with their voluntary public appearances or the positions they occupy, when there are legitimate public concerns present.[108] It is the public interest that often overweighs the privacy of individuals, and in cases of public figures this interest is far greater. Therefore, it appears to be far more complex to guarantee the enjoyment of the the right to be forgotten by such individuals, since it would be harder to balance their privacy rights against the public right to know. The extensive case law does not provide a dominating opinion on the protection of the right to privacy of public figures. Despite the existing tendency of common-law jurisdictions defending freedom of expression in conflicts with the right to privacy, and civil-law states doing the opposite,[109] it is typical that there are discrepancies in the practice even within the same state. For instance, in the case of American film actress Pamela Anderson based on the sex videotape scandal that occurred in 1998, the Court limited her privacy, stating that her deliberate effort to become famous made her a "*voluntary figure*".[110] When Anderson and her then-partner initiated a legal action against Paramount and Internet Entertainment Group, known as IEG, for broadcasting a segment that included eight segments of their private tape, the celebrities were looking

[105] A. Koltay, 'Elements of Protecting the Reputation of Public Figures in European Legal Systems' [2013] (p.59) eltelawjournal_2013/1. <http://eltelawjournal.hu/elements-of-protecting-the-reputation-of-public-figures-in-european-legal-systems/> accessed 14 July 2017.
[106] *Ibid.*.
[107] *Ibid.*.
[108] S. Choul Hong, 'Kids Sell: Celebrity Kids' Right to Privacy', Department of Journalism & Communication, Kyonggi University, Seoul 120-702. 2015. p. 2.
[109] A. De Baets, 'A Historian'S View On The Right To Be Forgotten', International Review of Law, Computers & Technology. 2016. P. 59.
[110] *Michaels v Internet Entertainment Group,* CV 98-0583 DDP, United States District Court for the Central District of California (1998).

for a compensation for the infringement of their right to privacy. Nevertheless, the Court considered that even if there was no particular social value of adding the parts of the videotape to the segment, it has been reasonably expected that the public would have a legitimate interest in the story featuring the plaintiffs.[111] While in this case the Court confirmed that absolute public figures have a rather limited exercise of the right to privacy, another US court applied a different approach to the privacy issues of Jacqueline Onassis, the widow of assassinated US President John F. Kennedy.[112] Mrs. Onassis had a counterclaim for the invasion of privacy on the behalf of herself and her children, when Ronald Galella, a renowned paparazzo, filed a suit against her on the grounds of unlawful arrest and interference with his business activity. The extensive conflict between the parties was based on the actions of Mr. Galella, who repeatedly appeared at the school of her children, came within a dangerous proximity when the plaintiff was swimming, blocked Mrs. Onassis's way when she was getting into a taxi, and even jumped in front of the bicycle her son was riding. All in order to take pictures of Jacqueline and the children and sell the images to the media. During the last incident with her son's bicycle, the Secret Service reacted to the danger posed to the child and arrested Galella, which he claimed to be unlawful. In the decision the Court clarified that although Mrs. Onassis was a public figure, and thus the public had a legitimate interest in the life of her family, which respectively allowed certain level of intrusion to their privacy, the actions of Mr. Galella "*went far beyond the reasonable bounds of news gathering. When weighed against the de minimis public importance of the daily activities of the defendant, Galella's constant surveillance, his obtrusive and intruding presence, was unwarranted and unreasonable*".[113] Consequently, Mrs. Onassis and her children suffered an unproportionate interference with their right to privacy and Galella was imposed to pay the fine and faced far more severe restrictions on getting within close proximity to Onassis and her children, than the previous violated restraining order.[114] Taking into account the challenge of balancing freedom of expression and privacy of individuals, it is clear there is no common approach to determining the extent of privacy absolute public figures may reasonably expect, *i.e*., the exercising of the right to be forgotten by absolute public figures will have a different application of the proportionality principle, taken that the public interest acquires a greater value and waivers privacy rights of such individuals to a certain extent. Moreover, the tremendous amount of the

[111] S. Choul Hong, 'Kids Sell: Celebrity Kids' Right to Privacy', Department of Journalism & Communication, Kyonggi University, Seoul 120-702. 2015. p. 4
[112] *Galella v Onassis* , 353 F. Supp. 196, U.S. District Court for the Southern District of New York (1972).
[113] D. L. Hudson, *The Right to Privacy* (Infobase Publishing). 2009. p.50.
[114] *Galella v Onassis* , 353 F. Supp. 196, U.S. District Court for the Southern District of New York (1972).

available information concerning absolute public figures could be another challenge for the application of the right to oblivion, given that the data often appears in numerous sources.

Another type of public figures is usually referred to as *relative public figures* (relative figures of contemporary society). This group of individuals is known to the general public due a particular event in contemporary history, often crimes or trials. Typically, relative public figures are well known for a certain period of time, shortly after the distinguished event they are associated with. Thus, criminals, judges, victims, and even their families fall under this category during the sensation period of the trial etc. In fact, families of absolute public figures are also exposed to media attention and could be considered as a relative public figures, since they gain their fame from the connection with the latter.[115] Considering that such individuals have previously lead a private life, their privacy rights could be limited only during the period of their new-found "fame", and possibly further on in the connection with that particular event. The main justified reasons of the interference with their private life are newsworthiness and public interest.[116] The exercise of the right to be forgotten by relative public figures could affect the flow of history in a different way than absolute public figures. If the latter have an excessive amount of information available for preserving historical records and writing their biographies, if, theoretically speaking, relative public figures erased all the references to them in the past, although it would not have a substantial influence on the progress of scholarship, the history of everyday life and social-economic history would cease to exist due to the lack of resources.[117] The aforementioned studies focus on the accumulated data and statistical research, rather than dossiers of individuals. In order to analyse and/or predict predominant patterns and trends in society, historians and analysts conduct the research using the information that is publicly available. Therefore, finding out tendencies that cause or perpetuate a particular crime, for instance corruption, in order to deter it, would be problematic if statistical data would not be accurate due to numerous erasures and alterations. Thus, the consideration of newsworthiness and input to the public debate and academic field in cases involving relative public figures, could potentially justify the interference with their privacy, making the right to be forgotten harder or almost impossible to apply.

[115] A. Koltay, 'Elements of Protecting the Reputation of Public Figures in European Legal Systems' [2013] (p.59) eltelawjournal_2013/1. <http://eltelawjournal.hu/elements-of-protecting-the-reputation-of-public-figures-in-european-legal-systems/> accessed 14 July 2017.
[116] A. De Baets, 'A Historian'S View On The Right To Be Forgotten'. International Review of Law, Computers & Technology. 2016. p. 60.
[117] *Ibid.* p. 60.

Private figures are indeed the largest group of individuals that are not well known to the general public. Legal doctrine provides a higher protection of privacy of private persons, given that their behaviour and actions demonstrate a will to retain their life private. Other unofficial sources suggest that 95% of all requests to erase information submitted to Google are not from public figures or criminals, but rather common citizens.[118] The individuals expressed their concern mostly to the violation of privacy by their private data being currently publicly available. According to Google Interactive Transparency Report, the top ten domains, which have been affected the most by the removal of the requested URLs (Uniform Resource Locator, known as the web address) include social media platforms, such as Facebook, Twitter, Youtube, Google Plus and Badoo.[119] The numbers demonstrate that the majority of links that have been de-listed are from the websites with user generated content, rather than mass media websites. Thus, one can make an observation that current application of the right to be forgotten is covering mostly private figures who wish to remove their private data that has been posted by themselves or third parties from the Web search. Without a doubt, a higher protection of privacy of common individuals provided by law increases the chances of private persons having their request satisfied, making the right to oblivion easier to exercise.

An interesting question arises when the data subject is deceased and cannot protect his/her right to privacy anymore. Although discussing the right to privacy of the dead may seem absurd at first glance, since the individual is no longer alive and thus doesn't possess any rights as such, there is an ongoing debate on the existence of *posthumous privacy*. In particular, the application of certain restrictions on the public disclosure of information about them is often discussed to be the "*right of the dead*".[120] Common-law jurisdictions are rather strict with the application of *actio personalis moritur cum persona* (a personal action dies with the person), compared to civil-law jurisdictions that protect posthumous privacy. Typically, it is assumed that the posthumous privacy of a private person amounts to approximately 70 years, while deceased public figures may enjoy the right for weeks or even days. Nevertheless, there is a great distinction between the duration of such privacy and the duration of its

[118] S.Tippmann and Julia Powles, 'Google accidentally reveals data on 'right to be forgotten' requests ' (2015) <https://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests> accessed 13 July 2017.
[119] ' Transparency Report. European privacy requests for search removals ' (2017) <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en-US> accessed 13 July 2017.
[120] A. De Baets, 'A Historian'S View On The Right To Be Forgotten'. International Review of Law, Computers & Technology. 2016. p. 63.

legal protection.[121] The period of legal protection of posthumous privacy is commonly much shorter due to the fact that the argument for disclosure of the data is balancing out non-disclosure considerations far greater than in cases with living individuals.[122] This controversy suggests a logical question: Can the right to be forgotten be applied to the dead? And more importantly, what could justify the application of this right to the deceased? The incident that happened in the USA in 2006 illustrates why such right could be beneficial to the family and the reputation of the dead. When 19 years-old Nicole Castouras lost her life in a traffic accident, Highway Patrol in California arrived at the scene and routinely took pictures of the examination of the decapitated body. The photographs were later leaked by a member the Highway Patrol, who posted them online on Halloween for his friends to see. Gruesome images have sparked curiosity over the Web and have been reposted thousands of times. The grieving family of the young woman started a legal action against the California Highway Patrol and Google, asking for damages for the negligence and intentional infliction of emotional distress and requesting the search engine to de-link the pages that contained the photographs. Six years after the beginning of the legal battle the family received the damages from the law enforcement agency.[123] Nevertheless, the claim against Google has not been satisfied, as the First Amendment conflicts with erasing and altering the content on the Internet.[124] The photographs of Nicole's dead body appear on the Web search of her name up until this day. From an ethical point of view, should the right to be forgotten be applied in cases like this? European practice suggests that, in fact, in certain circumstances it can be exercised by the relatives of the deceased or even anonymous applicants. In 2014 Google de-listed a link to the article in the Telegraph featuring a deceased pensioner, whose body has been found by her neighbors six months after she died. After receiving an anonymous request, Google removed the links, since it fell under the European right to be forgotten. (Ironically, the Telegraph published another article highlighting the de-listing of the links to the publication about the deceased woman, mentioning her name and including the link to the article still available on their website).[125] Therefore, the European approach to the right to oblivion includes the deceased data subjects in practice and individuals have an opportunity to request to remove the links to personal data of the dead.

---

[121] *Ibid*. p. 63.
[122] *Ibid*. p. 63.
[123] A. Gauberti., 'How To Remove Links About Dead People From Google' (*Crefovi*, 2017) <http://crefovi.com/articles/remove-links-dead-people-google-right-forgotten-deceased/> accessed 14 July 2017.
[124] G. Brock, *The Right to be Forgotten: Privacy and the Media in the Digital Age*, I.B.Tauris, 160. 2016. Extract. p.7.
[125] R. Williams, 'Google removes link to Telegraph story on deceased pensioner' (2014) <http://www.telegraph.co.uk/technology/google/11060606/Google-removes-link-to-Telegraph-story-on-deceased-pensioner.html> accessed 13 July 2017.

From another perspective, the profession of an individual who desires their private data being erased might have significant relevance due to the moral and practical consequences of the removal of data connected to their professional activity. For instance, doctors and other medical personnel often have reviews available online, not to mention the publications in the media in scandalous cases. Although under current EU legislation they have the right to oblivion and may request negative feedback or criticism being removed from the search engines or original sources, if that data is considered irrelevant, inadequate, inaccurate or excessive, the consequences of their removal from the Web will highly affect the perception of the public regarding their services. Thus, instead of being able to read the reviews on the doctor's practice and decide themselves if they would like to visit that particular specialist, the patients would be deprived of such opportunity. Although providing the doctors an opportunity to restore their reputation is certainly beneficial for their careers, many argue that the public has the right to know about their previous negligence or legal battles connected to their practice.[126] Similar opinions could be found regarding other professions as well: bankers, lawyers, child care specialist etc. Nevertheless, being the last instance bodies, it is the courts that are faced with a dilemma of how to balance these concerns and the public right to know against the right to privacy of the aforementioned individuals. In certain cases the link to the profession and the period of time that has passed since the publication would be an extra lever to determining if this data remains relevant up till today.

2.3. Types of Sources of Information.

Going back to the 1995 Data Protection Directive, the EU legislation focused more on data minimisation and provided individuals with a right to rectify and erase information under certain conditions. Being adopted almost at the beginning of the rapid development of the technological era, the document focused on the possibility of erasing documented information, rather than the one accessible on the World Wide Web (search engines and social media platforms did not exist at the time, and therefore did not create an

[126] K. Pollard, 'Has the EU Given Doctors the "Right to be Forgotten" When Medical Tourism Goes Wrong?' (2014) <https://www.imtj.com/blog/has-eu-given-doctors-right-be-forgotten-when-medical-tourism-goes-wrong/> accessed 13 July 2017.

issue for the protection of personal data). Hence, the Directive had in mind the actual sources of information, be that books, journals, public records or local newspapers archive. The document did not specify what kind of private data would fall under the scope of the Article 12(b) or what the origins of the data was. Meaning, that without detailed provisions specifying which sources of information the article should apply, it is up to the Court to interpret it and create precedents (also provide the exceptions of sources that could not be rectified nor censored). Naturally, the interference with the original sources happens to be more controversial in terms of potential censorship or re-writing history. Thus, every intrusion with the freedom of expression and the public right to know should be carefully balanced on a case-by-case basis.

Global impact of the Internet and new methods of sharing and storing information brought about a new dimension to the European right to erasure. Since the Directive no longer adequately covered new issues of data protection arising online, the CJEU first interpreted the right to be forgotten in 2014 in *Costeja* case, spreading the definition of "data controller" to search engines and thus holding accountable not only the subsidiaries of search giants that are registered in Europe, but also the companies abroad if they operate in the EU Member States.[127] Accordingly, the new extension of the right to erasure — the right to be forgotten — had its focal point on data protection in the online environment, targeting online sources and search results, rather than original sources of the information. The paradigm shift in data protection required new regulation, which has been addressed by the Commission of the European Union when it proposed the General Data Protection Regulation.[128] Subsequently, the Regulation expanded the notion of data controller and clarified the application of data erasure in the online world (GDPR enters into force in May 2018). It is worth pointing out that if the right to erasure covered the removal of private data from sources, the right to be forgotten protects the privacy of individuals by de-listing links to the sources of private data rather than deleting the original information. Google's senior vice-president for corporate development and chief legal officer, David Drummond, compared the process to taking a certain book out of the library catalogue instead of destroying the book itself.[129] This way the information will not be completely erased, but it becomes much harder to find and access it.

[127] *Google Spain SL, Google Inc. v AEPD and Mario Costeja Gonzalez,* C - 131 /12, CJEU (2014).
[128] Regulation (EU) 2016/679 On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016.
[129] D. Drummond, 'We need to talk about the right to be forgotten ' (2014) <https://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate> accessed 13 July 2017.

Respectively, the current discourse of the application of the right to be forgotten involves only online resources and their rectification. Both academic rhetoric and political debates underline the importance of regulating the online flow of data and establishing the scope of rights of the Internet users concerning the protection of their private data. Thus, current development of data protection on regional and international levels focuses on regulating new methods of data transmission and users regaining control over the data they have made public themselves or which has been published by third parties.

Since the right to be forgotten presently occupies with de-listing information from the Web search, it is necessary to take into account the worldwide versions of search engines and ones on a local level. For instance, if an Italian court rules that certain links should be removed from Google search, and Google, when complying with the judgement, de-lists the links on Google.it, the information could still be found on the global search Google.com and other national domains, to which users from the majority of countries have access. This way the effectiveness of the removal is limited and the data may have the same impact on the privacy of the individual as before the ruling. Such a conflict arose in France when the Commission Nationale de l'Informatique et des Libertes (CNIL) fined Google for not de-listing the links to the data, as ordered by the right to oblivion ruling, worldwide, but only on local domains Google.de and Google.fr. Google appealed to the France's highest court arguing that "*no one country should have the authority to control the content someone in the second country can access*".[130] The company emphasised that making the search engine comply with the right to be forgotten globally would set a dangerous precedent for other, not always democratic, states, which could therefore request the information being deleted worldwide.[131] This possibility would indeed have tremendous consequences for the adequacy of historical records and freedom of speech in many states. Although the 1995 Directive has *no territorial restrictions*, the application of the right to be forgotten in other jurisdictions, especially the ones that do not even recognise the right, would be highly controversial.

2.4. The Right to be Forgotten Enforcement. Mechanisms of Processing Requests.

[130] P. Fleischer, 'Implementing a European, not global, right to be forgotten' (2015) <https://europe.googleblog.com/2015/07/implementing-european-not-global-right.html> accessed 13 July 2017.
[131] *Ibid.*

Current EU legal framework on the right to oblivion provides an utterly ambiguous mechanism of its enforcement. The European Commission outlines that once individuals desire certain private data of theirs to be erased from the Web search, the first step they should take is to file a request to the respective search engine. Thus, a person who is not satisfied with search results that appear upon the inquiry of their name may address tech giants with a request to de-list individual links. Following the reception of the requests, search engines are required to assess each of them on a case-by-case basis, complying with the criteria set out by the Court of Justice of the European Union and the EU legal framework,[132] and determining whether the personal data is inaccurate, inadequate, irrelevant or excessive for processing purposes.[133] Upon the assessment of all facts of the request, including the type of data that is being displayed, the identity of the individual in question, the period of time that passed after the publication of the material, and, most importantly, the public interest involved in that particular private data remaining public, search engines will apply the proportionality principle established by the Court (proportionality of respective links in respect to the purposes of data processing or purposes for which this data has been collected).[134] Once the company has made the decision, they may rather de-list the requested links to private data or deny the request. The request may not be satisfied if it did not fall within the scope of criteria mentioned in the *Costeja* case,[135] or it did not pass the proportionality test.

In cases when search engines turn down the requests, individuals have an alternative of referring the case to the national supervisory authorities responsible for the data protection or to the national courts of EU Members that will establish whether the individual may exercise the right to be forgotten.[136] The commission clarified that, "*Public authorities will be the ultimate arbiters of the application of the Right to be Forgotten*".[137]

But what could be potentially problematic in the mechanism of processing requests of the right to oblivion? First and foremost, it appears that search engines have gained a great deal of authority, given that primary responsibility to establish the outline of the right to oblivion has fallen on them. In fact,

[132] 'Factsheet On The "Right To Be Forgotten" Ruling (C-131/12)' (2017) <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf> accessed 14 July 2017.
[133] *Google Spain SL, Google Inc. v AEPD and Mario Costeja Gonzalez,* C - 131 /12, CJEU (2014).
[134] 'Factsheet On The "Right To Be Forgotten" Ruling (C-131/12)' (2017) <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf> accessed 14 July 2017.
[135] *Google Spain SL, Google Inc. v AEPD and Mario Costeja Gonzalez,* C - 131 /12, CJEU (2014).
[136] 'Factsheet On The "Right To Be Forgotten" Ruling (C-131/12)' (2017) <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf> accessed 14 July 2017.
[137] *Ibid.*

Google has been playing the most crucial role in the discourse, mainly because in 2014, the year of the landmark right to be forgotten ruling, Google covered more than 92% of the search market in Europe, while Bing (2.67%) and Yahoo! (2.34%) followed with much smaller shares (Google remains absolute dominance on the market up to this day)[138]. Being the key player on market, it is no wonder that the majority of debates concerning the implementation of the right to oblivion and how to interpret criteria of removal justification set out by the Court, have been addressed to Google.[139] Eric Schmidt, the Executive Chairman of Alphabet Inc., which is the parental company of Google and its subsidiaries, emphasised that, "*[Google] didn't ask to be the decision maker*".[140] Nevertheless, it remains to be responsible for complying with the EU legislation, and thus the right to be forgotten, being obliged to make decisions concerning thousands of requests from the European citizens. In case Google would decide to trump this responsibility, it would face an extremely large amount of fines. And since Google is massively dominating the market, the responsibility appears to be far greater than that of other search engines, given that the extent of the impact is disproportionately enormous.[141]

Edward Lee suggests that it would have been rational to expect from lawmakers a rather different approach to the implementation of the right to be forgotten. Since every EU Member has respective Data Protection Authorities (DPA), they could become the decision-making bodies that process the requests of individuals claiming the right to oblivion. Being competent in determining whether the request should be satisfied or not, the DPA would further order search engines to comply with their decisions and de-list the respective links from the search. [142]

Nevertheless, that is not the procedure that has been imposed. Instead, Google and other search engines were delegated a great deal of authority, given that they are the primary body that will be assessing all right to be forgotten claims. Since *Costeja* case did not set out clear criteria on the application of the

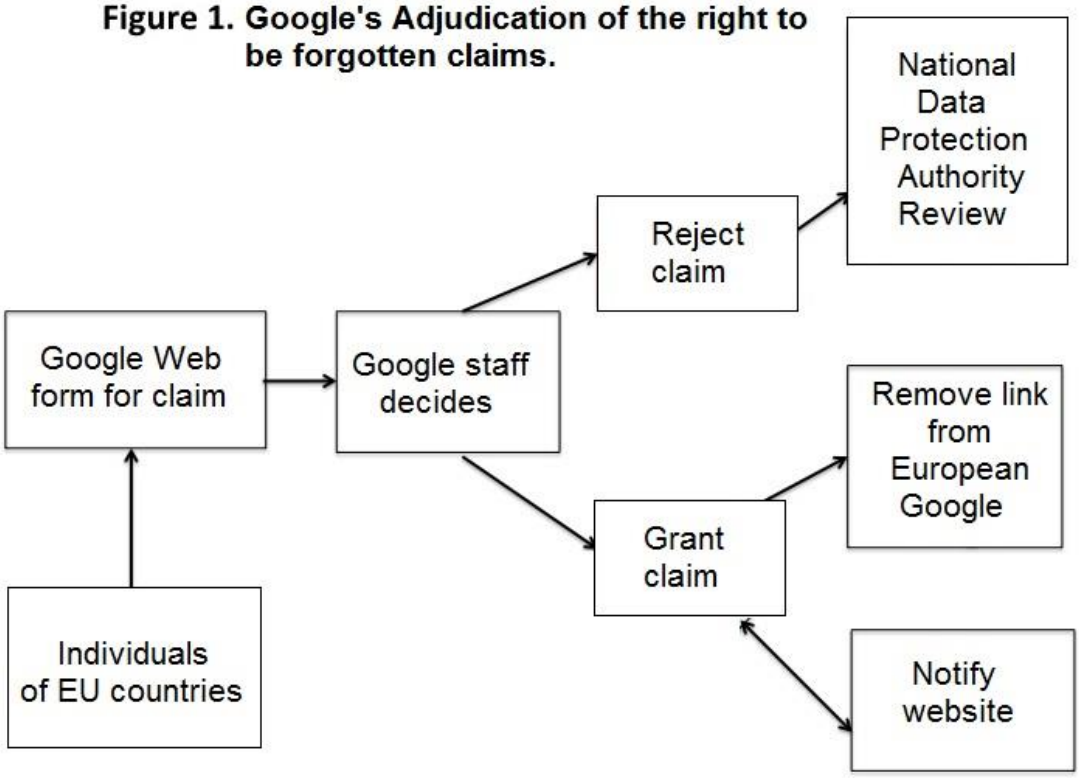
[138] As of June 2017 Google had 93.06% of search market share, while Bing - 3.19%, Yandex.ru - 1.9%, Yahoo! - 1.48%, DuckDuckGo - 0,18%. 'Search Engine Market Share In Europe | Statcounter Global Stats' (*StatCounter Global Stats*, 2017) <http://gs.statcounter.com/search-engine-market-share/all/europe> accessed 14 July 2017.
[139] E. Lee, *Recognizing Rights In Real Time: The Role Of Google In The EU Right To Be Forgotten.* 49th edn, University of California, Davis. 2017. p. 1035.
[140] A. White, 'Google EU Ruling Response Vetted As Complaints Pile Up' (2014) <http://www.bloomberg.com/news/articles/2014-09-18/google-eu-ruling-response-vetted-as-complaints-pile-up.> accessed 14 July 2017.
[141] E. Lee, *Recognizing Rights In Real Time: The Role Of Google In The EU Right To Be Forgotten.* 49th edn, University of California, Davis. 2017. P. 1035.
[142] *Ibid.*. p. 1036.

right, it is search engines that will have to define the contours of the right to oblivion on a case-by-case basis. Undoubtedly, their decision will be able to be appealed to the respective DPA and national courts. However, primary decision-making and analysis will be performed by Google, and thus concluding the vast majority of cases if they will not be further appealed.[143]

Following the *Costeja* decision, Google implemented the right to be forgotten administrative procedure (displayed in Figure 1.) shortly after the last court hearing. They introduced a Web form, which users can use in order to file the request to invoke their right to be forgotten and therefore de-list certain personal data from the search.[144] The Web form is accessible in twenty five languages and contains detailed instructions of what information should be submitted in order to file a request. Among other data, the individuals are required to submit personal information (name, email address, on whose behalf the request is filed and the relation between the applicant and the data subject, relevant documents confirming the identity of the subject of the request), country whose laws apply to this request (one of the EU Member States, since the right to be forgotten is currently implemented only in the European framework and not globally), list of the search results the data subject desires to remove (specific URLs) and detailed justification of potential removal. The form clarifies that the request should include and explanation of how the links are related to the respective data subject and why could it be considered "*unlawful, inaccurate, or outdated*".[145] Although there are no alternative ways to submit the right to be forgotten requests, Google provided and *ad hoc* procedure for applications filed otherwise than through the form (letter, fax or email).[146]

[143] E. Lee, *Recognizing Rights In Real Time: The Role Of Google In The EU Right To Be Forgotten.* 49th edn, University of California, Davis. 2017. p. 1036.
[144] *Ibid.*. p. 1038.
[145] 'EU Privacy Removal. Request removal of content indexed on Google Search based on data protection law in Europe' (n.d.) <https://accounts.google.com/ServiceLogin?service=sitemaps&passive=1209600&continue=https://www.google.com/webmasters/tools/dmca-notice?hl%3Den%26pid%3D0%26complaint_type%3D14&followup=https://www.google.com/webmasters/tools/dmca-notice?hl%3Den%26pid%3D0%26complaint_type%3D14&hl=en> accessed 13 July 2017.
[146] E. Lee, *Recognizing Rights In Real Time: The Role Of Google In The EU Right To Be Forgotten.* 49th edn, University of California. Davis. 2017. p. 1039.

Figure 1. Google's Adjudication of the right to be forgotten claims.



[147]

The excessive amount of requests poses another challenge to the implementation of the right to be forgotten. As of July 9th 2017, Google has received *586,926* requests and evaluated for removal *2,108,985* separate URLs (satisfying the removal of only *43.2%* of all requested URLs).[148] Taking into account the financial burden and the time spent for the processing of hundreds of thousands of requests, there is no wonder the mechanism of enforcement of the right has a room for improval. But more importantly, is it appropriate to make multinational corporations responsible for striking the balance between fundamental human rights?[149] This is the question European lawmakers will have to answer in order to find a more effective solution to the challenges of the right to be forgotten implementation.

[147] E. Lee, *Recognizing Rights In Real Time: The Role Of Google In The EU Right To Be Forgotten.* (49th edn, University of California, Davis 2017). P. 1038.
[148] 'Transparency Report. European privacy requests for search removals ' (2017) <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en-US> accessed 13 July 2017.
[149] M. Douglas , 'Google expands the 'right to be forgotten', but Australia doesn't need it ' (2016) <http://theconversation.com/google-expands-the-right-to-be-forgotten-but-australia-doesnt-need-it-54887> accessed 13 July 2017.

CHAPTER III. HUMAN RIGHTS CONTROVERSIES.

3.1. Interest of the State vs. the Right to Privacy.

Privacy, free media, freedom of speech and expression are being constantly redefined with the development of communications technology. These technological advancements not only improved the life of common citizens and pushed the developments of science and scholarship, they also facilitated the process of mass-surveillance and created new ways of governmental control of the Internet. Watching its citizens has become a new reality for the states, since governments justify it with security reasons and keep expanding the mandates of intelligence agencies. Global impact of the Internet has enabled surveillance to reach a whole new level. During the Cold War era states were sending people to spy on one another; a method which has proven to be no longer necessary. The very technology we interact with on a daily basis and carry in our pockets can now provide all necessary information about our private life, location, interactions and any kind of communication.

People inevitably entrust their data to third parties in order to use the Internet and communication devices. Some of this data is being given deliberately and with full consent of the owner of its processing and storage. At the same time, there is an astonishingly huge amount of data that is being collected and stored without our knowledge and consent. Privacy policies on social networks and cookies on various websites have proven to be the tip of the iceberg of which common Internet users are aware. The majority of data that is being collected would not bring even a shadow of suspicion of its occurrence to the citizens that are being under constant surveillance. Before the historical coming out of the most famous whistleblower Edward Snowden, a former CIA contractor, millions of people had no clue about the extensive Internet and phone surveillance of citizens by the US government.[150] The scandal revealed that intelligence agencies had access to emails, were tapping phone calls and using Web and CCTV cameras and other devices not only to spy on the governments of the opponent states, but also monitor their own citizens.

[150] 'Edward Snowden: Leaks That Exposed US Spy Programme - BBC News' (*BBC News*, 2017) <http://www.bbc.com/news/world-us-canada-23123964> accessed 14 July 2017.

Commonly, the main justification of surveillance is a critical threat of terrorism, crime prevention and state security. But is this invasion of privacy always justified? The extensive case law suggests that more often state interference with privacy is not proportionate and violates fundamental human rights. One of the examples of individuals fighting for regaining the control over their private data, is the case of *Liberty v. UK*,[151] three British NGOs, Liberty, the Irish Council for Civil Liberties (ICCL), and the British-Irish Rights Watch, started a legal action against the UK on the grounds of the inexcusable violation of privacy of thousands of citizens through mass surveillance. The legal battle commenced back in 1999, when civil society actors claimed that the UK Ministry of Defence has been intercepting phone calls, fax and email exchange, collecting and storing private data of unsuspecting individuals for a period of seven years. The organisations believed that this intrusion was completely disproportionate and unlawful, and vainly fought to protect their rights in British courts for nine consecutive years before the case reached the European Court of Human Rights (ECtHR). The latter Court had a different opinion from the British judicial system and condemned the operation of surveillance programs by the government.[152] Although ECtHR pointed out that the lack of an adequate legal framework, that would regulate governmental surveillance programs, provided the UK an opportunity to have their hands untied when creating the system of surveillance, it recognised that the right to privacy, protected under the Article 8 of the ECHR,[153] has been violated by their actions. The ruling sustained the position of the Court towards the justification of mass surveillance programs as unclear, but settled an important precedent, confirming the European stance on surveillance operations.[154]

The latest case in the ECtHR, titled *10 Human Rights Organisations v. United Kingdom*,[155] also concerns the surveillance regime of the United Kingdom. In particular, the actions of the government that were uncovered in 2013 by Edward Snowden. The whistleblower revealed that the UK, in collaboration with the USA, was bulk tapping underwater fibre-optic cables, that carry traffic from Europe to North America. This surveillance program was called "TEMPORA" and it allowed the Government Communications Headquarters (GCHQ) to collect gigantic amount of content and metadata

[151] *Liberty and Others v United Kingdom,* 58243/00, ECHR (2008).
[152] C. Lopez-Curzi, '8 Years Since Massive Mass Surveillance Case' (2016) <https://rightsinfo.org/8-years-since-massive-mass-surveillance-case/> accessed 13 July 2017.
[153] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as Amended) (ECHR), 1950. Art. 8.
[154] C. Lopez-Curzi, '8 Years Since Massive Mass Surveillance Case' (2016) <https://rightsinfo.org/8-years-since-massive-mass-surveillance-case/> accessed 13 July 2017.
[155] *10 Human Rights Organisations and Others against the United Kingdom,* ECHR (2015).

(descriptive data concerning the communications; includes the date and time of said communication and from which computer network it has been sent) that passed through the cables and share it with the US National Security Agency (NSA). The NGOs claimed that the actions of the UK violated Article 8 of ECHR, since it could not be considered proportionate and necessary to collect *all* private data of millions of users, and the program did not foresee essential safeguards.[156] The ECtHR is yet to rule the decision, but previous court practice suggests that it will balance fundamental human rights with higher regard to privacy protection.[157]

Considering that the right to be forgotten primarily concerns the removal of links to private data that is available through search engines, the right does not grant the erasure of the content. This way it appears that the introduction of the right to oblivion will not change the picture from the perspective of governments obtaining personal data for their interests. All data that is currently publicly accessible or has been sent through the Internet can be easily traced and accessed (unless encrypted), technically speaking, and could have been already collected and stored. From a practical point of view, the right to be forgotten will not have any impact on surveillance programs and data collection.

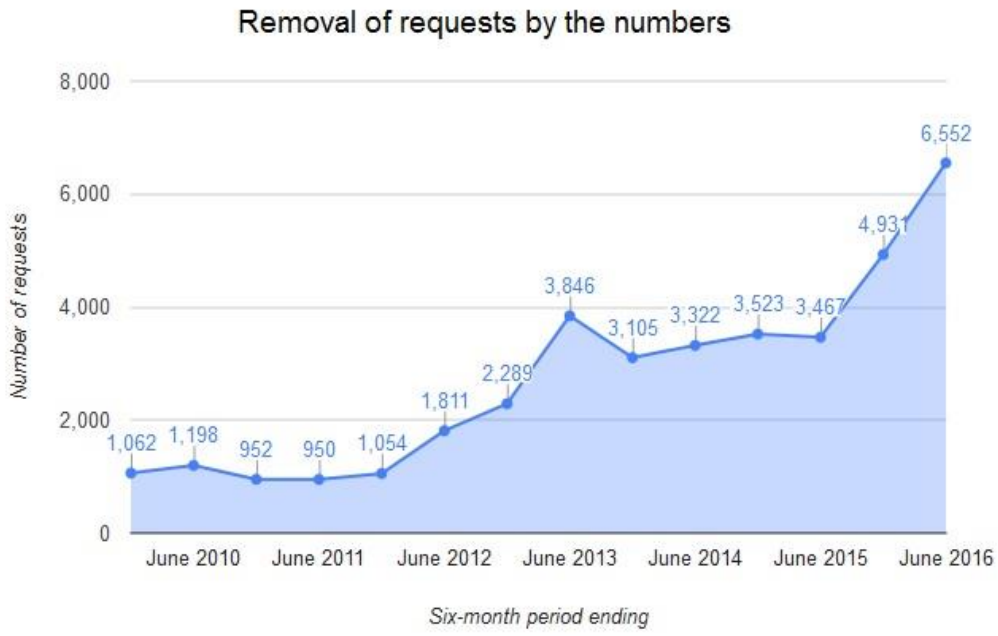
Where it makes a difference is how the states decide to use the right to oblivion. There is an ongoing debate on whether states could use the right to be forgotten as an instrument of influencing the opinion of the population (often not only their citizens, but a larger auditorium, due to the global impact of the Internet), or even re-write history. The opponents of the right argue that its implementation could potentially grant governments (which are not always democratic regimes) a tool to remove links or erase content that doesn't fit into their agenda and/or substitute information with their versions. This Orwellian total control of the Internet would not only violate the privacy of the data subjects, but more importantly, oppress the freedom of expression and damage the accuracy and adequacy of historical records.

Notwithstanding, the reality differs from the dystopia described in "1984".[158] Multinational corporations, that *de facto* direct the future of the Internet, openly advocate against any kind of

[156] *Big Brother Watch v United Kingdom*, 58170/13, ECHR (2017).
[157] C. Lopez-Curzi, '8 Years Since Massive Mass Surveillance Case' (2016) <https://rightsinfo.org/8-years-since-massive-mass-surveillance-case/> accessed 13 July 2017.
[158] G. Orwell, *1984* (New American Library, 1950). 648.

censorship and are for freedom of data flow on the Web. Rachel Whetstone, former Senior Vice President of Google stated that the company believed that, "*...more information generally means more choice, more freedom and ultimately more power for the individual.*"[159] At the same time, the tech giant acknowledged that freedom of expression is indeed not an absolute right and has certain limitations. In order to guarantee the adequacy and transparency of removal requests received from government authorities, Google started publishing Transparency Reports in 2010, making updates to the data every six months. Featuring the numbers, reasons of requests, as well as the state authorities that have filed them, Google provides almost full statistics of the request they receive from governments, including details of examples of separate requests.[160] The numbers of requests demonstrate that there has been an increase of cases of governments wanting to remove certain content. From 2015 to 2016 the number of requests grew almost in double (Figure 2.).

Figure 2.



[161]

To a bigger surprise, not only states that oppressed the freedom of expression requested to remove political content, but often Western countries that were not associated with censorship policies *per se*.[162]

[159] R. Whetstone, 'Global Communications and Public Policy. Our approach to free expression and controversial content ' (2012) <https://googleblog.blogspot.co.at/2012/03/our-approach-to-free-expression-and.html> accessed 13 July 2017.
[160] 'Transparency Report. Government requests to remove content ' (2017) <https://www.google.com/transparencyreport/removals/government/> accessed 13 July 2017.
[161] *Ibid.*

For instance, from July to December 2011 Google received fourteen requests from Spanish DPAs asking to de-list two hundred and seventy search results that featured individuals and public figures, often claiming the corruption of individuals occupying governmental positions.[163] Similarly, in 2013 French local officials requested to remove six blog posts featuring their town due to the fact that the content allegedly defamed the town, its mayor and other elected officials.[164] Google did not comply with those requests, declaring that it would remove the content only when it violates the law or respective guidelines of the state.

Consequently, the possibility that governments could use the right to be forgotten for their own purposes and violate the freedom of expression is rather unrealistic, considering the influence of search engines, national and supranational court systems, in defining the contours of the right and its implementation.

3.2. The Public Interest vs. the Right to Privacy.

The notion of privacy is being constantly re-defined in the digital era due to the global reach of the internet and a self-revealing nature of social media platforms. With privacy not being an absolute right, both public and private figures face certain limitations once it collides with public's interest. But is the interest of the public greater than privacy of an individual?

The definition of public's interest is present in every jurisdiction and does not vary in its core. Stephen Whittle and Glenda Cooper describe public's interest as "*the exposure of issues which are unambiguously of a public nature and of public concern—which has become the officially dominant one, as against the popular one*".[165] Both public nature and public concern are the key criteria in defining whether public's interest outweighs privacy concerns. When it comes to public's interest in public availability of particular information, journalistic practice may be the

[162] D. Chou, 'More transparency into government requests ' (2012) <https://www.blog.google/topics/safety-security/more-transparency-into-government/> accessed 13 July 2017.
[163] 'Transparency Report. Explore Requests. Spain.' (2017) <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en-US> accessed 13 July 2017.
[164] *Ibid.*
[165] G. Cooper and S. Whittle, *Privacy, Probity And Public Interest*, Reuters Institute for the Study of Journalism, University of Oxford. 2009. p.73

most influential in speaking out on behalf of the public and justifying the newsworthiness and contribution to the public debate of sometimes private data that has been published.

Commonly, the main justifications of mass media interference with privacy are: uncovering the hypocrisy of people of influence (usually public figures), providing "public accountability", being an intermediary between celebrities and the public (especially in cases when the latter reveal the details of their private lives in exchange for money or fame; in that case the media sees it as a *carte blanche* to continue intruding their privacy), exposing role models that do not comply with their reputation.[166] Noticeably, the media industry has assumed the role of moral police which intends to ensure public virtue and morality.[167] The idea behind playing this role in society is based on the assumption that in a democratic society citizens have the right to know about the actions of state authorities or its officials (regardless if they were appointed by the state or elected by the citizens), as well as organisations whose activity is based on public trust and private companies that hold considerable influence.[168]

The argumentation for revealing the hypocrisy of individuals in the positions of power often focuses on the fact that even private behaviour may sometimes affect the conduct of public actions. Although it is hard to prove the direct link between the two, it is much harder the completely separate private and professional lives of absolute public figures that occupy influential positions. For instance, during the 1998 scandal that revealed sexual relationship between President Bill Clinton and a former White House intern Monica Lewinsky, the coverage in the media was very influential. Even though there was no indication that extra-marital affair of the US President could breach national security or affect public policies, the moral indignation of the public and the Senate led to his impeachment, despite his false testimony that denied the sexual relations.[169] Media coverage did not only aim to sensationalise the scandal, but also to hold liable the most powerful person in the country for making a false public statement.

[166] S. Whittle, 'Privacy vs the Right to Know' (2009) <http://reutersinstitute.politics.ox.ac.uk/news/privacy-vs-right-know> accessed 13 July 2017.
[167] G. Cooper and S. Whittle, *Privacy, Probity And Public Interest*, Reuters Institute for the Study of Journalism, University of Oxford. 2009. p.67
[168] *Ibid.* p. 76
[169] *Ibid.*. p. 71

Concerning the role model argument, journalists point out that the public has a particular interest in stories covering public figures that act as an example for younger generations. In the view of the media, the public has the right to know that Naomi Campbell was visiting a drug treatment center, despite continuously denying that she has any kind of addiction,[170] or that celebrities like Kate Moss, Lindsay Lohan or Jennifer Lawrence have been engaging in illegal activities, *i.e.* taking narcotic substances.[171] The problematic nature of this argument is that not all public figures serve as role models from any moral perspective, and they should not be held as such out of curiosity of the public.[172] It is quite often that tabloids race for sensations in order to satisfy the public's appreciation of *Schadenfreude* — pleasure derived from someone's misfortune or humiliation.[173] Moreover, it is arguable that journalists always use verifiable sources and provide evidence that could potentially stand a trial.[174] Although the media has embraced the role of moral police, the fact is they lack the authority to assume such a position and the competence and training to pass such judgements.

Recent practice of the national courts (the UK, Germany, France) and European Court of Human Rights demonstrate that the European approach towards balancing the right to privacy and the public right to know has shifted to higher regards of privacy protection.[175] Reuters Institute summarises the findings of Mr. Whittle in a very comprehensive way, "*that the progressive intervention by the court reflects the overwhelming public interest in the issue and he [Stephen Whittle] called for a 'humane and human media that takes care of people and their lives*".

Concerning the right to be forgotten, public interest constitutes an exception for the erasure of the data. Although there is no definite framework on the application of the right, it is the courts and national DPAs that will have to establish the scope of the exception. Moreover, new legislation includes different provisions on the public's interest. As proposed in the GDPR, the burden of proof that certain data is in

[170] *Campbell v MGN Limited*, [n.d.] UKHL 22, United Kingdom House of Lords, (2004).
[171] S. Goncalves, V. Castro, 'A History of Celebrities Getting Caught with Drugs' (2013) <http://www.complex.com/pop-culture/2013/06/history-of-celebrities-getting-caught-with-drugs/> accessed 13 July 2017.
[172] G. Cooper and S. Whittle, *Privacy, Probity And Public Interest*, Reuters Institute for the Study of Journalism, University of Oxford. 2009. p.79
[173] *Ibid.*. p.72
[174] *Ibid.* P. 67
[175] For the detailed analysis of court practice in balancing the right to privacy and freedom of expression see Chapter I. The Ongoing Conflict Between the Right to Privacy and Freedom of Expression.

the public's interest will lie on the data controller, rather than data subject, as it is under the current legal framework.[176]

3.3. Search Engine's Commercial Interest vs. the Right to Privacy.

In a landmark decision on the right to be forgotten, the Court of Justice of the European Union has introduced a new player to balance freedom of expression with the right to privacy. For the first time in history individuals gained a right to ask search engines to remove links to their private data in an online search once it is no longer relevant and could stand a test against the public's right to know. But more importantly, the Court handed the power to decide whether personal data meets the criteria required for removal directly to the search engines. This does not mean *de jure* that tech giants are the decision-makers behind the balancing of fundamental human rights. Nevertheless, from 2014 Google, Bing, Yahoo! and other search engines have become the first instance for individuals to inquire their right to be forgotten.

Although Google, the absolute leader on the European market, has launched a mechanism of processing the requests right after the Court ruling, the decision-making process remains behind the closed doors. Since the CJEU did not establish any requirements to make the procedure of handling the requests open to public, the way Google makes these decisions remains unknown to all, Data Protection Authorities, courts and individuals.[177] By all means, the company is obliged to comply with the guidelines set out by the decision and apply proportionality principle. Yet, since the requests have to be assessed on a case-by-case basis, search engine will have to interpret the meaning of "inaccurate, inadequate, irrelevant or excessive" itself. How influential could it be? Considering that Google will be the primary body that will deal with all the requests, the majority of cases will be decided by the tech giant, unless individuals appeal the decisions to DPAs or courts. And the portion of decisions that do get appealed? Mathias

[176] Regulation (EU) 2016/679 On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016. p.119/32-33.
[177] M. Scott, 'Europe Tried To Rein In Google. It Backfired.' (*Nytimes.com*, 2017) <https://www.nytimes.com/2016/04/19/technology/google-europe-privacy-watchdog.html> accessed 14 July 2017.

Moulin, a deputy director at the Commission National de l'Informatique et des Libertés (French DPA), admitted, "*When it comes to appeals, we agree with Google most of the time*".[178]

Having an extensive amount of power in establishing the basis of the right to be forgotten, multinational corporations that dominate the search market are facing a great deal of responsibility. Ironically, the very companies that are processing private data to generate search results for search engine users and contribute to their commercial interest, are now deciding if links to personal information should stay online. The Court also acknowledged that search engines generate revenue from advertising online and having more content considerably contributes to their commercial goal.[179] Nevertheless, CJEU found that the commercial interest could not override the right to privacy of individuals.[180]

The ultimate interest in data collection and expanding the pool of the clients has opened for discussion the commercial interest of search engines in protecting privacy of the individuals. It hasn't been the first time Google has been cornered with disregard to the privacy of its users, when in February 2010 the company launched Google Buzz, a social-networking tool that had been incorporated in the email platform Gmail. Without notifying users, the program revealed personal networks, identifying contacts that were interacted with the most.[181] The breach of privacy was met with significant criticism since it made public a considerable amount of sensitive information. It turned out that the list of frequently used contacts could reveal more information than previously thought; from the name of your private physician or the person you had an affair with to previously anonymous journalistic sources, on some occasions Google Buzz even uncovered the exact locations from where the messages were sent.[182] After facing a number of legal issues due to privacy concerns, the platform was taken down by the company the following year.[183]

---

[178] M. Scott, 'Europe Tried To Rein In Google. It Backfired.' (*Nytimes.com*, 2017) <https://www.nytimes.com/2016/04/19/technology/google-europe-privacy-watchdog.html> accessed 14 July 2017.
[179] Google Spain SL, Google Inc. v AEPD and Mario Costeja Gonzalez [2014] C - 131 /12 (CJEU). Para 57.
[180] K. Sheridan , 'One view: ECJ's Google ruling will make it harder to trust search results ' (2014) <http://www.lexology.com/library/detail.aspx?g=52594059-1f39-460e-bd85-74a2a3db66af> accessed 13 July 2017.
[181] M. Wood, 'Google Buzz: Privacy nightmare' (2010) <https://www.cnet.com/news/google-buzz-privacy-nightmare/> accessed 13 July 2017.
[182] L. Magid , 'Google Buzz Raises Privacy and Safety Concerns' (2011) <http://www.lexology.com/library/detailhttp://www.huffingtonpost.com/larry-magid/googles-buzz-raises-some_b_455711.html.aspx?g=52594059-1f39-460e-bd85-74a2a3db66af> accessed 13 July 2017.
[183] Gmail Help, 'Google Buzz has gone away' (2011) <https://support.google.com/mail/answer/1698228?hl=en> accessed 13 July 2017.

Besides Google Buzz, the tech giant faced far more severe accusations for invasion of privacy due to the Google Street View platform. Although the service has had an objective to launch an accurate coverage of streets around the world through panoramic images, thousands of individuals were concerned with their privacy not only because it captured their homes, but also that data capturing equipment included images of individuals.[184] Moreover, on multiple occasions Google has been reportedly collecting and storing payload data from unencrypted Wi-Fi connections as part of the street view. This led to the company suspending or not providing the service in a number of countries, including Austria, Australia and Germany.[185] Despite removing images once the users have reported them, Google has faced a series of lawsuits for violating privacy around the world (Ben Joffe v. Google,[186] Boring v. Google, Inc.,[187] Google v. Vederi,[188] Pia Grillo v. Google inc.[189]).

Taking into account the systematic disregard of Google to the privacy of its users, one could conclude that privacy protection might not be the main objective of the multinational corporation after all. Throughout the years the company has demonstrated that its commercial goals often outweigh privacy considerations. The extensive practice provides sufficient ground to believe that the search giant is not the entity to entrust your personal data to, let alone to balance the fundamental human rights.

CHAPTER IV. The Right to Be Forgotten Challenges.

4.1. Vague and Ambiguous Criteria Established in the Existing Legal Framework.

Considering that CJEU ruling on the *Costeja* case appointed search engines as the *de facto* decision-makers in processing all requests of individuals inquiring the right to be forgotten, the decision has been

[184] C. MacDonald, 'Google's Street View site raises alarm over privacy' (2007) <http://www.heraldscotland.com/news/12778601.Google_apos_s_Street_ViewMacDonald,%20Calum%20%28June%204,%202007%29.%20%22Google's%20Street%20View%20site%20raises%20alarm%20over%20privacy%22_site_raises_alarm_over_privacy/> accessed 13 July 2017.
[185] 'Google Admits It Sniffed Out People's Data' (2017) <http://news.techeye.net/security/google-admits-it-sniffed-out-peoples-data> accessed 14 July 2017.
[186] *Benjamin Joffe v Google Inc.* 11 – 17483, United States Court of Appeals (2013).
[187] *Aaron C. Boring v Google Inc.* 09- 2350, United States Court of Appeals (2010).
[188] *Vederi LLC v Google Inc.,* 744 F. 3d 1376, United States Court of Appeals, Federal Circuit (2014).
[189] *Pia Grillo v Google Inc.,* 500-32-130991-112, QQ (2014).

met with a wide range of criticism from the governments, individuals and search engines themselves. In the opinion of Lady Prashar, chairman of the Judicial Appointments Commission of the UK House of Lords, "*It is crystal clear that the neither the 1995 directive nor the [ECJ's] interpretation of it reflects the incredible advancement in technology that we see today, over 20 years since the directive was drafted*".[190] Indeed, since the Data Protection Directive was adopted three years before the emergence of the first search engine, current legal framework is clearly outdated in respect to new developments of information technology.

The main criticism concerning the judgement is based around the fact that the criteria for data removal are "*vague, ambiguous and unhelpful*" and leave broad room for interpretation for data controllers.[191] The judgement reflected on the 1995 Directive and stated that private data can be erased when it "*...appear[s] to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes and in the light of the time that has elapsed*".[192] Nevertheless, the Court did not clarify when the information could be considered irrelevant, no longer relevant, or what period of time has to pass in order to claim the right. What seem to be the main guidelines for implementing the right has not been clarified and thus left for the search engines to decide themselves when accessing the removal requests. Hence, Google and other search engines were left with responsibility to establish a system of criteria they would apply in practice. Tech giants resorted to assembling groups of lawyers and other specialists in order face the challenge posed by the CJEU.[193]

The Article 29 Working Party (the 29WP), also known as the Data Protection Working Party established by Article 29 of 1995 Directive, provides the EU Commission with recommendations on data protection issues.[194] In November 2014 the 29WP has published guidelines on the implementation of the *Costeja* judgement. The guidelines had a goal of clarifying the criteria set out by the Court and include practical advice on how to balance the privacy of an individual with the public's interest involved. Meanwhile, the 29WP recommended the following: "*A balance of the relevant rights and interests has to be made and the outcome may depend on the nature and sensitivity of the processed data and on the interest of*

[190] O. Bowcott, 'Right to be forgotten is unworkable, say peers ' (2014) <https://www.theguardian.com/technology/2014/jul/30/right-to-be-forgotten-unworkable-peers> accessed 13 July 2017.
[191] H. M. Brammer, 'The Law: The Right to be Forgotten', ASA Institute for Risk & Innovation. 2015. pp. 3-4.
[192] *Google Spain SL, Google Inc. v AEPD and Mario Costeja Gonzalez,* C - 131 /12, CJEU (2014). Para 93.
[193] H. M. Brammer, 'The Law: The Right to be Forgotten', ASA Institute for Risk & Innovation. 2015.p. 4.
[194] European Data Protection Supervisor. , 'Glossary - A.' (n.d.) <https://edps.europa.eu/data-protection/data-protection/glossary/a_en> accessed 13 July 2017.

the public in having access to that particular information. The interest of the public will be significantly greater if the data subject plays a role in public life".[195] Besides that, the Working Party stressed the priority of public interest in deciding whether the links to private data should be de-listed: "*In practice, the impact of the de-listing on individuals' rights to freedom of expression and access to information will prove to be very limited. When assessing the relevant circumstances, European Data Protection Authorities ... will systematically take into account the interest of the public in having access to the information. If the interest of the public overrides the rights of the data subject, de-listing will not be appropriate".*[196] Although the 29WP recognised the relevance of the role of applicants in society, stating that when public figures are involved the extent of the public's interest differs greatly, and emphasised that, as a rule, the latter overrules the interests of individuals.[197]

Regarding the practical advice of how to balance particular cases or to what extent the public's interest overrides individuals' privacy, the 29WP guidelines did not provide any clarification.[198] In fact, neither did they facilitate the decision-making burden laid on the search engines. Therefore, to what extent does the vague criteria of the right to be forgotten in the current legal framework complicate the application of the right? The correlation between the numbers of processed and satisfied requests may suggest that a big portion of requests are not satisfied not only when they do not fulfill the ambiguous criteria, but also because search engines could potentially decline the requests if it was not clear whether the privacy of the data subject passes the public interest test. Hence, the latest statistical data demonstrates that among 2,114,035 URLs that have been evaluated by Google for removal, only 774,372 (43.2%) have been successfully removed,[199] while Bing search engines that operated under Microsoft accepted 19,242 (37%) of URLs out of requested 51,784.[200] Other smaller search engines did not go public with the number of requests they have received and accepted after the right to be forgotten ruling. Since the processing of requests and exact criteria search engines are using are not as transparent as they could have been, the reasons of why such a high percentage of requests are being denied remains unknown.

---

[195] Guidelines (EU) 14/EN WP 22 5 On the Implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez C - 131/12, Article 29 Data Protection Working Party. 2014. p.2
[196] *Ibid.*. p.2
[197] *Ibid.* p.2
[198] *Ibid.*
[199] 'Transparency Report. European privacy requests for search removals ' (2017) <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en-US> accessed 13 July 2017.
[200] Microsoft, 'Content Removal Requests Report' (2016) <http://www.microsoft.com/en-us/about/corporate-responsibility/crrr/> accessed 13 July 2017.

Apart from the ambiguity of the criteria, one of the main criticisms of the judgement was that it did not consider the application of the right by smaller search engines. If Google covers more than 90% of the European search market and has resources to establish departments to process thousands of requests, how could other search engines that hold 1-3% of the market possibly financially and practically cope with the number of requests they keep receiving and deliver an adequate level of compliance with the ruling and 1995 Directive. Neither the ruling, the Data Protection Directive nor new provisions of the GDPR, include any provisions on how the right should be applied in practice by the various search engines. The definition of search engines as data controllers remains quite general and distinguishes them only from publishers and third party websites, but does not establish any particular characteristics.[201]

More importantly, it is the individuals that have voiced the most concern over commercial corporations being given power to make decisions on what should or should not remain on Web searches. And without clear guidelines of doing so, how could search engines be expected to adequately analyse and evaluate each request inquiring the right to be forgotten? The EU legal framework leaves room for interpretation and the only way to make the right to oblivion effectively applicable in practice without human rights concerns, is to update the current legislation with more specific guidelines for implementation.

4.2. Impact of the Right to be Forgotten on Journalism: Freedom of Speech and Information, Censorship Issues.

In the world of information technology that expands the boundaries of sharing information, journalism is the industry that is most affected by the fast-changing notions of privacy, data protection, free expression and the public's right to know. New communications technology has changed the way we view information sharing once and for all. If earlier the publications were put in print and archived in

[201] Guidelines (EU) 14/EN WP 22 5 On the Implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez C - 131/12, Article 29 Data Protection Working Party. 2014. p.2.

editorial archives or libraries, the digital era has given media channels an opportunity to reach an unlimited audience around the world and stay publicly available without time constraints.

With all the benefits to freedom of information and satisfaction of the public's right to know, journalism acquired a much more prominent role in regard to historical research and demanding public accountability. Using investigating techniques and verifiable sources, the industry claims to be an independent voice that discloses truth to the public. But publishing material online does not only result in reaching new audiences and making news more available, it also has long-term ramifications for disseminating information about individuals. Although journalists are required to regularly weigh the newsworthiness of material with its potentially negative impact on individuals, the constant race for sensation and bigger revenue often undermines the privacy of individuals. A common practice of journalism is to prioritise its audience's desire and freedom of information over minimising any potential harm the publication could have on public and private figures.[202]

Since publishing online reaches a larger audience and could remain publicly available for an unlimited period of time, the level of impact or possible harm it could bring has become far greater than any printed publication. At the same time, digital content is technologically accessible for rectification, clarification or removal. Besides the obvious benefits of providing the most accurate information and/or updating it according to relevance, these opportunities have provided a new challenge for keeping historical records and media staying independent from the influence of governments or corporations. Historically, journalists have been actively resisting the idea of "*unpublishing*" a so-called retrospective revision or removal of accurate and legally published content.[203] In 2009 Canadian Associated Press Managing Editors (APME) surveyed editors of the most influential media channels in order to compile a report on freedom of media. The report uncovered a growing number of requests to news platforms from data subjects and sources of news to unpublish information concerning them.[204] The response of the editors was that media channels "*do not rewrite history; we report what happened*," as well as, "*Sorry,*

[202] I. Shapiro, and B. Rogers, 'How The "Right To Be Forgotten" Challenges Journalistic Principles'. Digital Journalism. 2016., p. 5.
Ibid.. p.5.
[204] K. English, 'Online Journalism Credibility Project: The Long Tail of News Archives and "Unpublishing" Requests' (2012) <http://www.apme.com/page/Unpublishing> accessed 13 July 2017.

life isn't fair. Journalism's job isn't to clean up your driving record so you can get a job, is it?"[205] Nevertheless, journalists agreed that publishing faced certain limitations, and in justified circumstances such as violation of law or threat to life or safety of individuals, data could be removed.[206]

Although the industry has foreseen the possibility of harm reduction on legitimate occasions, it has also pointed out the subjectivity of relevance of data. Thus, the notion of newsworthiness derives from the word "news" and implies that current stories are more relevant than yesterday's news. In fact, in some circumstances it might be the case. For instance, the relevance of the records and coverage of bankruptcy, suffered by Mario Costeja and addressed in the landmark CJEU ruling, is debatable after the passage of almost sixteen years. Did it contribute to public interest more than it caused damage to Costeja? The Court ruled that in this case it did not. But let's say records from more than thirty years ago were found, stating that the current head of the state was an active supporter of a racist organisation and had repeatedly expressed his utter contempt for slavery abolishment. Would that information be relevant even thirty or forty years after the occurrence? Such a difference between perceptions of relevance suggests that although it is objectively temporary, it cannot be appropriately calculated in months, years or decades.[207] Each case will undoubtedly differ and will have to assessed separately.

Where journalism has to draw the line is between availability and being easily findable. Considering that the newly introduced right to be forgotten does not demand the removal of original content, which includes private data, such articles or publications will remain available on the websites or archives. At the same time the right to oblivion will de-list the links to these sources as a part of the European data protection policy. This means that Internet users will no longer be able to access de-linked pages through Web search. The content of it will be untouched and users will still be able to access it directly, but to find the source will be rather difficult.

The introduction of the right in 2014 by the CJEU ruling has stirred a wave of reactions from media around the world. While European platforms condemned the right, claiming that it directly affects freedom of expression, journalists in the US supported their view and openly opposed the possibility of

[205] I. Shapiro, and B. Rogers, 'How The "Right To Be Forgotten" Challenges Journalistic Principles'. Digital Journalism. 2016., p. 5.
Ibid., p. 5.
[207] *Ibid.*., p. 7.

the right to oblivion reaching their citizens. The New York Times editorial expressed the opinion that the new data protection approach in Europe was threatening freedom of press and expression in particular, and could result in hindering the accessibility of journalists' opinions.[208] The BBC[209] and The Telegraph[210], also disapproving of the de-listing of their articles by Google, published detailed lists of publications that have been de-linked under the right to be forgotten in order for the public to know what kind of information is being affected. Although the media finds it newsworthy to reveal what content is being de-listed, such publications undermine the main objective of the right to oblivion - to not be found by the search result of your name in relation to specific information. After a wave of criticism from the media, Google has decided to host a series of conferences for journalists in Europe with a goal to find possible solutions for the implementation of the right.[211] Some argued that the company used this opportunity as a political stunt aimed to add fuel to the fire of public opinion on the right to oblivion.[212]

Regardless of massive disapproval of the right to be forgotten by the media, it is worth mentioning that journalists have expressed an opinion that some cases do require a certain level of protection of privacy. In fact, in practice the industry had often gone beyond the provisions enshrined in the law. Although neither of the courts have put an obligation on the media to remove names or anonymise individuals from the articles they have published, some editorials have admitted that such an option was under consideration in order to minimise or restrict the damage caused to individuals by interference with their privacy.[213]

[208] NY Times, 'Ordering Google to Forget' (2014) <https://www.nytimes.com/2014/05/14/opinion/ordering-google-to-forget.html?_r=0> accessed 13 July 2017.
[209] N. McIntosh, 'List of BBC web pages which have been removed from Google's search results' (2015) <http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379> accessed 13 July 2017.
[210] R. Williams, 'Telegraph stories affected by EU 'right to be forgotten'' (2015) <http://www.telegraph.co.uk/technology/google/11036257/Telegraph-stories-affected-by-EU-right-to-be-forgotten.html> accessed 13 July 2017.
[211] J. Kiss, 'Dear Google: open letter from 80 academics on 'right to be forgotten' ' (2015) <https://www.theguardian.com/technology/2015/may/14/dear-google-open-letter-from-80-academics-on-right-to-be-forgotten> accessed 13 July 2017.
[212] T. Cheshire, 'Is Google Trying To Make The Law An Ass?' (2014) <https://www.theguardian.com/media/2003/jan/2http://news.sky.com/story/is-google-trying-to-make-the-law-an-ass-103981439/pressandpublishing.broadcasting> accessed 13 July 2017.
[213] M. Santin, 'The problem of the right to be forgotten from the perspective of self-regulation in journalism'. El profesional de la información, v. 26., n.2, 2017. p. 308.

4.2. Territorial Reach. The Possibility of Global Enforcement of the Right to be Forgotten.

One of the most urgent issues raised by the CJEU ruling concerns the practical approach to the implementation of the ruling and its consequences in a legal context. With the ruling having no territorial limitations to particular countries or regions, the question remains open: When complying with the right to be forgotten, how far are search engines obliged to implement it? Global reach of the Internet has brought a new dimension to the issues of territorial reach of public and private international law doctrines in the online environment.

The problem of extraterritoriality in the context of privacy and data protection laws is not new in the EU practice. Intelligence surveillance performed by foreign states could be one example when it is often unclear what law should be applicable. When data protection regimes collide, the only thing that could be certain is the position of supranational courts, like the ECtHR, towards disproportionate surveillance operations which violates human rights.[214] But extraterritoriality issues do not cease with the intelligence surveillance argument, constant international transfer of data raises new issues concerning data processing and storage. Considering that Internet users are sending and receiving data from different countries and visiting foreign websites on a daily basis, the scope of the problem of deciding which data protection regime applies appears far greater.[215] This dilemma has been also timely recognised at the Hague Conference on Private International Law in 2010, which highlighted that "*...cross-border data transfers have raised serious questions of international jurisdiction...*".[216] Notwithstanding, extraterritoriality issue appears even more complicated and unresolved when it comes to data processing by private parties.[217]

Hence, the universal reach of search engines and their hierarchal structure of global and state-based domains (global - .com; national: Spain - .es, France - .fr, Germany - .de etc.) has created a debate over the implementation of the ruling. From both, legal and technological perspectives, the right to be

[214] Liberty and Others v United Kingdom [2008] 58243/00 (ECHR).
[215] C. Kuner, 'Extraterritoriality and the Fundamental Right to Data Protection' (2013) <https://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/> accessed 13 July 2017.
[216] *'Cross-Border Data Flows and Protection', Hague Conference on Private International Law.* Hague, Permanent Bureau, 2010, p.7.
[217] C. Kuner, 'Extraterritoriality and the Fundamental Right to Data Protection' (2013) <https://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/> accessed 13 July 2017.

forgotten could be applied on two levels: local and global. The arguments for and against the two approaches could be formed based on legal precedents of international public and private law.

The idea to implement the ruling locally has gained a number of supporters, including search engines themselves. Since the ruling did not include any particular provisions in its implementation, tech giants that have been faced with the responsibility to come up with an approach to the application of the right to be forgotten in practice, have chosen to comply with the ruling of the Court of Justice of the European Union in European Union. Thus, Google's present approach was to de-list requested links from country-based domains in Europe but not on the global version Google.com.[218] Since the latter version is accessible to all European users with a click of a mouse, supporters of the right to oblivion have argued that it undermines or even diminishes the effectiveness of the right.[219] The application of the right has already sparked a debate in a number of states and even reached the ECtHR. The first and only (so far) precedent started with France arguing that Google must de-list the respective links on the global index Google.com and not only in the EU. Conseil d'Etat, the highest French legal decision-making body, has assessed the case after three years of legal battle and suspended the judgement on the grounds of not being authorised to make decisions on this matter preceding the decision of the European Court of Justice (ECJ). Consequently, the case has been forwarded to the ECJ and currently remains in process.[220]

A strong argument for local implementation can be formed on the basis of a well-known *UEJF and Licra v. Yahoo!* case. The Union of French Jewish Students and the League against Racism and Anti-Semitism has brought legal action against Yahoo! For hosting an online auction that included items of Nazi paraphernalia. The auction could be accessed from any country in the world with Yahoo! being a mere intermediary.[221] However, if selling Nazi memorabilia is not against the law in the state where the company is registered, the USA, French law prohibits the display of the latter objects. The plaintiffs

[218] S. Schechner and Lisa Fleisher, 'EU Invites Google, Microsoft to Discuss 'Right to Be Forgotten'' (2014) <https://www.wsj.com/articles/eu-regulators-invite-google-microsoft-to-discuss-right-to-be-forgotten-1405592730> accessed 13 July 2017.
[219] B. Koekkoek, 'The Territorial Reach Of The EU'S "Right To Be Forgotten": Think Locally, But Act Globally?' (*EJIL: Talk!*, 2017) <https://www.ejiltalk.org/the-territorial-reach-of-the-eus-right-to-be-forgotten-think-locally-but-act-globally/> accessed 14 July 2017.
[220] The Conseil d'Etat , 'Right to be delisted' (2017) <http://english.conseil-etat.fr/Activities/Press-releases/Right-to-be-delisted> accessed 13 July 2017.
[221] *LICRA v Yahoo!*, RG:00/0538, Tribunal de grande instance (2015).

argued that the company was violating the law advertising these items in France, where it is illegal.[222] The decision of Parisian Tribunal de Grande Instance (TGI) has ordered Yahoo! to restrict the access to aforementioned pages for French users. The TGI has subsequently noted that determining the geographic origin of the search inquiry, in particular whether it originated in France, would be a rather technologically challenging task for the company.[223]

The reasoning of the TGI is relevant for a number of reasons. Firstly, the decision was based on the international public law principle that is the key to establishing jurisdiction - *the territoriality principle*. Just as has been stated by Lord Macmillan "*It is an essential attribute of the sovereignty of this realm, as of all sovereign independent States, that it should possess jurisdiction over all persons and things within its territorial limits and in all cases, civil and criminal, arising within these limits*".[224] Hence, if TGI would have decided to order Yahoo! to limit the access to respective pages on a global level, the decision would have interfered with other state's sovereignties.[225] Drawing a parallel with the French case against Google, their argument would not have stood. Secondly, if we consider the scenario without any territorial limitations, another supporting argument for local implementation could be concluded. In the event of the states being able to decide which content should be available online and which should be restricted on the global level, the Internet would host information that has been approved by everybody, including most anti-democratic regimes. This nightmare for freedom of expression and information on the Internet is highly unlikely to be allowed by the international community. Subsequently, international public law provides geographical boundaries for the states when it comes to establishing the limits for accessibility of information on the Web.[226]

Although from one perspective imposing territorial limitations seems like the most reasonable thing to do, analysing separate cases might bring about a different conclusion. Hence, when we take into account the very facts of the known *Costeja* case, global application of the right to be forgotten may appear as a

[222] B. Koekkoek, 'The Territorial Reach Of The EU'S "Right To Be Forgotten": Think Locally, But Act Globally?' (*EJIL: Talk!*, 2017) <https://www.ejiltalk.org/the-territorial-reach-of-the-eus-right-to-be-forgotten-think-locally-but-act-globally/> accessed 14 July 2017.
[223] *Ibid.*
[224] F. Alexander Mann, *The Doctrine of Jurisdiction in International Law*, A.W. Sijthoff, 162. (internal citations omitted). 1964. p.30.
[225] B. Koekkoek, 'The Territorial Reach Of The EU'S "Right To Be Forgotten": Think Locally, But Act Globally?' (*EJIL: Talk!*, 2017) <https://www.ejiltalk.org/the-territorial-reach-of-the-eus-right-to-be-forgotten-think-locally-but-act-globally/> accessed 14 July 2017.
[226] *Ibid.*

logical option. Considering it was a Spanish newspaper that published the article about the plaintiff which was referred to by Google--the server that hosted the website, which was referenced by Google, has been located in Spain--the private data under the scrutiny of the Court related to a Spanish citizen; the search query, that has been assessed, consisted of the name of the plaintiff, who was a Spanish citizen; one can conclude that the content addressed in the case had the closest link to Spain, compared to other states.[227] This reasoning could assume that since it was Spain that had most relation to the information, it is the authorities of Spain who have the most grounds to make a decision on the territorial reach of de-listing. In fact, Spain had all the right to remove information from the original source if it decided to. That way the data could not be accessed locally or globally. From this perspective it could be not considered a "*jurisdictional overreach*" if Spain ordered Google to de-list the links worldwide.[228]

After the French action against Google, *Equustek Solutions Inc. v. Jack*. is the most recent case supporting this argumentation. The case was based on the misappropriation of goodwill of Canadian business Equustek by another company Jack et al. The latter used the images of Equustek's products in order to make sales, substituting the items with ones of their production. The plaintiff also demanded that Google Inc. and Google Canada remove the links to search results generated from the defendant's websites.[229] When considering the judgement, the Supreme Court of British Columbia ruled that the search engine was required to comply with de-listing globally "*in order to adapt to the borderless nature of the internet*".[230] Moreover, the Court stated that "*Traditional principles of international jurisdiction, particularly territoriality, are poorly suited for this sort of environment of geographic anonymity. Courts have struggled to develop a satisfactory solution, yet no progress has been made toward a uniform global standard of Internet jurisdiction*".[231] Naturally, the judgement was received with very diverse reactions. It is worth noting that although the subject matter in *Equustek Solutions Inc. v. Jack*. was of international private law, international public law also considered "*interest-balancing*" in the jurisdictional assertion.[232]

---

[227] B. Koekkoek, 'The Territorial Reach Of The EU'S "Right To Be Forgotten": Think Locally, But Act Globally?' (*EJIL: Talk!*, 2017) <https://www.ejiltalk.org/the-territorial-reach-of-the-eus-right-to-be-forgotten-think-locally-but-act-globally/> accessed 14 July 2017.
[228] *Ibid.*
[229] *Ibid.*
[230] *Equustek Solutions Inc. v Jack,* BCSC 1063, The Supreme Court of British Columbia (2014). Para 159.
[231] *Ibid.* Para 37.
[232] C. Ryngaert, 'The Limits of Substantive International Economic Law: In Support of Reasonable Extraterritorial Jurisdiction', Institute for International Law. Working Paper No 99. 2006. p.4.

Therefore, the potential reach of the right to be forgotten ruling does not have clear boundaries. The supporters of the territoriality principle will argue that the CJEU ruling should only be applied locally since no state has the authority of imposing restrictions on any other state. Yet, others will find that since the CJEU is an institution that interprets the European Union legislation, in particular 1995 Data Protection Directive, the implementation of the ruling may as well cover all EU Member States. Further, others may see the EU territoriality argumentation as a justification for global application of the right to oblivion. Another argument is based on the global nature of the Internet, stating that the right could only be effectively applied worldwide.[233] Consequently, future provisions on the implementation of the right will depend mostly on the EU practice and how far the new legislation will expand the right. Nevertheless, it does not mean that Europe will be dictating to the rest of the world to remove content that is considered irrelevant or no longer relevant under the EU data protection regime. The negative response of the US to the right to be forgotten suggests that *prima facie* any endeavor to apply the right in the United States will notably fail.[234]

4.4. Impact on Reputation and Human Dignity.

Since the main objective of right to be forgotten is to remove private information that could be damaging to an individual (clearly when it meets the criteria established by law) from the Web search, it is based on rectifying information that molds the public's perception about us. Reputation, or our image in social context, is a formed opinion about us based on numerous factors established by society. In other words, it is an impression about an individual that has an impact in all spheres of social interactions: from relationships and education to employment and position in society. Undoubtedly, our social image matters to a great extent, since it directly affects our lives.

Hence, individuals commonly monitor their behaviour and actions primarily not to "stain" their reputation. But what happens when a silly misdemeanor or an embarrassing moment has been recorded

[233] B. Koekkoek, 'The Territorial Reach Of The EU'S "Right To Be Forgotten": Think Locally, But Act Globally?' (*EJIL: Talk!*, 2017) <https://www.ejiltalk.org/the-territorial-reach-of-the-eus-right-to-be-forgotten-think-locally-but-act-globally/> accessed 14 July 2017.
[234] *Ibid.*

in one way or another and is out there for everyone to see? Public perception about the subject might potentially change in a negative way and remain that way to no end due to constant reminders about the event. This type of scenario has become common in the world of communication technologies and the various ways to record and store information. As the common conception of the online world states: the Internet doesn't forget. Indeed, once the data has entered the World Wide Web it might remain there forever despite the limited time-lapse of hyperlinks. Search engines have introduced a new dimension to the notion of reputation. It has become routine for employers to check the social media of applicants, or individuals Google searching the person they are going on a date with. This way keeping your online record "clean" has become a necessity in order to live your life without discrimination or public judging.

The idea behind the protection of one's reputation is not new. Legal doctrine of Germany, France, Spain and Italy has a traditional foundation for personal data protection. The practice provides individuals with the right to regain certain control over their image, reputation and honour. The historical background of Europe has also served as a basis for stronger data protection policies. The Nazi regime in Germany, together with the East German secret police, has made an influence on the countries when it comes to information control; that the history of atrocities should not be repeated. Thus, thirteen states in Europe have provided data protection assurance directly in the constitutions.[235]

Yet, data protection policies are becoming harder to impose outside of national context. With international transfer of data and the Internet being accessible from almost every part of the planet, the collision of jurisdictions and legal approaches towards privacy becomes inevitable. The right to be forgotten could be the light at the end of the tunnel for those who have been victims of their reputation. The CJEU ruling has introduced the right to oblivion primarily because it was Mario Costeja that aimed to restore his reputation and no longer face the consequences of past mistakes that are no longer relevant. The highly arguable ruling has made a precedent suggesting that individuals should not be punished for their deeds eternally.

The same approach could be applied to criminals. Although it is necessary to assess the relevance of the information concerning served convictions or arrests, most jurisdictions recognise the right of individuals with criminal records to be rehabilitated in society. The concept implies that everyone

[235] G. Brock, *The Right to be Forgotten: Privacy and the Media in the Digital Age* (I.B.Tauris) 160. 2016. Extract p.12

deserves a second chance, and thus an opportunity for a fresh start in society. The accessibility of publications regarding former criminal records most definitely has a negative effect that hinders the idea behind the rehabilitation process. Introducing the right to be forgotten will undoubtedly support the rehabilitation practice.

Defamation cases have been addressed by court systems around the world. The protection of the individual's reputation and honour has been commonly invoked on the grounds of privacy considerations. In the ECtHR *A. v. Norway* case, the plaintiff, who had a criminal record, filed defamation proceedings and claimed the presumption of innocence when another crime was committed in his close proximity. After the actual perpetrators have been arrested, A. claimed that the accessibility of the data concerning his criminal record was damaging to his moral and personal integrity. The Court ruled that media publications had gravely harmed the reputation and honour of the plaintiff and that national courts had failed to balance the rights proportionally.[236]

From a broader human rights law perspective, the right to be forgotten covers the protection of human dignity. As a basic fundamental human right enshrined in the Universal Declaration of Human Rights, human dignity is at the core of human identity, "*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*".[237] Being the foundation of the modern concept of human rights, it is evident that protecting human dignity against the phenomenon of "*default remembering*" that may bring negative consequences by keeping certain data eternally accessible, should be in the interest of humanity.[238] Therefore, the human rights argument for the implementation of the right to oblivion could be valid only if we perceive the concept as "*an instrument for the preservation of people's dignity*".[239]

Following the argument of necessity of the protection of reputation, honour and dignity of individuals, the right to be forgotten could be viewed as a significant tool for the protection of human rights.

[236] *A v Norway*, ECHR (2009).
[237] Universal Declaration of Human Rights, 1948.
[238] C. Santos Colnago, 'The Right to be Forgotten and the Duty to Implement Oblivion: A Challenge to Both "Old" and "New" Media'. 2014. p.9. <https://www.jus.uio.no/english/research/news-and-events/events/conferences/2014/wccl-cmdc/wccl/papers/ws14/w14-colnago.pdf> accessed 13 July 2017.
[239] *Ibid.*.

Notwithstanding, considering the conflict of oblivion with freedom of expression, it is important to find a fair balance that will proportionally weigh fundamental human rights.

4.5. Future Development of the Right to Be Forgotten and Its Implications.

Due to the fact that the right to oblivion has been met with sufficient criticism over posing potential danger to the fundamental human right of freedom of expression, as well as the concept of remembering and archiving the data on the Web, the implementation of the right has had a rather limited scope. With search engines deciding on the criteria of the application of oblivion behind the closed doors, the very basis of the practical approach to the implementation of the CJEU ruling remains unclear. Since current legal framework on data protection does not adequately cover privacy risks present in the digital era, the entrance into force of the General Data Protection Regulation should answer the main questions relating to the right.

Primarily, the GDPR will provide a new perspective to the discussion on the potential freedom of expression concerns. The regulation provides exceptions to the compliance with the requests for erasure. Exercising the freedom of expression and information is one of them, together with public interest provisions and archiving purposes. Clear definitions of the exceptions to the right to erasure, current legal basis of the right to be forgotten, could serve as an end to the discussion of the unlikely risks and shift the challenges towards the technological aspect of the implementation of the right. Moreover, the clarifications on the cases when the right to erasure applies should also substantially narrow down the number of requests to de-list private data submitted to search engines, relieving tech giants from a portion of pressure put on them by the towering mass of right to be forgotten queries.

Yet, scholars and qualified specialists have been actively searching for effective ways to implement the right to oblivion in practice. Many of the proposed approaches have been rather technological responses to the problems of massive data retention, failure to secure private data and the very nature of the Internet undermining the efficiency of de-listing the links to private data (*i.e. Streisand effect* - a wide phenomenon present when any attempt to remove, censor or restrict the public from getting to know

certain information proceeds with society opposing the limitation of data and reacts with spreading and publishing the information in question to a greater extent on the Internet).[240]

One of the possible solutions to the implementation of the right to oblivion is the concept of setting an *expiry date* to information. The idea behind this approach suggests that individuals will no longer have to worry about their private data being publicly accessible after a certain period established by them. The concept could be enforced in two possible ways. The first approach to implementation of the expiry date solution will be to include it in the metadata. Thus, personal information would be "marked" with an expiry date when the data subject wants the data to stop being accessible to the public, as well as further processed or stored. This proposal would *de facto* be based on the good conscience of the data users (which is reasonably highly doubtful), and would require additional enforcement by law that would oblige the users to comply with it. Since this approach would not necessarily be effective in practice for a number of reasons, including the absurdity of giving an expiration date every time private information is being retained, the alternative way of setting data expiry could be seen as a better option. A second implementation method would be the protection of data as a part of technology. In a comparable way to the DRM (Digital Rights Management) protection used specifically for intellectual property, the expiry date could be included in the data itself. A number of technological solutions have been proposed by researchers that aimed to bypass the possibility of giving an expiration date as a formality (could be compared to the current consent mechanisms, when data users unknowingly or without proper understanding agree to data processing by simply accepting cookie policies, etc.).[241] One of such technological responses is a new technology known as "Vanish". The research department of the University of Washington, USA, has come up with a way to program data to "automatically deconstruct" after a set period of time. This way the will to comply with data processing standards of data users and especially tech giants like Google or Facebook will be no longer necessary. The private data with an expiry date would not accessible anymore.[242] Nevertheless, both approaches to the concept would require sufficient effort from data subjects that want to protect their private data. Academics

[240] D. Burnett, 'Why government censorship [in no way at all] carries greater risks than benefits ' (2015) <https://www.theguardian.com/science/brain-flapping/2015/may/22/government-censorship-psychology-theresa-may> accessed 14 July 2017.

[241] J.Ausloos , 'The 'Right to Be Forgotten' - Worth Remembering?'. Computer Law & Security Review, Volume 28, Issue 2. 143-152. 2011. p. 148.

[242] *Ibid.*. p. 149.

suggest that an expiry date idea will never ensure the complete safety of data or that it will be fully erased.[243]

Another possible solution to the implementation of the right to be forgotten is the alternative to private data erasure - *anonymisation*. The concept proposes that in circumstances when it is possible, from a technological point of view, sensitive personal data could be anonymised by the data controller. Although the data would not be linked to any individual anymore, researchers suggest that unless it is deleted, it could be easily traced and identified. Extensive research has proven that even anonymised data could be retrospectively reversed and de-anonymised.[244] First indication of this theory derived from 1997 research carried out by Latanya Sweeney. The academic provided a great example how data could still be identified despite anonymisation by combining a hospital discharge database, that has been anonymous, and public voting records. The combination resulted in "*identifiable health data*".[245] Similarly, 2008 research by the University of Texas students demonstrated that by putting together the databases of Netflix users and the IMDB movie platform, one could identify the user with an 84% probability once you had information about the country the Netflix account was based at and at least one film that has been rented out by the user.[246] These indications imply that although anonymisation could be a solution in theory, in reality it would be nothing more than a legal loophole to go around the obligation to erase or rectify data.[247]

When assessing the perspectives of the current development of the right to be forgotten, one should mention the necessity of improvement of the existing law and practice. As has been discussed in the previous chapters, the right to oblivion has not been clearly defined in the European legal framework from which it emerged. Although the right is based on the right to erasure enshrined in the 1995 Data Protection Directive and other data protection legislation, the right has not been clearly "put to place" and as a result faces difficulties in practical aspect of its implementation. Some argue that current EU framework already provided individuals with control over their private data. The problem is rather in its

[243] J.Ausloos , 'The 'Right to Be Forgotten' - Worth Remembering?'. Computer Law & Security Review, Volume 28, Issue 2. 143-152. 2011. p.. 149.
[244] P. A. Bernal, 'A Right To Delete?', European Journal of Law and Technology. 2011. p.11.
[245] L. Sweeney, 'Weaving technology and policy together to maintain confidentiality', Journal of Law, Medicine and Ethics, 25 ,1997. pp. 98-110.
[246] A. Narayanan and V. Shmatikov, 'Robust De-anonymization of Large Sparse Datasets', The University of Texas at Austin Press. 2008.
[247] P. A. Bernal, 'A Right To Delete?', European Journal of Law and Technology. 2011. p. 11.

application in practice, which has to be reassessed.[248] the most reasonable suggestions for the updating of the legal framework include "*enhancing data controllers' liability*", which essentially means making the purpose limitation principle have more effective control,[249] as well as clearly defining the understanding of relevance of personal data.[250]

The right to be forgotten can potentially change the future of the Internet. The idea behind data subjects regaining effective control over their personal data bears an array of consequences, both positive and negative. Besides protecting personal data and individuals' right to privacy, it also interferes with freedom of expression and the public's right to know. The direction in which the current discourse on the right to oblivion will move will have to be defined by legal practice, in particular supranational legal institutions like ECtHR and CJEU, that will have to interpret the provisions of current legislation and give practical recommendations on how to apply it in practice. The highly debatable right to be forgotten, that puts fundamental human rights in conflict, will have to be assessed on a case-by-case basis in order to proportionally balance the interests of individuals and that of the public.

[248] J. Ausloos , 'The 'Right to Be Forgotten' - Worth Remembering?'. Computer Law & Security Review, Volume 28, Issue 2. 143-152. 2011. p. 150.
[249] *Ibid.*. p. 150.
[250] *Ibid.* p.151.

Conclusions.

The broader interpretation of privacy of an individual in European law doctrine has resulted into surpassing the known concept of private data erasure. Although the right to be forgotten finds its legal basis in the EU's right to erasure, the emerged framework addresses pivotal privacy issues posed by phenomenon that does not have boundaries - the Internet.

With the main objective of protection of privacy and reputation of the individual, the right to oblivion creates a conflict with other fundamental human rights. The introduction of the right in Europe has sparked a universal debate over potential damage that could be caused by oblivion. A far-reaching wave of resisting the right argues that the right to be forgotten is nothing but a tool for oppression of freedom of expression and universal censorship. Opponents of the right declare that integrity of historical records is endangered and that Europe cannot dictate to the world what content should or should not be accessible on the Internet. Another argument emphasises that the right will bring our reality closer to the Orwellian dystopia of information control and re-writing history that does not fit under the agenda of data controllers or particular states.

But is the danger as imminent as claimed by opponents of the right, or is it a mere emotional reaction based on misconceptions and a misunderstanding of what is being proposed? Taking into account the discussed risks of introducing the right, one may conclude that it appears to be the latter. If the argument is that the right to oblivion will become an absolute censorship, this scenario is hardly possible for a number of reasons. Firstly, the right could be applied only when it meets particular criteria established by law. Thus, in order to restrict online access to a piece of private data, it has to assess what kind of information is in question, whether it remains relevant at the moment and in foreseeable future, who is the data subject in question and how does the removal of search queries affect the interest of the public. Moreover, both search engines and national DPAs are required to comply with international human rights standards and balance the rights in conflict with the proportionality principle. Only this fact completely diminishes the possibility of universal censorship imposed on the Internet, as it would violate the fundamental human right of freedom of expression as well as freedom of press and information, which would not be permitted by the international community.

Another argument against the right to oblivion is stating that the right will erase historical records and possibly re-write history. First and foremost, the practice of removing certain content from Web archives on demand already exists and professionals satisfy the erasure requests in certain circumstances. Secondly, compared to the right to be forgotten, other legal framework could be far more damaging in respect to integrity of the public's memory. Namely, copyright generates a far greater number of memory holes by removing online content. [251] The debate over the potential danger of the right to oblivion for the integrity of historical record should cease to exist after May 2018, when the GDPR comes into force. The Regulation explicitly provides an exception to erasure requests when private data is relevant for the archiving or historical purposes. Hence, the re-writing of history is highly improbable considering the current development of the right to be forgotten.

The real challenges of the right are of the legal or technological nature. From a legal perspective, the implementation of the right appears challenging due to the extraterritorial character of the Internet. The questions of determining jurisdiction and applying data protection regimes remain currently unresolved and pose a substantial challenge for supranational courts in application of their decisions in the online world. Moreover, the vast amount of data and the Internet phenomenon of spreading information at the speed of the light undermine the effectiveness of posing any limitations on the accessibility of private data. In fact, from a practical point of view, any information on the Web could be found, stored and shared.

Therefore, besides the practical aspects of the applicability, the main question in the right to be forgotten discourse should focus on the conflict between the freedom of expression and privacy. Analysing an extensive legal practice around the world, it is impossible to establish a common approach in balancing the two rights; the priorities differ from jurisdiction to jurisdiction. Common-law practice has had a lengthy tradition of weighing freedom of expression over privacy concerns and civil-law practice doing the opposite. Nevertheless, the right to be forgotten doctrine may apply one of the approaches. The CJEU ruling clearly stipulates that "*...it is true that the data subject's rights protected by those articles [7 and 8 of the Charter of Fundamental Rights of the European Union] also override, as a general rule...*" [252] This statement could be regarded as a sign that the Court will consider the right to privacy in

[251] M. Dulong de Rosnay and A. Guadamuz, 'Memory Hole or Right to Delist? Implications of the Right to be Forgotten for Web Archiving'. 2017. p.15. <https://reset.revues.org/807#bibliography> accessed 13 July 2017.
[252] *Google Spain SL, Google Inc. v AEPD and Mario Costeja Gonzalez,* C - 131 /12, CJEU (2014). Para 81.

the right to be forgotten cases over the freedom of expression when the interest of the individual in particular case is greater than the one of the public. Meanwhile, the first ruling of the right to oblivion in Japan has demonstrated a contrasting approach in the balancing of the rights "*any decision to delete information from search results should prioritise the public's right to information*".[253] Consequently, it is reasonable to expect that the approach to the right will vary in different countries. Yet, with the EU being the originator and regulator of the right, it goes without saying that it will establish the direction for the right to be forgotten in the foreseeable future.

Finally, it is important that the public has a better understanding of the idea behind the right. Emotional reactions have a broad political and social impact that complicates the implementation of the tool which could allow individuals to regain control over their private data at a time when it is necessary more than ever. Instead of speculating over unlikely scenarios of universal censorship and the re-writing of history, individuals could benefit from the international community finding new solutions for better protection of privacy rights in the digital era.

[253] Reuters, 'Japanese court rejects demand to remove web search result - media' (2017) <http://www.reuters.com/article/google-japan-privacy-idUSL4N1FM24D> accessed 13 July 2017.

Bibliography

Monographies

Brock, G., *The Right to be Forgotten: Privacy and the Media in the Digital Age,* I.B.Tauris, 160. 2016.

Cooper, G., and S. Whittle, *Privacy, Probity And Public Interest*, Reuters Institute for the Study of Journalism, University of Oxford. 2009.

Hudson, D. L., *The Right to Privacy,* Infobase Publishing. 2009.

Lee, E., *Recognizing Rights In Real Time: The Role Of Google In The EU Right To Be Forgotten.* 49th edn, University of California, Davis. 2017.

Mann, F. A., *The Doctrine of Jurisdiction in International Law,* A.W. Sijthoff, 162. 1964.

Mayer-Schönberger V., *Delete: The Virtue of Forgetting in the Digital Age,* Princeton University Press, Princeton and Oxford. 272. 2011.

Nowak, M., *U.N. Covenant on Civil and Political Rights: CCPR Commentary.* N.P. Engel. 1277. 2005.

Orwell, G., *1984*, New American Library, 648. 1950.

Rainer, A., *The Convergence of the Fundamental Rights Protection in Europe,* Springer, 214. 2016.

Reid, K., *A Practitioner's Guide to the European Convention on Human Rights,* Sweet & Maxwell. 915. 2011.

Van Hoboken, J., *Search Engine Freedom. On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines*, Kluwer Law International, 432. 2012.

Westin, A., *Privacy And Freedom,* Atheneum. 1967.

Journal Articles

Ausloos, J., 'The 'Right to Be Forgotten' - Worth Remembering?', Computer Law & Security Review, Volume 28, Issue 2. 2011. pp.143-152.

Bernal, P., 'A Right To Delete?', European Journal of Law and Technology, 2011.

Brammer H. M., 'The Law: The Right to be Forgotten', ASA Institute for Risk & Innovation, 2015.

Finnemann, N.O., 'Internet - a Cultural Heritage of Our Time', Forskning, 2001.

Koltay, A., 'Elements of Protecting the Reputation of Public Figures in European Legal Systems', Elte Law Journal, 2013.

Koops, B. , 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice', Tilburg Law School Research Paper No. 08/2012 229, 2011, p.256.

Lawrence, S., and C.L. Giles, 'Accessibility of Information on the Web,' Nature, 1999, pp. 107-109.

McNealy, J. E., 'The Emerging Conflict between Newsworthiness and the Right to Be Forgotten', Northern Kentucky Law Review, Vol. 39, No. 2 , 2012. pp.119-135.

Narayanan, A., and V. Shmatikov, 'Robust De-anonymization of Large Sparse Datasets'. The University of Texas at Austin Press, 2008.

Ryngaert, C., 'The Limits of Substantive International Economic Law: In Support of Reasonable Extraterritorial Jurisdiction', Institute for International Law. Working Paper No 99., 2006.

Santin, M., 'The problem of the right to be forgotten from the perspective of self-regulation in journalism', El profesional de la información, v. 26., n.2, 2017. p. 308.

Shapiro, I., and B. Rogers, 'How The "Right To Be Forgotten" Challenges Journalistic Principles'. Digital Journalism. 2016.

Shmueli, B., and A. Blecher-Prigat., 'Privacy for children', Columbia Human Rights Law Review 2011. pp.759-795.

Sweeney L., 'Weaving technology and policy together to maintain confidentiality', Journal of Law, Medicine and Ethics, 25 , 1997. pp. 98-110.

Van Hoboken, J., ‘The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Freedom of Expression Safeguards in a Converging Information Environment’, European Commission, Amsterdam, 2013, p.3.

Legal Sources

African Charter on Human and Peoples' Rights. 1981.

American Convention on Human Rights, 1969.

Constitution of the United States of America, Amendment I, 1789.

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as Amended) (ECHR), 1950.

Directive (EU) 95/46/EC On the protection of individuals with regard to the processing of personal data and on the free movement of such data of the European Parliament and of the Council, 1995.

Guidelines (EU) 14/EN WP 22 5 On the Implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez C - 131/12, Article 29 Data Protection Working Party, 2014.

International Covenant on Civil and Political Rights, 1966.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

Press Release. (EU) 27/17, Court of Justice of the European Union, 2017.

Regulation (EU) 2016/679 On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016.

United Nations Human Rights Committee General Comment No. 34: Article 19: Freedoms of Opinion and Expression, GE.11-45331, 2011.

Universal Declaration of Human Rights, 1948.

Case Law

10 Human Rights Organisations and Others against the United Kingdom, ECHR (2015).

A v Norway, ECHR (2009).

Aaron C. Boring v Google Inc. 09- 2350, United States Court of Appeals (2010).

Benjamin Joffe v Google Inc. 11 – 17483, United States Court of Appeals (2013).

Big Brother Watch v United Kingdom, 58170/13, ECHR (2017).

Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, C-398/15, CJEU (2017).

Campbell v MGN Limited [n.d.] UKHL 22, United Kingdom House of Lords (2004).

Coco v AN Clark (Engineers) Ltd. F.S.R. 415, The High Court of Justice (1968).

Equustek Solutions Inc. v Jack, BCSC 1063, The Supreme Court of British Columbia (2014).

Finger v Omni Publications International, Ltd., 77 N.Y.2d 138, Court of Appeals of the State of New York (1990).

Foster v Svenson, 651826/13 12998, US Supreme Court (2015).

Galella v Onassis , 353 F. Supp. 196, U.S. District Court for the Southern District of New York (1972).

Google Spain SL, Google Inc. v AEPD and Mario Costeja Gonzalez, C - 131 /12, CJEU (2014).

His Royal Highness The Prince of Wales v Associated Newspapers, EWCA Civ 1776, UK Court of Appeal (2006).

Italy v Drummond, De Los Reyes, Fleischer, Arvind,14667/08, Milan Court of Appeals (2010).

Julie Gayet v Closer, Le tribunal de Nanterre (2014).

Liberty and Others v United Kingdom, 58243/00, ECHR (2008).

LICRA v Yahoo!, RG:00/0538, Tribunal de grande instance (2015).

Michael Douglas, Catherine Zeta-Jones, Northern and Shell plc v Hello Ltd., WC2A 2LL, England and Wales Court of Appeal (2000).

Michaels v Internet Entertainment Group, CV 98-0583 DDP, United States District Court for the Central District of California (1998).

Mosley v News Group Newspapers Ltd., EWHC 1777, QB (2008).

Peck v United Kingdom, 44647/98, ECHR (2003).

Pia Grillo v Google Inc., 500-32-130991-112, QQ (2014).

Vederi LLC v Google Inc., 744 F. 3d 1376, United States Court of Appeals, Federal Circuit (2014).

Conferences

'Cross-Border Data Flows and Protection', Hague Conference on Private International Law. Hague, Permanent Bureau, 2010.

Gina Stevens, '*Data Security Breach Notification Laws', Congressional Research Service,* 2012.

Viviane Reding, 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age', Speech/12/26. Innovation Conference Digital, Life, Design, 2012.

Internet Sources

‘Transparency Report . European privacy requests for search removals ' (2017) <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en-US> accessed 13 July 2017.

Balona D. and R. Mahoney, 'Long-ago charge to cost man his home' (2007) <http://articles.orlandosentinel.com/2007-03-21/news/VOFFENDER21_1_matamoros-deltona-incident> accessed 13 July 2017.

Bird&Bird, 'Individual rights | Right to erasure and right to restriction of processing' (2013) <https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/34--guide-to-the-gdpr--right-to-erasure-and-right-to-restriction-of-processing.pdf?la=en> accessed 14 July 2017.

Bowcott, O., 'Right to be forgotten is unworkable, say peers ' (2014) <https://www.theguardian.com/technology/2014/jul/30/right-to-be-forgotten-unworkable-peers> accessed 13 July 2017.

Bruner, J., 'Where the World's Data Is Stored' (Forbes, 2011) <https://www.forbes.com/sites/jonbruner/2011/07/19/where-the-worlds-data-is-stored-infographic/#1341c51373af> accessed 13 July 2017.

Cheshire, T., 'Is Google Trying To Make The Law An Ass?' (2014) <https://www.theguardian.com/media/2003/jan/2http://news.sky.com/story/is-google-trying-to-make-the-law-an-ass-103981439/pressandpublishing.broadcasting> accessed 13 July 2017.

Chou, D., 'More transparency into government requests ' (2012) <https://www.blog.google/topics/safety-security/more-transparency-into-government/> accessed 13 July 2017.

Dean, B.,'Why government censorship [in no way at all] carries greater risks than benefits ' (2015) <https://www.theguardian.com/science/brain-flapping/2015/may/22/government-censorship-psychology-theresa-may> accessed 14 July 2017.

Douglas, M., 'Google expands the ‘right to be forgotten’, but Australia doesn’t need it ' (2016) <http://theconversation.com/google-expands-the-right-to-be-forgotten-but-australia-doesnt-need-it-54887> accessed 13 July 2017.

Drummond, D., 'We need to talk about the right to be forgotten ' (2014) <https://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate> accessed 13 July 2017.

Dulong de Rosnay M. and A. Guadamuz, 'Memory Hole or Right to Delist? Implications of the Right to be Forgotten for Web Archiving' (2017) <https://reset.revues.org/807#bibliography> accessed 13 July 2017.

Dyer, C., 'Suicide bid on CCTV may herald new privacy law ' (2003) <https://www.theguardian.com/media/2003/jan/29/pressandpublishing.broadcasting> accessed 13 July 2017.

'Edward Snowden: Leaks That Exposed US Spy Programme - BBC News' (*BBC News*, 2017) <http://www.bbc.com/news/world-us-canada-23123964> accessed 14 July 2017.

Edwards, L., 'Revenge porn: why the right to be forgotten is the right remedy' (2014) <https://www.theguardian.com/technology/2014/jul/29/revenge-porn-right-to-be-forgotten-house-of-lords> accessed 13 July 2017.

English, K., 'Online Journalism Credibility Project: The Long Tail of News Archives and "Unpublishing" Requests' (2012) <http://www.apme.com/page/Unpublishing> accessed 13 July 2017.

'EU Privacy Removal. Request removal of content indexed on Google Search based on data protection law in Europe' (n.d.) <https://accounts.google.com/ServiceLogin?service=sitemaps&passive=1209600&continue=https://www.google.com/webmasters/tools/dmca-notice?hl%3Den%26pid%3D0%26complaint_type%3D14&followup=https://www.google.com/webmasters/tools/dmca-notice?hl%3Den%26pid%3D0%26complaint_type%3D14&hl=en> accessed 13 July 2017.

European Data Protection Supervisor., 'Glossary - A.' (n.d.) <https://edps.europa.eu/data-protection/data-protection/glossary/a_en> accessed 13 July 2017.

'Factsheet On The “Right To Be Forgotten” Ruling (C-131/12)' (2017) <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf> accessed 14 July 2017.

Fleischer, P., 'Implementing a European, not global, right to be forgotten' (2015) <https://europe.googleblog.com/2015/07/implementing-european-not-global-right.html> accessed 13 July 2017.

Gauberti, A., 'How To Remove Links About Dead People From Google' (*Crefovi*, 2017) <http://crefovi.com/articles/remove-links-dead-people-google-right-forgotten-deceased/> accessed 14 July 2017.

GDPR Portal, 'GDPR Key Changes' (n.d.) <http://www.eugdpr.org/key-changes.html> accessed 13 July 2017.

Gmail Help, 'Google Buzz has gone away' (2011). <https://support.google.com/mail/answer/1698228?hl=en> accessed 13 July 2017.

Goncalves, S., and V. Castro, 'A History of Celebrities Getting Caught with Drugs' (2013) <http://www.complex.com/pop-culture/2013/06/history-of-celebrities-getting-caught-with-drugs/> accessed 13 July 2017.

'Google Admits It Sniffed Out People's Data' (2017) <http://news.techeye.net/security/google-admits-it-sniffed-out-peoples-data> accessed 14 July 2017.

Israely, J., ' Italy's Google Verdict Starts Debate on Web Freedom' (2010) <http://content.time.com/time/business/article/0,8599,1968123,00.html> accessed 13 July 2017.

Kiss, J. 'Dear Google: open letter from 80 academics on 'right to be forgotten' ' (2015) <https://www.theguardian.com/technology/2015/may/14/dear-google-open-letter-from-80-academics-on-right-to-be-forgotten> accessed 13 July 2017.

Koekkoek, B., 'The Territorial Reach Of The EU'S "Right To Be Forgotten": Think Locally, But Act Globally?' (*EJIL: Talk!*, 2017) <https://www.ejiltalk.org/the-territorial-reach-of-the-eus-right-to-be-forgotten-think-locally-but-act-globally/> accessed 14 July 2017.

Kuner, C., 'Extraterritoriality and the Fundamental Right to Data Protection' (2013) <https://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/> accessed 13 July 2017.

Lopez-Curzi, C., '8 Years Since Massive Mass Surveillance Case' (2016) <https://rightsinfo.org/8-years-since-massive-mass-surveillance-case/> accessed 13 July 2017.

MacDonald, C., 'Google's Street View site raises alarm over privacy' (2007) <http://www.heraldscotland.com/news/12778601.Google_apos_s_Street_ViewMacDonald,%20Calum%20%28June%204,%202007%29.%20%22Google's%20Street%20View%20site%20raises%20alarm%20over%20privacy%22_site_raises_alarm_over_privacy/> accessed 13 July 2017.

Magid, L., 'Google Buzz Raises Privacy and Safety Concerns' (2011) <http://www.lexology.com/library/detailhttp://www.huffingtonpost.com/larry-magid/googles-buzz-raises-some_b_455711.html.aspx?g=52594059-1f39-460e-bd85-74a2a3db66af> accessed 13 July 2017.

McCurry, J., 'Japan recognises 'right to be forgotten' of man convicted of child sex offences ' (2016) <https://www.theguardian.com/technology/2016/mar/01/japan-recognises-right-to-be-forgotten-of-man-convicted-of-child-sex-offences> accessed 13 July 2017.

McIntosh, N., 'List of BBC web pages which have been removed from Google's search results' (2015) <http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379> accessed 13 July 2017.

Microsoft, 'Content Removal Requests Report' (2016) <http://www.microsoft.com/en-us/about/corporate-responsibility/crrr/> accessed 13 July 2017.

NY Times, 'Ordering Google to Forget' (2014) <https://www.nytimes.com/2014/05/14/opinion/ordering-google-to-forget.html?_r=0> accessed 13 July 2017.

Nyst, C., 'Two sides of the same coin – the right to privacy and freedom of expression' (2013) <https://www.privacyinternational.org/node/103> accessed 14 July 2017.

Official Google Blog, ' Serious threat to the web in Italy ' (2010) <http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379> accessed 13 July 2017.

Pfanner, E., 'Italian Appeals Court Acquits 3 Google Executives in Privacy Case' (2012) <http://www.nytimes.com/2012/12/22/business/global/italian-appeals-court-acquits-3-google-executives-in-privacy-case.html> accessed 13 July 2017.

Pollard, K., 'Has the EU Given Doctors the "Right to be Forgotten" When Medical Tourism Goes Wrong?' (2014) <https://www.imtj.com/blog/has-eu-given-doctors-right-be-forgotten-when-medical-tourism-goes-wrong/> accessed 13 July 2017.

Reuters, 'Japanese court rejects demand to remove web search result - media' (2017) <http://www.reuters.com/article/google-japan-privacy-idUSL4N1FM24D> accessed 13 July 2017.

Robinson, B., 'Is this the end of the internet as we know it? Thousands rush to apply for their 'right to be forgotten' by having details of their past erased from Google ' (*Dailymail*, 2014) <http://www.dailymail.co.uk/news/article-2644578/Thousands-paedophiles-apply-Google-right-forgotten.html> accessed 14 July 2017.

Rose, A. and K. Ollerhead, 'Data Protection And The Right To Be Forgotten.' (*Uk.practicallaw.thomsonreuters.com*, 2017) <https://uk.practicallaw.thomsonreuters.com/9-518-8790?__lrTS=20170521111238152&transitionType=Default&contextData=%28sc.Default%29&firstPage=true&bhcp=1> accessed 14 July 2017.

Sachdeva, A. and B. Hitchens, 'UK Supreme Court Confirms That There Can Be No Liability For Misuse Of Trade Secrets Unless And Until Confidential Information Is Acquired' (2013) <http://www.mondaq.com/uk/x/251460/Trade+Secrets/UK+Supreme+Court+Confirms+That+There+Can+Be+No+Liability+For+Misuse+Of+Trade+Secrets+Unless+And+Until+Confidential+Information+Is+Acquired> accessed 14 July 2017.

Santos Colnago, C. 'The Right to be Forgotten and the Duty to Implement Oblivion: A Challenge to Both "Old" and "New" Media' (2014) <https://www.jus.uio.no/english/research/news-and-events/events/conferences/2014/wccl-cmdc/wccl/papers/ws14/w14-colnago.pdf> accessed 13 July 2017.

Schechner, S.and L. Fleisher, 'EU Invites Google, Microsoft to Discuss 'Right to Be Forgotten" (2014) <https://www.wsj.com/articles/eu-regulators-invite-google-microsoft-to-discuss-right-to-be-forgotten-1405592730> accessed 13 July 2017.

Scott, M., 'Europe Tried To Rein In Google. It Backfired.' (*Nytimes.com*, 2017) <https://www.nytimes.com/2016/04/19/technology/google-europe-privacy-watchdog.html> accessed 14 July 2017.

'Search Engine Market Share In Europe | Statcounter Global Stats' (*StatCounter Global Stats*, 2017) <http://gs.statcounter.com/search-engine-market-share/all/europe> accessed 14 July 2017.

Sheridan, K., 'One view: ECJ's Google ruling will make it harder to trust search results ' (2014) <http://www.lexology.com/library/detail.aspx?g=52594059-1f39-460e-bd85-74a2a3db66af> accessed 13 July 2017.

Stacey, C., 'The Google effect – Criminal records and the 'right to be forgotten'' (2015) <https://www.ejiltalk.org/extraterritohttps://www.linkedin.com/pulse/google-effect-criminal-records-right-forgotten-stacey-llb-llmriality-and-the-fundamental-right-to-data-protection/> accessed 13 July 2017.

Sterling, G., 'Report: 2 years in, 75 percent of Right to Be Forgotten asks denied by Google' (2016) <http://searchengineland.com/report-2-years-75-percent-right-forgotten-asks-denied-google-249424> accessed 13 July 2017.

Teacher, L. 'Invasion of Privacy is not an acknowledged Tort in the UK' (2013) <https://www.lawteacher.net/free-law-essays/constitutional-law/invasion-of-privacy-is-not-law-essays.php?cref=1 > accessed 13 July 2017.

Temperton, J., 'Unelected peers: EU right to be forgotten is 'unreasonable, unworkable and wrong" (2014) <http://www.expertreviews.co.uk/software/internet-security/1400843/unelected-peers-eu-right-to-be-forgotten-is-unreasonable> accessed 13 July 2017.

The Conseil d'Etat , 'Right to be delisted' (2017) <http://english.conseil-etat.fr/Activities/Press-releases/Right-to-be-delisted> accessed 13 July 2017.

Tippmann, S., and J. Powles, 'Google accidentally reveals data on 'right to be forgotten' requests ' (2015) <https://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests> accessed 13 July 2017.

'Transparency Report. Explore Requests. France.' (2017) <https://www.google.com/transparencyreport/removals/government/notes/?hl=en#authority=FR> accessed 13 July 2017.

'Transparency Report. Explore Requests. Spain.' (2017) <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en-US> accessed 13 July 2017.

'Transparency Report. Government requests to remove content ' (2017) <https://www.google.com/transparencyreport/removals/government/> accessed 13 July 2017.

Truong. A., 'Google Is Giving Revenge Porn Victims The Right To Be Forgotten' (*Quartz*, 2015) <https://qz.com/432939/google-is-giving-revenge-porn-victims-the-right-to-be-forgotten/> accessed 14 July 2017.

Vassall-Adams, G., 'Case comment: Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos, Mario Costeja González' (2014) <https://eutopialaw.com/2014/05/16/case-comment-google-spain-sl-google-inc-v-agencia-espanola-de-proteccion-de-datos-mario-costeja-gonzalez/> accessed 13 July 2017.

Whetstone, R., 'Global Communications and Public Policy. Our approach to free expression and controversial content ' (2012) <https://googleblog.blogspot.co.at/2012/03/our-approach-to-free-expression-and.html> accessed 13 July 2017.

White, A., 'Google EU Ruling Response Vetted As Complaints Pile Up' (2014) <http://www.bloomberg.com/news/articles/2014-09-18/google-eu-ruling-response-vetted-as-complaints-pile-up.> accessed 14 July 2017.

Whittle, S., 'Privacy vs the Right to Know' (2009) <http://reutersinstitute.politics.ox.ac.uk/news/privacy-vs-right-know> accessed 13 July 2017.

Williams, R., 'Google removes link to Telegraph story on deceased pensioner' (2014) <http://www.telegraph.co.uk/technology/google/11060606/Google-removes-link-to-Telegraph-story-on-deceased-pensioner.html> accessed 13 July 2017.

Williams, R., 'Telegraph stories affected by EU 'right to be forgotten'' (2015) <http://www.telegraph.co.uk/technology/google/11036257/Telegraph-stories-affected-by-EU-right-to-be-forgotten.html> accessed 13 July 2017.

Wood, M., 'Google Buzz: Privacy nightmare' (2010) <https://www.cnet.com/news/google-buzz-privacy-nightmare/> accessed 13 July 2017.