TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Social Sciences
Tallinn Law School

Andres Illak

Comprehensive Analysis of the Application of the Right to Be Forgotten in Relation to the Case C-131/12

Master Thesis

Supervisor: Professor Dr. Katrin Nyman-Metcalf

Tallinn 2015

I hereby declare that I am the sole author
of this Master Thesis and it has
not been presented to any other
university of examination.

Andres Illak
“ ..... “ 2015

The Master Thesis meets the established requirements

Supervisor Professor Dr. Katrin Nyman-Metcalf
“ ..... “ 2015

Accepted for examination “ ..... “ 2015

Board of Examiners of Law Master’s Theses

……

Table of Contents

List of Abbreviations

AEPD	Agencia de Protección de Datos
AG	Advocate General
CFREU	The European Charter of Fundamental Rights
CJEU	European Court of Justice
CV	Curriculum Vitae
EC	European Commission
ECHR	European Convention on Human Rights
ECtHR	The European Court of Human Rights
EU	European Union
GDPR	General Data Protection Regulation
ICRI	International Conference on Research Infrastructures
O.J	Official Journal
OSCE	Organization for Security and Co-operation in Europe
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UN	United Nations
U.S	United States of America
WP29	Article 29 Data Protection Working Party

Introduction

The right to be forgotten is a concept that has arisen into debate recently, because it has been applied both within the European Union and beyond, such as in Argentina.[1] Although the right is in essence a positive privacy right for individuals, preventing one's life from being influenced by actions performed in the past, there are many questions that arise. In recent times, the EU court has also backed the application of the right with its case C-131/12[2].

The concept of the right to be forgotten is broad and vague and brings with it some troubling questions about its impact on freedom of expression, the censorship of history, historical truth etc. Is application of the right even possible in light of upcoming EU data protection regulation?[3] Furthermore, where is the balance between freedom of speech and the right to be forgotten, and dealing with media – what is newsworthy enough to fit the criteria of journalistic purposes? There is also the vital question of whether the right to be forgotten should be given the status of an international human right.[4]

Although these are only a few of the problematic questions that arise, there is another aspect of this issue that is linked to privatization of the right to determine the definition of the right to be forgotten. Will it be Google that determines what makes history?

It has to be emphasized that the C-131/12 ruling is controversial and some questions were answered but far from everything, there will no doubt be attempts to re-visit the questions.

As a new and a broad concept, there is a vital need for a comprehensive research on the topic of the right to be forgotten.

---

[1] E.L. Carter, *Argentina's Right to be Forgotten*, Emory International Law Review, 27, at 23-39 (2013)
[2] Judgment of 13 May 2014 in case C-131/12, *Google Spain and Google*, Google Spain SL, Google Inc. v. Agencia de Protección de Datos (AEPD),Mario Costeja González, CJEU
[3] European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Brussels, COM(2012) 11 final 2012/0011 (COD) (25 January 2012) (hereafter GDPR Proposal)
[4] H. Nys, *Towards a Human Right 'to be Forgotten Online'?*, European Journal of Health Law, 18, at 469-475 (2011)

Imagine a situation in which a 40 year old man with a good education and reasonable job experience one day finds himself unemployed. The company he worked for had economic difficulties and the man was discharged. He now looks through the ads in a local newspaper and identifies a job that he finds interesting. He sends his CV and cover letter and hopes for the best. A couple of weeks go by and he receives a phone call announcing that he has been chosen to attend an interview for the vacancy. The applicant is excited and starts preparing for the meeting.

The big day arrives and the man heads to the interview at what he hopes is his soon-to-be workplace. When it comes time for his interview, he enters the room where a committee asks him questions and discusses his qualifications. He leaves the interview and heads back to his apartment, feeling that everything went even better than expected.

Meanwhile the committee is making their decision and finds that the applicant is a great choice for the job. Before making their final decision, as employers are wont to do nowadays, the committee searches the Internet for information about the prospective applicants. After typing in the name of the applicant, the first thing that appears in the search engine results list is an article about the man in question having been arrested for alleged attempted rape. The events in the article, published on a local newspaper's website, occurred more than 20 years in the past. After viewing the article, the committee quickly decides that the man in question is not the right man for the job and sends him a letter explaining that he, unfortunately, has not been chosen to fill the vacancy.

In reality, after the man's arrest prosecutors dropped the charges completely and the man's record was expunged. Though more than twenty years had passed, the original article still exists in the online version of the paper.
Anyone who searches for the man's name will find the article among the top search engine results.

One can only imagine how much trouble an individual may have due to the inaccurate, inadequate, irrelevant or excessive information that can be found in the Internet. Such information plays a significant role in a person's life, as for example in our fictional example of one man's job hunt. Although the person is not guilty, the newspaper is not required to remove the article or correct it, and it may stay online in perpetuity. Public opinion may be formed more on the basis of an inaccurate article than the juridical reality of an individual's record.

A solution to the concerned person's interest in having the information removed can be found in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[5]

With regards to the previous, the European Commissioner for Justice, Fundamental Rights, and Citizenship, Viviane Reding, announced, in January, the European Commission's proposal to create a new privacy right that is called the right to be forgotten.[6]

The proposed right has been depicted as a modest expansion of existing privacy rights, but in fact it poses a serious threat to freedom of speech in the Internet era. It could make Internet actors like Facebook and Google liable for up to two percent of their income if they are not able to remove data about individuals once it becomes undesirable.[7] Although the uploader is not the one liable for removal and the data may be widely distributed, the burden is still upon them to fulfill the application of this right. So with this there is a fine balance between the right to privacy and free speech that could lead to a less open Internet.

The aim of this research is to identify the feasibility for actual implementation of the right to be forgotten, and to explicate the problematic aspects and critiques of the concept. Through a comprehensive analysis it will be thoroughly explored and explained, and the broad aim of this thesis is a comprehensive overview of the topic surrounding the right to be forgotten, with its pros and cons.

A broad question that may serve to introduce the topic is as follows: is the right to be forgotten compatible with other rights, and is the application of the right actually possible and proportionate?

Answering this question is no easy task, and requires a complex methodology that combines

---

[5] European Union, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Official Journal L 281 , 23/11/1995 P. 0031 – 0050, (24 October 1995)
(hereafter Directive 95/46/EC [Data Protection Directive])
[6] J. Rosen, *Symposium Issue: The Right To Be Forgotten*, Stanford Law Review Online, 64, at 88-92 (2012)
[7] Ibid.

aspects of primary research and secondary research techniques. Secondary data will be used through literature reviews and articles composed by other authors. In addition, case-studies will also be conducted and compared with existing literature and research. This is supported by comparisons of different legislation and legal proposals. In order to achieve its aims, both primary and secondary research techniques will be utilized and the research will also include empirical and comparative research methods. In order to address the questions above, some examples related to social media/Internet media and privacy are taken under consideration: court cases, articles and opinions. In addition, the European Convention on Human Rights[8] and other international law is covered in this thesis.

The issue at hand is derived from the newly established right for a person to be forgotten in accordance with new data protection reforms. The main contribution of this paper is to assess the right to be forgotten from a legal perspective, and to bring it together with other conflicting rights like freedom of expression. There is a critical point of view that highlights problematic issues that have been indicated by other authors who are conducting research in this area.[9] The legal status of the right to be forgotten is still uncertain, and thus it must be clarified. Attention is mostly given to the European approach, but there are some examples that will be considered from other countries like the United States of America.

This paper is divided into several different sections and subsections. The first section contains a description of broad Internet privacy situation and the European Union data protection law in place today, as well as ongoing data protection reforms. This section also gives a definition of the right to be forgotten, as it is actually a broad concept in need of clarification.

The second section will discuss a European Court judgment[10] that has supported the right to be forgotten in the European Union, certain aspects of which are specified in the court case and have an important role in the further implementation of the right itself.

The following sections deal with criticism of and conflicts with the right to be forgotten. This includes an analysis of the relation between freedom of speech and the right to be forgotten, as

---

[8] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, (4 November 1950) (hereafter ECHR)
[9] B.-J.Koops, *Forgetting footprints, shunning shadows: A critical analysis of the 'right to be forgotten' in big data practice*, SCRIPTed, 8, 3, at 233 (2011)
[10] Case C-131/12, *Google Spain and Google*

well as a discussion of historic truth and its possible ambiguity. Further, analysis of the delegation of rights and privatization of the implementation of the law will be considered. The shaping of history is an important aspect of this debate, as data controllers seem to have an important role to play with regard to the Internet.

Consequently, the theoretical first section of the thesis that describes the legal framework of the right to be forgotten is supported by the second, empirical portion of the thesis, which describes the real situation with regard to the right to be forgotten. The constraints of this thesis do not allow every significant aspect of the right to be forgotten to be addressed in detail, and it will therefore focus on the legal implications of the right. As this is a thesis in legal studies, it concentrates primarily on the legal aspects of the right to be forgotten and data protection. There are also moral, ethical, and sociological sides to the right that invite analysis by specialists in these respective fields.

A. Internet Privacy

Defining privacy is essential to the description and application of the right to be forgotten, as it is to protect an individual's privacy that the right is proposed in the first place. Therefore, it is essential to discuss the three definitions on which the argument in this thesis is based.

Privacy is the desire of an individual to be free of intrusion.[11]

"...the state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion."[12]

An important aspect of privacy is the ability to exclude others from the premises. The right to be free from intrusion or interference is a key element of privacy.[13]

Privacy may also be defined as the right of the individual to determine when, how, and to what extent he or she will release his personal information. A reasonable expectation of privacy demands that an individual may assume, that only in circumstances where it is established that an offence has been or is being committed, and the interception of private communications stands to afford evidence of the offence.[14]

As the above definitions illustrate, privacy is the notion that an individual ought to have control over his personal life and the information related to it.

Having established this broad definition of privacy, we come to the primary focus of this thesis.

The advent of the Internet has generated previously unimaginable ways to intrude upon the privacy of individuals and to communicate that information globally. In today's society, as

[11] G. Black, Publicity Rights and Image, Oxford: Hart Publishing, at 61-62 (2011)
[12] R v Edwards, Supreme Court of Canada, 24297 (1996)
[13] Ibid.
[14] R v Duarte (also *R v Sanelli*) Supreme Court of Canada, 20542 (1990)

Richard A. Spinello has said: "Each of us can become an open book to anyone who wants to take the time to investigate our background."[15]

This opinion is supported by the growing impact of technology and the Internet, from Facebook and Google Street View to the innumerable other Internet-based-media accessible to an ever-increasing number of persons and institutions. It takes only minutes to spread information – true or false – globally, and it could be said that nowadays, London is as distant as Tokyo or Nigeria. Distances no longer matter and time is no obstacle.

There are approximately 2,5 billion Internet users in the world at this moment[16], making fully 1/3 of the world's population Internet users. By These figures suggest that nothing will remain confidential if someone really wishes to spread the word around.

However in a digitalized world, where a lot of actions like paying bills and shopping are conducted through the Internet, relying on it for the satisfaction of our daily needs, secret wishes or simply for keeping up the illusion of not being alone through online chats, the actual amount of information we put out there about ourselves is enormous. The digital profiles of ourselves and the digital traces we leave have grown to become a threat to our future development and our privacy for that matter.[17]

A recent example of the power of the Internet, to rapidly spread information and to instigate social and political change, was the "Arab Spring", for which Palestinian protesters used Facebook for organizing their meetings.[18] Use of the Internet as a tool for communication and spreading information and data can also be shown by the "Wikileaks"[19] webpage and the situation related to the blogger Malala Yousufzai[20]. As the significance of the Internet as a

---

[15] R.A. Spinello, The End of Privacy, America, at 12 (1997)
[16] Miniwatts Marketing Group. (2012) http://www.internetworldstats.com/stats.htm, accessed 12.2014
[17] A. Giurgiu, *Challenges Of Regulating A Right To Be Forgotten With Particular Reference To Facebook*, 7(2), Masaryk University Journal Of Law And Technology, at 362 (2013)
[18] K. Flower, *Facebook page supporting Palestinian intifada pulled down,* Cable News Network. Turner Broadcasting System, Inc. (2011) http://edition.cnn.com/2011/WORLD/meast/03/29/palestinian.facebook/index.html?_s=PM:WORLD accessed 12.2014
[19] Wikileaks, http://wikileaks.org/About.html (2011) accessed 12.2014
[20] S. Khan, *Taliban attack wounds teen activist blogger,* Cable News Network. Turner Broadcasting System, Inc. (2012) http://edition.cnn.com/2012/10/09/world/asia/pakistan-teen-activist-attack/ accessed 12.2014

medium for information and communication becomes increasingly evident, conflicts with privacy laws inevitably arise. Indeed, this state of affairs challenges us to question whether the existing notions of privacy and laws protecting it remain relevant today.

In general, there exist two primary instruments for privacy and data protection in the European Union. The first of these is The Convention for the Protection of Human Rights and Fundamental Freedoms, also known as the European Convention on Human Rights[21], signed in 1950 by the 12 Member States of the Council of Europe. The Convention on Human Rights was the first legal instrument to support the Universal Declaration of Human Rights[22] and to confer a binding effect on certain of the rights established in the Declaration.[23]

The ECHR was the first treaty that established the European Court of Human Rights, which ensures the safekeeping of human rights. After Member States had accepted the court, it could challenge the decisions made by those Member State courts, where they concerned issues of human rights. With that supranational organization, human rights gained importance in Europe. In order to join the European Council, states were required to sign and ratify the European Convention on Human Rights.[24] The most significant aspect of the ECHR and the European Court of Human Rights is summed up in the following declaration:

"Any individual, group of individuals, company or non-governmental organization can apply to the Strasbourg Court, provided that they have exhausted all domestic remedies."[25]

The European Charter of Fundamental Rights[26] is a more modern instrument, proclaimed at the Nice European Council meeting on December 7, 2000. The CFREU takes into account new developments in technology and society and thus updates the provisions of the ECHR. In the beginning the CFREU had no binding legal effect, but on December 1, 2009 it came into force

[21] ECHR
[22] UN General Assembly, *Universal Declaration of Human Rights*, 217 A (III), (10 December 1948) (hereafter UDHR)
[23] ECHR
[24] ECHR
[25] Ibid.
[26] European Union, *Charter of Fundamental Rights of the European Union*, 2012/C 326/02, (26 October 2012) (hereafter CFREU)

with the Treaty of Lisbon[27]. The CFREU clarifies and strengthens the protection of fundamental rights by making them more visible and explicit for citizens.[28]

The right to privacy as a human right has been seen as the basis for data protection in Europe. In the ECHR, privacy is covered in Article 8:

"Right to respect for private and family life

Everyone has the right to respect for his private and family life, his home and his correspondence.
There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[29]

The scope of ECHR Article 8 paragraph 1 is thus as follows:

Private life – The ECHR embraces personal autonomy, the right to make choices regarding one's own life without interference by the state, to develop one's own personality and to establish relationships with others and to communicate. It includes the physical and psychological integrity of a person, sex life and gender, personal data, reputation, names and photos.[30]

Family life - ties between persons related by blood or marriage, the central relationships of family life are those of husband and wife and parent and child. It also covers the ties between siblings, grandparents and grandchildren or uncle/aunt and nephews/niece, in some cases. In other cases, the European Court of Human Rights applies a number of criteria (such as duration of the relationship, cohabitation) in order to ascertain whether a given relationship is embraced by the right to family life under article 8 of the ECHR.[31]

---

[27]European Union, *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*, 2007/C 306/01, (13 December 2007)
[28] CFREU
[29] ECHR, at Art. 8
[30] Ibid.
[31] Ibid.

Home - is the physically defined place where private life and family life develops. It does not matter whether this space is the property of the affected person or even legally inhabited. The notion also may also encompass business premises, temporarily inhabited spaces or caravans.[32]

Respect for correspondence - the right for uncensored and uninterrupted communication. The article does not refer to letters only; it is acknowledged that article 8 also affords protection to communication via the phone, fax, parcels, telexes, Internet or private radio.[33]

In more modern instruments, most notably the European Charter of Fundamental Rights, data protection is mentioned as a separate right on its own. Protection of personal data is covered under Article 8 of the CFREU, which states:

"1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."[34]

Article 7 of the CFREU also covers the right to respect for private life:

"Everyone has the right to respect for his or her private and family life, home and communications."[35]

As privacy and the right to respect for private and family life are currently established and defined – under the ECHR and the CFREU – it is clear what actions may potentially infringe upon this right. Although there are exceptions in paragraph 2 of the article, the issues described in the following are not justified under those considerations.

Mark Gibbs highlights two different meanings, or contexts, of privacy. The first he calls "factual privacy", which concerns what one may consider "static" data about a person. The other aspect

[32] Ibid.
[33] Ibid.
[34] CFREU, at Art. 8.
[35] Ibid., at Art. 7.

of privacy Gibbs refers to as "real time" or "life stream" privacy: this in broad sense is the freedom to go about our business unobserved and anonymously. This "life stream" privacy is increasingly threatened as different Internet actors collect data about individuals, and as many voluntary applications broadcast and collect this kind of data about one's personal life.[36]

I. European Union Data Protection Directive

The data protection legislation that is in place in the European Union is built primarily upon the Data Protection Directive[37] which regulates the processing of personal data.

As mentioned above, privacy is also covered in the ECHR under Article 8, which provides the right to respect for one's private and family life, home and correspondence[38], as well as the CFREU that covers the right to data protection and the right to the respect for private life. There are some justified exceptions but they are not relevant to the present discussion. The Member States of the EU have signed and agreed to the ECHR and the CFREU, and they must honor the right to privacy outlined therein.

The data protection directive was adopted in 1995, at a time when several Member States already had their own national data protection laws.[39] The rationale for a unified data protection directive argued that the free movement of goods, capital, services and people, in the EU's internal market, required the free flow of data. That free flow of data could not be achieved unless Member States had a uniformly high level of data protection. Although Convention 108[40] was already in place, the Data Protection Directive was designed to add to the principles of privacy that were contained in that Convention.[41]

---

[36] M. Gibbs, *Freedom and privacy, R.I.P*, Network world (2011) http://www.networkworld.com/article/2179900/security/freedom-and-privacy--r-i-p-.html accessed 12.2014
[37] Directive 95/46/EC (Data Protection Directive)
[38] ECHR, at Art. 8
[39] *European Union Agency for Fundamental Rights, Council of Europe – European Court of Human Rights* , Handbook on European data protection law, Belgium, 17-18 (2013) (hereafter Handbook on European data protection law)
[40] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, CETS No. 108, (28 January 1981)
[41] Handbook on European data protection law, at 17-18

The Data Protection Directive defines the basic elements of data protection in the EU, and Member States must transpose those elements into their national laws.[42] Each Member State then manages the regulation and enforcement of data protection within their own jurisdiction. Although the Data Protection Directive, with its purposes of the free flow and protection of data, was a positive regulation, in accordance with Framework Decision 2008/977/JHA[43], technological developments in the intervening years have raised new challenges and concerns for the protection of personal data. The amount of data that is shared and collected has drastically grown and modern technology allows companies and authorities to use personal data on a tremendous scale. By providing access to such data, technology has transformed the social and economic realities of the world as we know it. The European Commission has thus concluded that a more comprehensive and coherent policy regarding the right to personal data protection is needed.[44]

From this perspective, data protection is an essential component to the social and economic functioning of modern nations, and the European Union is justified in its efforts to ensure the establishment and application of these protections. However, an alternative perspective suggests that the loss of privacy is an unfortunate but unavoidable consequence of the information age and developing technology – a necessary cost of doing business when information is the economy's most vital asset. In this case, should privacy seen by ordinary citizens and public policy makers as a trivial, even antiquated right unworthy of their attention? Or have individuals become the powerless victims of a technology that has stripped away their essential right to privacy?[45]

Governmental organizations have databases overflowing with information, while personal information of the most trivial or significant kind is freely available on the Internet. Security cameras survey public and private spaces, computers are ubiquitous, smartphones abound, and data travels instantly and constantly across continents and media with an unimaginable speed and frequency. One might be tempted to ask whether, in this technological environment, there

---

[42] Electronic Privacy Information Center, http://epic.org/privacy/intl/eu_data_protection_directive.html#background accessed 08.2014

[43] Council of the European Union, *Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, Official Journal J L 350, (27 November 2008)

[44] GDPR Proposal

[45] Spinello (1997), at 9

exists the need or even possibility for data protection, security, or even privacy itself. Yet the desire for privacy and individuals' insistence on its guarantee persists, and privacy constantly reasserts itself as a fundamental and precious right, irrespective of the changing technological landscape.

The fight for privacy has recently gained attention in print, television, the Internet and other media.[46] Individuals are becoming more aware and better informed about the technology that surrounds them, and thus also about how their privacy is being compromised in various large and small ways. Some have begun to take simple measures to protect their privacy, for example by making only cash transactions, refusing to provide their Social Security numbers – or providing false ones – or entering false data into registration forms and other documents. People have started to speak out in favor of technology with privacy, and have begun to develop systems and services that protect rather than compromise privacy.[47]

While some assume that privacy is not compatible with an environment where data moves as fast and freely as our technology now allows[48], others, both individuals and institutions, have begun to take steps to prevent the loss of privacy. Implementing new data protection reforms is a strong push in the latter direction, and, as explained below, the motivation for this move comes primarily from the Internet, technology and its developments.

1. Reform of Data Protection Legislation

On January 25, 2012 the European Commission finally proposed an overwhelming reform plan on the data protection rules that have been in place since 1995. The reform is supposed to strengthen online privacy rights and with that give a boost to the EU's digital economy.[49] The logic behind this reform is that the rapid change that has come with technological progress and globalization demands corresponding changes to policy. The way data is collected, used and

[46] S. Garfinkel, Database Nation: The Death of Privacy in the 21st Century, O'Reilly Media inc., at 9 (2000)
[47] Ibid.
[48] D.J. Solove, *The End of Privacy?*, 299, Scientific American, 3, at 100-106 (2008)
[49] European Commission, *Commission proposes a comprehensive reform of the data protection rules* http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm accessed 09.2014

accessed has changed and with that, Member States have implemented the previous, 1995, rules differently. By using different approaches, Member States have achieved a result in which there are many divergences in the rules enforcement.[50] This is among the primary reasons that the EU is in need of a single, comprehensive regulation. After reform there should be no fragmentation and with that the administrative costs and costs to businesses are projected to lead to savings of around 2.3 billion Euros a year.[51] The European Commission also hopes that the initiative will help to encourage consumer confidence and thus provide a boost to employment and innovation.[52]

The reasoning is made explicit in an EC memo that describes the situation as follows:

With the development of social networking sites, cloud computing, location-based services and smart cards, the amount of digital traces being left with an individual's every move, is enormous. In order to protect the right to personal data protection, that is recognized by the EU Charter of Fundamental Rights, in Article 8 and in Article 16 of the Treaty on the Functioning of the European Union. With the previous documents signed, the EU has new responsibilities to protect personal data in all areas of EU law, including police and judicial cooperation. The legislation that is in place in Europe, has applied since 1995. Although the Data Protection Directive guarantees the protection of the fundamental right to data protection, there are differences in the way that each EU Member State implements the law. Those differences have thus led to inconsistencies, which create complexity, legal uncertainty and administrative costs. With the previous, affecting the trust and the confidence of individuals as well as the competitiveness of the European economy and the current need for modernization, because of the rapid development of online services, there is a need for a reform of data protection rules.[53]

Social networking brings with it a host of problematic issues and questions as well. Social networks are a useful and enjoyable means of staying in touch with friends and family, but this activity is not without risk. Information shared on these networks may be distributed more widely than individuals imagine and foresee, and there may be financial, reputational and psychological consequences unique to the medium. Around 66% of Europeans polled think that

[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] European Commission, *Data protection reform: Frequently asked questions*, (25 January 2012) http://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=en, accessed 08.2014

publishing personal data is an increasing and an essential aspect of modern life, but at the same time an even greater 72 percent thinks that there is too much of their data is available online[54]. People feel that they are not in direct control of their own data.

It is for these reasons that the European Commission proposes a strengthened right to be forgotten so that if an individual no longer wants his personal data to be processed, and there is no legitimate reason for a data processor to keep it and it must be removed from their system. The burden of proof is reversed so that controllers must prove that they need to keep the data, rather than an individual having to prove that collecting their data is not necessary.[55]

Another important change is that online service providers must act upon the principle of 'privacy by default', which means that the default privacy settings should be those that provide the most privacy. An individual should have the best possible option to decide what data he shares and for that, companies are obliged to inform individuals as clearly, understandably and transparently as possible about how their personal data will be used.[56]

With these provisions in place, an individual's access to his own data will be made easier and portability – that is, the ease of data transfer between service providers – is enhanced.[57] The further implications have to do with individuals giving consent to the use of their personal data. The agreement is made clear, and consent must be given explicitly and with full awareness of its implications. These measures are meant to bring about a more trustworthy online environment.[58]

In its press release[59] the European Commission has highlighted the key changes that come with reform of the data protection rules in the EU:

With data protection legislation in the EU becoming a single set of rules on data protection that are valid across the EU, there will be some benefits like the removal of unnecessary

---

[54] European Commission, How will the data protection reform affect social networks? http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf, accessed 08.2014
[55] Ibid.
[56] Ibid.
[57] Ibid.
[58] Ibid.
[59] European Commission, *Data protection reform: Frequently asked questions*, (25 January 2012) http://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=en, accessed 08.2014

administrative requirements, such as notification requirements for companies. This will help save EU businesses around €2.3 billion a year.[60]

A single set of rules in this case is an important aspect of these reforms, and is discussed in the comparison of directive and regulation below. Legislation enacted following data protection reform will be regulatory, and that, as we shall see, is of great importance.

Current obligation is that all companies have to notify all their data protection activities to data protection supervisors. This requirement has proven to lead to unnecessary paperwork and costs. The costs that accompany the requirement are about €130 million per year. The upcoming GDPR provides increased responsibility and accountability for those who are processing personal data. An example is set that companies and organizations have an obligation to notify the national supervisory authority of serious data breaches, if feasible within 24 hours, but in any case as soon as possible.[61]

This change actually puts more responsibility on the processing party and will bring with it many of the issues that are discussed later in this thesis.

"Organizations will only have to deal with a single national data protection authority in the EU country where they have their main establishment. Likewise, people can refer to the data protection authority in their country, even when their data is processed by a company based outside the EU. Wherever consent is required for data to be processed, it is clarified that it has to be given explicitly, rather than assumed."[62]

The section quoted above concerns organizational changes which allow organizations to refer to a single authority on data protections, rather than dealing with several data protection authorities as before the implementation of regulation. Regulation is directly applicable to individuals and companies and thus unifies the rules in the EU.

[60] Ibid.
[61] Ibid.
[62] Ibid.

Another accompanied change is that individuals will have easier access to their own data and they are also able to transfer personal data from one service provider to another more easily With the right to data portability competition among services will improve.[63]

As this change is not directly related to our topic, it will not be further discussed in the thesis.

"A 'right to be forgotten' will help people better manage data protection risks online: people will be able to delete their data if there are no legitimate grounds for retaining it."[64]

The right to be forgotten is the most attractive change in the data protection reforms process. This right has been the subject of much discussion and is the central topic of this thesis. The right to be forgotten will give individuals greater control over their personal data on the Internet.[65]

"EU rules must apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens."[66]

The above declaration represents an important change, stating that even for cases in which a company or its servers are situated outside of the European Union, they are still responsible under EU law if they are active in the EU market. This is obviously a change in response to the rapid development of the technology sector and especially the growth of the Internet.

"Independent national data protection authorities will be strengthened so they can better enforce the EU rules at home. They will be empowered to fine companies that violate EU data protection rules. This can lead to penalties of up to €1 million or up to 2% of the global annual turnover of a company."[67]

---

[63] Ibid.
[64] Ibid.
[65] J. McNealy, *The Emerging Right to be Forgotten: How a Proposal in Europe Could Affect the Sharing of Information*, 12, Insights on Law **&** Society, 3, at 14 (2012)
[66] European Commission, *Data protection reform: Frequently asked questions*, (25 January 2012) http://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=en, accessed 08.2014
[67] Ibid.

Creating the possibility to levy fines against companies is important in conjunction with the right to be forgotten and the redistribution of responsibilities. Companies are now responsible for certain tasks that have no clear guidelines, and this, on the other hand, may prove to be a threat to the freedom of the Internet and freedom of speech.

Finally a new regulation will apply general data protection principles and rules for police and judicial cooperation in criminal matters and the rules will apply to both domestic and cross-border transfers of data and thus have a wider reach than the previous Data Protection Directive.[68]

As can be seen, one of the key changes to data protection provisions concerns the right to be forgotten:

The right to be forgotten will help individuals to better manage data protection risks that appear online. With the right, people will be able to delete their data if there are no legitimate grounds for retaining it in an online source.[69]

The right to be forgotten would be ineffective if the rules established to protect it do not apply to non-European companies, including search engines.[70] That is why the new regulation leaves no doubt that the physical location of the server, of the data processing company, has no importance in implementing European data protection rules.

The European Commission has also reversed the burden of proof: the data processing company is now liable for proving that the data is still relevant and can't be deleted.[71]

The next important change with regard to the right to be forgotten is that the controller, who has made personal data public, is required take reasonable steps to inform other third party actors when an individual requests that his data be deleted. The European Parliament amended this point to include the obligation of the controller to ensure the erasure of data. The final addition

[68] Ibid.
[69] Ibid.
[70] European Commission Factsheet about data protection http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, accessed 08.2014
[71] Ibid.

stated that an individual has the right to erasure when a court or another regulatory authority, based in the EU, has ruled that the data must be erased.[72]

In the previous directive, the right to be forgotten was noted under Article 12(b)[73]. This Article stated that a Member State shall guarantee any data subject the right to obtain from the controller the following:

"(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;"[74]

In the forthcoming regulation, the European Commission suggested the right to be forgotten in its proposal[75], in a clarified form, as Article 17:

"1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:"[76]

The grounds for removal are divided into different subsections of the Article:

"(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
(c) the data subject objects to the processing of personal data pursuant to Article 19;
(d) the processing of the data does not comply with this Regulation for other reasons."[77]

---

[72] Ibid.
[73] Directive 95/46/EC (Data Protection Directive), at Art. 12(b)
[74] Ibid.
[75] GDPR Proposal
[76] Ibid., at Art. 17
[77] Ibid.

The first section of the Article thus concerns with the rights of data subjects as it gives them the positive right to erase information that is about them. This section emphasizes the point that the data subject, when making the data available, may have been a child or a young adult.

"2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorized a third party publication of personal data, the controller shall be considered responsible for that publication."[78]

This section refers to the responsibilities of the data controller. One important implication of this section is that the controller is responsible for third party actors who process data that has been published by the data controller.

"3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:
(a) for exercising the right of freedom of expression in accordance with Article 80;
(b) for reasons of public interest in the area of public health in accordance with Article 81;
(c) for historical, statistical and scientific research purposes in accordance with Article 83;
(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;
(e) in the cases referred to in paragraph 4."[79]

This section lays out the timeline for erasure but also implies that there are several exceptions and justified grounds on which to refuse the implementation of the right to be forgotten.

As we have shown, the revised Article 17 specifies the right of erasure and provides certain conditions for the application of the right to be forgotten, including the obligation of the

[78] Ibid.
[79] Ibid.

controller to inform third parties of the data subject's request for erasure.[80] The proposal also "integrates the right to have the processing restricted in certain cases, avoiding the ambiguous terminology 'blocking'."[81]

Once again the European Commission states that anyone should have the right to be forgotten.[82] They point out that subjects need to have the right to have their personal data erased when it is no longer necessary for the purpose to which it was collected and processed, or when subjects have withdrawn their consent for processing. The right to be forgotten is particularly relevant when an individual/data subject has given consent as a minor, not fully aware of the risks involved, and now wants to remove that data from the Internet.

The EC reaches an important conclusion in its proposition, allowing the further:

"retention of the data where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them."[83]

The European Commission has made its proposal, and the European Parliament has also had their say and added the following paragraph to amend the EC's view on the right to be forgotten:

"...and to obtain from third parties the erasure of any links to, or copy or replication of that data, where one of the following grounds applies:"[84]

In order for the Regulation to become law, it must be approved by a European Council comprised of ministers of the EU Member States that should happen in 2015.[85] There are also assumptions that, given the lengthy European Parliamentary process and the matters which remain outstanding, it seems more likely that the Regulation will be finalized in late 2015 or in

[80] Ibid., at Art. 9
[81] Ibid.
[82] Ibid., at Art 25-26
[83] Ibid.
[84] European Commission Factsheet about data protection http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, accessed 08.2014
[85] European Council, Brussels, EUCO 169/13, (25. October 2013) http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf accessed 12.2014

2016 and the GDPR will be effective two years after it has been finalized and adopted by the European Parliament.[86]

2. Directive vs. Regulation

The biggest change regarding data protection reform is the distinction between the application of a directive and the application of a regulation. The basic definition of the differences between different EU legal acts is given in the TFEU:

"To exercise the Union's competences, the institutions shall adopt regulations, directives, decisions, recommendations and opinions.
A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States.
A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods."[87]

A regulation is a legal act that is generally applicable, it shall be binding in its entirety, for an unlimited number of targeted individuals and is directly applicable in the Member States after the entry into force. It is given by the European Parliament, European Council and the European Commission and is a general act that is binding in all Member States.[88] This means that Member States have a duty to apply the regulation prior to their own national law. Member States also have an obligation not to violate the principle of the direct application and to comply with the European Court's interpretation.
Regulations are the most far-reaching type of legislation in EU law. They are abstract, generally regulatory, targeted at an undefined number of people and need not conform to national law.

---

[86] C. Lynch, P. Whitaker, The General Data Protection Regulation:update on the latest developments, (2014)
http://www.lexology.com/library/detail.aspx?g=49dc9633-e8d6-4cf9-abeb-348a6b59a464 accessed 12.2014
[87] European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, 2008/C 115/01, (13 December 2007) (hereafter TFEU)
[88] J. Steiner & L. Woods & C. Twigg-Flesner,. EU Law, 9th ed., Oxford, Oxford University Press, 56–60 (2006)

Regulations are applied to the entire territory of the EU and implementing national law is not allowed when it conflicts with a regulation.

A directive, on the other hand, is applied to national targets and aims to harmonize Member States' legislation. The broad reasoning behind this is the single market objective that needs a somewhat harmonized environment.[89] "National target" means that a Member State must adopt a national law that follows the provisions and guidelines of the directive.[90] Broadly, a directive is a result that must be achieved by each Member State, but it leaves open the choice of form and methods to the Member States' national authorities.

Unlike regulations, directives are not usually directly applicable, but require transposition into national law. Member States are obliged to adhere to the goals, deadlines and other requirements that are set out in directives but they have the right to choose the form of necessary national measures.

To sum up the previous sub-chapter, a directive, under European Union law, is legislation that serves as a guideline for a Member State and forces each Member State to transpose the legal act into its own national legislation within a specified period of time and following other requirements[91]. A regulation, however, does not need clear transposition and is an obligatory part of law within each Member State since its adoption.[92]

Therefore, in essence, proposing a regulation before a directive seeks to create a universal data protection law that is unified and applicable immediately upon the enactment of the GDPR Proposal.[93]

[89] European Union, http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm, accessed 12.2014.
[90] Steiner, Woods, Twigg-Flesner, at 56–60 (2006)
[91] D. Bender, A Guide to Cyberlaw and Data Privacy, §51.04 (rev. 2013); *CDT Analysis of the Proposed Data Protection Regulation*, CTR. for Democracy & Tech." (2012) https://www.cdt.org/files/pdfs/CDTDPR-analysis.pdf accessed 08.2014
[92] Ibid.
[93] Bermann *et al*, Cases and Materials on European Union Law 230, 3rd. ed., at 230 (2011)

II. The Right to Be Forgotten

This section cannot be correctly presented without clarifying some essential definitions that are important when in the context of the right to be forgotten and data protection in general.

The first essential term is "data subject", which

"…means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."[94]

The second term that is crucial here is "personal data", which "means any information relating to a data subject."[95]

There are also other important definitions like "processor" and "controller" but they are of less importance to this thesis.

The problem with these definitions, mainly "data subject" and "personal data" is that they are quite broad in their essence.[96] This lack of clarity decreases the level of certainty required to identify the data subject.

Having clarified these essential definitions, we move on to a discussion of the essence of the right to be forgotten.

---

[94] GDPR Proposal
[95] Ibid., at Art. 4
[96] M. Backes, P. Druschel, R. Tirtea, The Right to Be Forgotten—Between Expectations and Practice, European Union Agency for Network and Information Security (2012) http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/at_download/fullReport accessed 09.2014

The right to be forgotten is a right that, in today's European Union, is derived from the Data Protection Directive, wherein Article 12 states that every Member State shall guarantee every data subject the right to obtain from the controller:

"...as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data."[97]

This is therefore a right that gives individuals a means to have data located on the Internet deleted, so that it is no longer accessible. The data in mind may consist of photos, videos, articles, etc. that are about an individual.

One of the best-known theorists of the right to be forgotten is Koops[98], who claims that the right to be forgotten takes three forms[99]:

First is the right to have information deleted after a certain time, meaning that individuals should have the right to request that others, who are in possession of information about said individuals, delete it. This primarily concerns time, and argues that if an individual has uploaded information about themselves as a minor, for example, he now should have the possibility to have it erased.[100]

The second form of the right is the right to a "clean slate", and the third is the right to be connected only to present information.[101] In a way the three forms are actually quite similar to each other, all stating that individuals change over time and should thus be able to separate themselves from information that could be damaging to them. This, broadly, makes it possible for individuals to choose what information about them should be made available.

Although the right to be forgotten is presented as a new right in the forthcoming regulation, it is derived from other, previously existing notions of privacy.[102] It could be argued that the

[97] Directive 95/46/EC (Data Protection Directive), at Art. 12(b)
[98] Koops, at 233 (2011)
[99] Ibid.
[100] Ibid.
[101] Ibid.
[102] E. Shoor, *Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the*

European approach to privacy is derived from its history with totalitarian countries in which, as in Hitler's Germany for example, data was used to identify and locate certain groups of people.[103] This is given as an explanation for why Europe, in comparison with the United States, for example, has comparatively strict privacy rules.[104]

Shoor, responding to Fleischer[105], argues that the origin of the right to be forgotten derives from the French concept *le Doit a l'Oubli*, which translates to "the right to oblivion" that allows people to escape their pasts and control what is said about them.[106] This sentiment is echoed in Reding´s communication, although she does not refer to French law but to the previous data protection directive[107] and already existing laws.[108] Koops agrees in his article that:

Vivian Reding by using the formulation "strengthening", implies that the right to be forgotten already exists and is in need of reinforcement. With that Reding, implies that the right to be forgotten is nothing more than the current obligations in data-protection law to delete personal data when no longer relevant or inaccurate, or following a justified objection by the data subject.[109]

The European Commission's factsheet on the right to be forgotten is in accordance with the previous viewpoints, stating the right to be forgotten was already present in the 1995 Data Protection Directive which, in Article 12, states that a person can ask for personal data to be deleted once it is no longer necessary.[110] The right to be forgotten is thus an "adoption of historical protections in a modern context."[111]

Proposed Data Protection Regulation, 39, Brooklyn Journal of International Law, 1, at 491 (2014)
[103] Ibid.
[104] Ibid.
[105] P. Fleischer Peter, *Foggy Thinking about the Right to Oblivion,* PETER FLEISCHER: PRIVACY…? (2011) http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-tooblivion.html accessed 09.2014
[106] Shoor, at 491-493 (2014)
[107] Directive 95/46/EC (Data Protection Directive)
[108] V. Reding, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, Speech held at Digital Life Design conference (2012)
[109] Koops, at 232, (2011)
[110] European Commission Factsheet about data protection http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf , accessed 08.2014
[111] Shoor, at 494 (2014)

A clearer definition of the right to be forgotten has been given in the new regulation proposal.[112] The Article is called "Right to be forgotten and to erasure"[113].

The first part of the definition is derived from the first section of the Article, which provides individuals with the

"right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child."[114]

The second section puts certain obligations on the data controller. It obliges the data controller to:

"…take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorized a third party publication of personal data, the controller shall be considered responsible for that publication." [115]

Section three and four state that "the controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary"[116] and in certain cases "instead of erasure, the controller shall restrict processing of personal data..."[117]

Essentially, the right to be forgotten is an individual privacy right that gives individuals the right to erase certain personal data relating to them from the Internet. With that right an obligation is also placed on data controllers to take reasonable steps to inform other parties about the request for removal. Data controllers are also responsible for third party actors who have published this data through the first data controller. The erasure or retention of data should have no

[112] GDPR Proposal
[113] Ibid., at Art. 17
[114] Ibid.
[115] Ibid.
[116] Ibid.
[117] Ibid.

unreasonable delay and the only justification for failing to fulfill that right is explained in Article 17[118] as well.

The article sets out certain justified exceptions to the right to be forgotten, which were not clarified in the previous Data Protection Directive:

"for exercising the right of freedom of expression in accordance with Article 80;
for reasons of public interest in the area of public health in accordance with Article 81;
for historical, statistical and scientific research purposes in accordance with Article 83;
for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;"[119]

As we can see, those exceptions that are indicated concern other conflicting rights and even fundamental conflicting rights. The problem with this is that the regulation leaves the decision process up to the controllers, and if the controller fails to act correctly there are penalties for it. This has important implications for Internet freedom, and some of these conflicts are discussed below.

In conclusion, the right to be forgotten gives individuals greater control over their information on the Internet, giving them more power to shape their own identities, but this brings with it a host of issues concerning freedom of speech and expression.[120]

[118] Ibid.
[119] Ibid.
[120] Rosen (2012)

B. Case C-131/12

The European Court of Justice recently made a decision in case C-131/12[121] that forced Google to remove certain search results that related to the plaintiff in the case. This case is something of a landmark ruling on the right to be forgotten and its existence. "The ruling has very far reaching implications and has generated conflicting opinions among digital rights advocates. It introduces some very positive – and some quite dangerous developments."[122]

I. The Dispute and the Preliminary Ruling Request

The central issue in this case[123] concerned a Spanish man, Mario Costeja Gonzales, who had financial difficulties, mainly social security debts, in 1998 and whose real estate, for that reason, was put up for auction on several occasions. Spanish law required that a notice of the auction be published in a newspaper, and that newspaper's content was also available online. When an Internet user entered the plaintiff's name in a Google groups search engine, two pages of the aforementioned newspaper would appear. Those articles connected Mr Gonzalez to the act of the recovery of his social security debt.[124]

Mr. Gonzalez then made a complaint to the Spanish Data Protection Authority, alleging that the information should be removed from the newspaper's website and the Google groups search engine's results. The AEPD decided that the information was legally justified because the auction, at that point in time, needed as much attention as possible. The complaint against Google, on the other hand, was upheld, and the AEPD decided that search engines are subject to data protection legislation. Search engines carry out data processing and are considered intermediaries in information society.[125]

---

[121] Case C-131/12, *Google Spain and Google*
[122] Open Rights Group, https://www.openrightsgroup.org/blog/2014/landmark-ruling-by-european-court-on-google-and-the-right-to-be-forgotten, accessed 08.2014
[123] Case C-131/12, *Google Spain and Google*
[124] Ibid., at para. 14
[125] Ibid., at paras. 16-17

With that, the AEPD took the viewpoint that search engines are liable to prohibit access to certain data and even withdraw it. The justification behind this decision was that the locating and dissemination of data may compromise the fundamental right to data protection and the dignity of the person at hand. Thus the individual is justified to require their data be made invisible to third persons. The burden of removal of that information was put on the search engines and their operators – in this case, Google Inc. and Google Spain, who both brought legal actions to the National Court of Spain.[126]

The National Court of Spain, after submission of the appeal, submitted a preliminary referral to the CJEU about the interpretation of the Data Protection Directive.[127]

There were three central issues in the requested preliminary ruling that the CJEU was requested to conduct an analysis of:

1) If dealing with search engines, can they be referred to as data controllers?[128]

2) How is the application process of the Data Protection Directive applied when the company at hand is based outside the European Union?[129]

3) Do individuals have the right to be forgotten and do those rights have to be upheld by search engines? The National Court of Spain required clarification of the scope of the right.[130]

The CJEU's decision on these three issues is analyzed below.

[126] Ibid., at paras. 17-18
[127] Ibid., at para. 20
[128] Ibid.
[129] Ibid.
[130] Ibid.

II. The CJEU Decision

As established earlier in this analysis, three main issues arose in the process of the preliminary ruling request. This thesis will conduct a brief analysis of each issue in turn.

1) Search Engines' Status Under Directive 95/46

Before addressing the three issues highlighted above, the CJEU dealt with some preliminary questions. It then examined whether a search engine should be interpreted as a data controller and whether it really deals with processing personal data. The CJEU discussed whether Article 2(b) of the Data Protection Directive should be interpreted as meaning that a search engine, in all of its activities, processes personal data and whether information should be classified as personal data. After clarifying the first question, the court moved on to Article 2(d) of the Data Protection Directive to specify whether a search engine should be regarded as a data controller.[131]

The CJEU, while analyzing the first half of the previously mentioned issue, referred to existing case law from the Lindqvist case[132], in which had already been stated that the:

"...operation of loading personal data on an internet page must be considered to be such 'processing' within the meaning of Article 2(b) of Directive 95/46."[133]

After clarifying that, in the context of the Data Protection Directive, a search engine should be regarded as a data processor, the CJEU stated that, without contest, the data the search engine deals with is not personal data according to the meaning of Article 2(a) of the Data Protection Directive.[134] Further on, the CJEU elaborated that a search engine collects personal data by automatically exploring the Internet and systematically searching information that has been published. It then stores the data on its servers and makes it available, in the form of search

[131] Ibid., at paras. 21-41
[132] Judgment of 6 November 2003 in case C-101/01, Bodil Lindqvist v Åklagarkammaren i Jönköping, CJEU
[133] Case C-131/12, *Google Spain and Google*, at para. 26
[134] Ibid., at para. 27

results, and thus carries out the processing of personal data[135]. In paragraph 29 of the decision the CJEU specified that it is of no importance that "those data have already been published on the Internet and are not altered by the search engine."[136]

By interpreting a search engine as a data controller, it exempts for the protection that is offered under Directive 2000/31 that gives three liability exemptions: mere conduit; caching; and hosting.[137]

From here the CJEU moved on to analyze the next two issues.

2) Google Spain as an Establishment

The CJEU seeks to establish whether it is possible to apply national legislation with regards to the circumstances in the proceedings at hand[138]. More specifically, the CJEU clarified questions regarding whether the Data Protection Directive Article 4(1)(a) applies if data processing is carried out.

Article 4(1) states that national law will be applicable when:[139]

"The processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable."[140]

Google's search engine was an undertaking of Google Incorporated, a United States based enterprise, but in this case, Google maintained an office located in Spain – Google Spain SL –

[135] Ibid., at para. 28
[136] Ibid., at para. 29
[137] European Union, *Directive 2000/31 of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)*, Official Journal L 178, 17.07.2000, 1-16. (8 June 2000)
[138] Case C-131/12, *Google Spain and Google*, at para. 42
[139] Directive 95/46/EC (Data Protection Directive), at Art. 4(1)
[140] Ibid., at Art. 4(1)(a)

which promotes the sale of advertising space and has a separate legal personality[141]. Therefore the CJEU was asked if the data concerning the case at hand was in fact processed in the context of the activities of an establishment in a Member State.[142]

The reasoning behind the application of the Data Protection Directive to Google Incorporated was concluded in paragraph 56 of the case, where the CJEU stated that in such circumstances the activities of the operator of a search engine and its establishment, situated in a Member State, are inextricably linked because the activities related to the sale of advertising space make the search engine economically profitable and at the same time, this enables performance of the activities of the operator of the search engine[143]. The CJEU thus stated that the two establishments, Google Inc. and Google Spain SL, are interdependent.

The previous aspect of the CJEU's decision is of great importance because it implies that being economically profitable in the European Union, to the extent that it profits and funds the processing of personal data outside the EU territory, may be sufficient for the Data Protection Directive to apply to a non-European controller – thus the decision has bearing on any outside EU operator with sales offices in the European Union, although they may never actually interact with the data at hand[144]. This means that every company that has an office in the EU could be held liable for being economically profitable and for pursuing the same aim that is to make a profit.

Although the analysis in the C-131/12 case was in relation to advertising space and search engines, it could be that this is not a strict justification. In further practice the Data Protection Directive may be applicable in other cases as well. For example, to the memberships of certain sites that are subscriptions or donation seeking – where this is made possible by an establishment within the European Union. Of further note is that the economic link between such undertakings need not be very direct.[145] Undertakings that are connected to each-other through control can apply as well, so there is a broad link between being related. This, in the future, may bring with it legal difficulties for companies that act in the global sphere, and thus a lengthy and detailed discussion is needed in order to clarify the links.

---

[141] Case C-131/12, *Google Spain and Google*, at para. 43
[142] Ibid., at para. 45
[143] Ibid., at para. 56
[144] Crowther (2014)
[145] Ibid.

3) The Right to Be Forgotten in Relation to Search Engines

Finally, the CJEU analyzed whether the Right to be Forgotten should be interpreted in such a way that search engines are obliged to comply with it and remove from search results links that are: "...displayed following a search made on the basis of a person's name...."[146] An important aspect of this question is whether the information is:

"...published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful."[147]

In a more simplistic definition, the CJEU analyzed whether a person has the right to prevent search engines from indexing their personal data, even if that data is lawfully published on a third party's website. In this case, the person whose data is concerned had not approached the third party website to remove the data.[148]

In conclusion, after determining that the Data Protection Directive applied to Google Inc. via the established criteria, the CJEU turned to search engines' obligations with regards to Article 12(b) and 14(1)(a) of the Data protection Directive[149], and stated that there is a high level of protection for an individual's right to privacy stated in the Data Protection Directive, and that the processing of data by the data controller must be in pursuit of a legitimate aim and be obviously necessary.[150]

After conducting its analysis, the CJEU stated that:

"...it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list

[146] Case C-131/12, *Google Spain and Google*, at para. 62
[147] Ibid.
[148] Crowther, at 164-165 (2014)
[149] Directive 95/46/EC (Data Protection Directive), at Art. *7*
[150] Case C-131/12, *Google Spain and Google*, at para. 89

causes prejudice to the data subject."[151]

The CJEU then emphasized that a balancing of different rights and interests was needed in every case. Though an individual's right to private life and protection of personal data are guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights[152], and those rights in general override the economic interests of search engines and the interest of the general public to have access to information, there are different exceptions – the role played by a subject in public life may be a reason to interfere with that person's fundamental rights, and the interest of the general public in having access to certain information could thus override the rights to privacy and data protection.[153]

III. The Advocate General's Opinion

The Advocate General, in his opinion, underscored a number of significant aspects of this case. First of all the AG emphasized that during the adoption of the Data Protection Directive, the Internet, as it is known today, had barely emerged and with it, search engines were at their earliest state of development. The AG then stated that the Data Protection Directive did not take into account the enormous amount of decentralized, hosted data that is now accessible from all over the world. The Data Protection Directive also did not account for the fact that data can so easily be copied and used by parties that have no connection to the whomever uploaded that data in the first place.[154] In this regard the AG referred to the fact that the Data Protection Directive was so old that it was simply not applicable to the state of the Internet today. He also noted that that the principle of proportionality should be taken into account in order to achieve a balanced and reasonable outcome.[155]

Further on in his analysis the AG found that search engines are not controllers in the sense of the Data Protection Directive because the data that they process is hosted on third party servers. The

[151] Ibid., at para. 99
[152] CFREU., at Art. 7-8
[153] Case C-131/12, *Google Spain and Google*, at para. 99
[154] Advocate General Jääskinen in Case C-131/12, *Google Spain and Google*, at para. 78
[155] Ibid., at para. 79

search engine is merely a passive site that has no control over the original data.[156] In fact, he stated that the opposite opinion would entail that search engines are incompatible with EU law, pointing out the absurdity of that situation. As an example, the AG described a situation in which an Internet search engine, if considered a controller in relation to a third-party website that hosts personal data (in the sense of Article 8[157] of the Data Protection Directive), would automatically become illegal if certain stringent conditions of processing were not met.[158]

However, the situation with the indexing process of search engines is different.

"Internet search engine service provider clearly controls the index of the search engine which links key words to the relevant URL addresses. The service provider determines how the index is structured, and it may technically block certain search results, for example by not displaying URL addresses from certain countries or domains within the search results."[159]

In AG Jääskinen's approach, a search engine is not considered a controller in the sense of controlling and collecting data, but they are considered controllers in their indexing of search results.

The AG then moved on to consideration of the right to be forgotten. He noted that the Data Protection Directive does not provide a general and an absolute right to be forgotten. More precisely, he pointed out that the restriction or removal of personal data cannot be left up to the data subject's subjective preferences. The purpose and the interests of processing should be compared to those of the data subject and a decision should be made under those criteria. He further emphasized that subjective preference alone does not amount to compelling and legitimate ground for erasure and removal.[160] With this he repeated that there is a balancing test needed in order to decide whether the application of the right to be forgotten is justified.

The Advocate General even stepped in for the protection of search engines and the right to access information. He stated that in an information society the right to search published information on the Internet via search engines is one of the most important ways to access

[156] Ibid., at paras. 84-89
[157] Directive 95/46/EC (Data Protection Directive), at Art. 8
[158] Advocate General Jääskinen in Case C-131/12, *Google Spain and Google*, at para. 90
[159] Ibid., at para. 91
[160] Ibid., at para. 108

information.[161]

"An internet user's right to information would be compromised if his search for information concerning an individual did not generate search results providing a truthful reflection of the relevant web…".[162]

With that AG Jääskinen referred to the alteration of the amount of information that could be found and point out that this would not present a truthful result. Thus the right to be forgotten would be in conflict with the right to access information.

A complex fundamental rights system with the addition of the right to be forgotten would entail sacrificing other rights like freedom of expression and information. The AG thus discouraged the CJEU from allowing these conflicting rights to be balanced on a case-by-case basis, with judgment ultimately left to the search engine service provider. Those procedures are likely to lead to automatic withdrawal of links to any content that is objected to. Another consideration is that an unmanageable number of requests would need to be processed by service providers. AG Jääskinen noted that there is a difference between unlawful content and a request for suppression of legitimate content[163]. He stressed that search engine providers should not be given this obligation because it would entail serious interference with the webpage publisher's freedom of expression and amount to the censoring of its legitimate content.[164]

In conclusion, the Advocate General answered that a subjective preference that one's information be removed does not amount to a compelling and legitimate ground, and with the proposed right to be forgotten the rights of Internet users to access information are compromised because they would not receive truthful results.[165]

[161] Ibid., at para. 131
[162] Ibid.
[163] Ibid.
[164] Ibid., at para. 134
[165] Crowther, at 165 (2014)

IV. Case C-131/12 Summary

Case C-131/12 is a landmark ruling by the CJEU with regards to the right to be forgotten and it has many significant implications. The ruling also clears up a many issues related to data protection and Internet search engines. The CJEU supported the right to be forgotten and proved that in their view it existed in the applicable European privacy law. The same argument is supported by other authors, for example, Andra Giurgiu, who states the following: "it is a mere re-branding of long standing data protection rules".[166] Yet again there is a fine balance needed between the right to be forgotten and other fundamental rights like freedom of expression and the freedom to access information, and this demands further clarification as there exists the potential for unnecessary censorship of the Internet.[167]
Several important questions were answered within the analysis of case C-131/12, and all of them have important implications for privacy law in Europe.

1) Search engines are to be considered as data controllers:

Before case C-131/12, search engines were not considered as data controllers because they did not have direct control over the data they were reproducing, but this case redefines the activities of search engines. It provides that the indexing, storing and making available of information is considered processing with regards to the Data Protection Directive and a search engine is a controller in the sense that it defines the purpose of the processing at hand.[168]

2) Territorial scope and the establishment:

Before this case, companies which were situated outside the EU and had subsidiaries within its area did not have data protection obligations in the European Union. Now it these obligations apply so long as a company has a branch or a subsidiary within a Member State that promotes the sale of advertising space, for example[169]. That is, if an establishment is inextricably and

[166] Giurgiu, at 366 (2013)
[167] Open Rights Group https://www.openrightsgroup.org/blog/2014/landmark-ruling-by-european-court-on-google-and-the-right-to-be-forgotten accessed 12.2014
[168] Case C-131/12, *Google Spain and Google*, at para. 41
[169] Ibid., at para. 60

economically linked to the company, it is enough to make the company responsible under EU data protection law.[170]

3) A search engine's responsibility:

A search engine operator is obliged to remove from the list of search results that are displayed following a search made on the basis of a person's name links to webpages, even if they are originally published by third parties and the publication on third party websites is in itself lawful[171]. With this, the CJEU differentiates between search engines and publishers. The Court says that they have different responsibilities and thus are both responsible under the Data Protection Directive. Data that is indexed and found with the help of a search engine helps to project an image of an individual, and this would otherwise be difficult to do and thus plays an important role with regards to a person's right to privacy.[172] Making search engines data controllers has broad implications, and the most notable of these is that a search engine operator is now subject to different obligations that arise from EU data protection legislation.

4) The right to data protection overrides the economic interests of a search engine and the right to access information:

The CJEU states that it is clear that the economic interest of a search engine operator does not justify their interference with an individual's privacy. There is also a fine balance to be struck between an individual's right to privacy and an Internet user's right to access information. In most cases, however, the right to privacy overrides other fundamental rights. The court also distinguishes between regular individuals and those that play a public role. It is stated that in relation to the role played by the data subject in public life, one can expect less protection of privacy.[173]

5) The right to be forgotten already exists in the Data Protection Directive:

[170] Ibid., at para. 56
[171] Ibid., at para. 88
[172] Ibid., at paras. 80; 87
[173] Ibid., at para. 81

With regard to the whole case under consideration, the CJEU supports the existence of the right to be forgotten. The court states that according to the Data Protection Directive, individuals have the right to ask for the removal of excessive, irrelevant, inaccurate and inadequate information about themselves.[174] Although the court did not clarify the situation with regard to the original publishers of the information, but only dealt with the search results provided by search engines, this right may have very far-reaching implications. Further clarification and court practice is certainly needed in order to make the criteria for removal more transparent.

This concludes our analysis of case C-131/12 and outlines its central and most important aspects. Further clarification is needed for the essential aspects of the right to be forgotten. Namely, the terms 'inaccurate', 'inadequate', 'irrelevant' and 'excessive', and have not actually been equipped with concrete guidelines and explanations.

V. Inaccurate, Inadequate, Irrelevant and Excessive Information

The first condition set out in Data Protection Directive Article 12(b)[175] concerns inaccurate information. The Article provides that Member States have the obligation to guarantee every data subject the right to obtain from the controller:

"as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data."[176]

The same is mentioned in case C-131/12, as it states the following in paragraph 70:

"Article 12(b) of Directive 95/46 provides that Member States are to guarantee every data subject the right to obtain from the controller, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of Directive 95/46, in particular because of the incomplete or inaccurate nature of the data. As this final point

[174] Ibid., at para. 99
[175] Directive 95/46/EC (Data Protection Directive), at Art. 12(b)
[176] Ibid.

relating to the case where certain requirements referred to in Article 6(1)(d) of Directive 95/46 are not observed is stated by way of example and is not exhaustive, it follows that non-compliant nature of the processing, which is capable of conferring upon the data subject the right guaranteed in Article 12(b) of the directive, may also arise from non-observance of the other conditions of lawfulness that are imposed by the directive upon the processing of personal data."[177]

It is clear that Article 12 gives every data subject the right for rectification, erasure or blocking of inaccurate data, but how do we define 'inaccurate'? This is a very subjective term in itself. The strict dictionary definition is as follows: "Not correct or exact: having a mistake or error: not accurate."[178] This definition is clearly not sufficient basis for a concrete argument, and must be clarified. Some help can be found in the Data Protection Directive[179] once again.

Article 6(d) states that all information, collected and processed, must be accurate, and where necessary kept up to date. The processor must ensure that data which is inaccurate or incomplete, with regard to the purposes for which it was collected or further processed, is erased or rectified.[180]

The same question also arises with other terms. The word 'inadequate', can be found defined as follows: "not enough or not good enough".[181] Such a definition is as subjective as the previous 'inaccurate'.

The situation is the same with other two terms 'irrelevant' and 'excessive'[182]. With these, the key issue is once again that their definitions are highly subjective terms that demand case-by-case analysis. But which actor ought to be tasked with identifying the irrelevant and excessive? Being so open-ended, these terms could lead to online censorship and violations of freedom of expression.[183]

---

[177] Case C-131/12, *Google Spain and Google*, at para. 70
[178] "inaccurate", Merriam-Webster (2014) http://Merriam-Webster.com accessed 09.2014
[179] Directive 95/46/EC (Data Protection Directive)
[180] Ibid.
[181] "inadequate", Merriam-Webster (2014) http://Merriam-Webster.com accessed 09.2014
[182] Case C-131/12, *Google Spain and Google*, at paras. 70-72
[183] O. Fisher, *Google Right to be Forgotten … but what about business data?,* Magnifica (2014) http://www.magnifica.co.uk/blog/google-right-to-be-forgotten-what-about-business-data accessed 12.2014

At this point in time, there are guidelines for how to assess whether something is inaccurate, inadequate, excessive or irrelevant and the obligation to assess this is placed upon search engines. These actors are neither objective nor impartial, and for that matter and it is not possible to ensure that a court will reach the same conclusion, should the argument reach that point. It needs to be stressed that although there are guidelines, they are not legally binding.

VI. Impact on Search Engines

As the ruling in case C-131/12 is based on the actions of search engines and search engine operators, a great deal of feedback has been generated in response to it and Google even met with EU officials to discuss the impact of the right to be forgotten and obtain further guidelines.[184]

Although the ruling brings with it a many positive outcomes for the protection of individual privacy, it has also aroused much criticism. Some search engines have responded negatively to the decision, for example, and the United Kingdom's House of Lords were also severely critical of the decision.[185]

In their analysis, the House of Lords considered to what extent is it practical for search engines to comply with the judgment: compliance here indicating the proportionate expenses required of search engine operators in light of the judgment.[186]

There are in fact numerous practical and economic reasons that make the new right to be forgotten burdensome to search engines like Google.[187]

---

[184] Q. Plummet, *Google, Microsoft, Yahoo meet EU data regulators to discuss 'right to be forgotten' ruling*, Tech Times (2014) http://www.techtimes.com/articles/11366/20140728/google-microsoft-yahoo-meet-eu-data-regulators-to-discuss-right-to-be-forgotten-ruling.htm accessed 12.2014

[185] House of Lords, European Union Committee, EU Data Protection law: a 'right to be forgotten'?, 2nd Report of Session 2014–15, London, 2014

[186] Ibid., at para. 24

[187] J. Lowe, *What's wrong with the "right to be forgotten"?,* Prospect Magazine (2014) http://www.prospectmagazine.co.uk/blogs/prospector-blog/whats-wrong-with-the-right-to-be-forgotten accessed 12.2014

In response, Google's "Search removal request under data protection law in Europe"[188] web form was made available on 30 May 2014. In the first 24 hours, Google received 12,000 requests; after four days, the number of requests totaled approximately 40,000[189]. By June 30, 2014 Google had received more than 70,000 requests for removal, each with an average of 3.8 URLs per request – that is, over a quarter of a million specific removal requests.[190] Clearly, these numbers indicate a tremendous burden for the search engine operators.

The specifics of these economic and practical burdens can be broken down into three categories:

Dedicated personnel:

Analyzing removal requests requires dedicated personnel. These personnel must have the capability to receive requests and respond to them. Had concrete terms of information removal been established, this could have been automatized to some degree; but given the fact that the removal process is subjective in its essence, the search engines and their employees must act as arbiters and make subjective decisions.[191] In light of the number of requests submitted in the first days of the right's implementation, there is clearly need for a remarkable amount of personnel in order to comply with the obligation.

Costs:

The number of dedicated personnel needed to maintain the tools that track and remove information has an economic impact. Search engines themselves have to bear the cost of those aspects of the obligation.[192]

Big Data[193]:

---

[188] Google Support page about search removal request (2014) http://www.prospectmagazine.co.uk/blogs/prospector-blog/whats-wrong-with-the-right-to-be-forgotten accessed 09.2014

[189] House of Lords, European Union Committee, EU Data Protection law: a 'right to be forgotten'? 2nd Report of Session 2014–15, London, 2014, at para. 32

[190] Ibid.

[191] Lowe (2014)

[192] Ibid.

[193] Big Data is a loosely defined term used to describe data sets so large and complex that they become awkward to work with using standard statistical software.

In a technological society, there are "data sets so large and complex that they become awkward to work with using standard statistical software".[194] Within this complex network of Big Data, even if the information that has been requested is removed, it may still be active through Big Data.[195] It is clearly too burdensome to reverse-engineer all such information in order to remove data.

The biggest initial burden handed to search engine operators was the subjective reasoning behind what is to be considered 'excessive', 'irrelevant', 'inadequate' or 'inaccurate'. It is impossible for a private actor to decide in every case what qualifies for erasure under these terms. Furthermore, it is difficult for a search engine to decide what is of public interest and what is not. The task of balancing different rights was given to private actors who themselves are made responsible under data protection legislation. This point has been reiterated the ICRI research group:

"Private companies might not have enough legal knowledge to make the necessary balancing of the rights in question. This is particularly the case in situations where content is not *manifestly* illegal. This might be the case, for example, when the subjective rights of individuals are at stake (e.g. in case of privacy infringements)."[196]

The balancing is even more difficult because private actors have to assess the proportionality test that is enforced under Article 10 of the ECHR that states that any restriction to freedom of expression has to be prescribed by law; necessary in a democratic society; and have a legitimate aim.[197]

It is practically impossible to legally balance these rights without guidelines, when there is need for a case-by-case analysis.

---

[194] C. Snijders, U. Matzat, U.-D. Reips, '*Big Data': Big gaps of knowledge in the field of Internet*, 7, International Journal of Internet Science, at 1, (2012)
[195] Lowe (2014)
[196] B. Van Alsenoy, A. Kuczerawy, J. Ausloos, *Search engines after Google Spain: internet@liberty or privacy@peril?*, ICRI working paper, at 65 (2013)
[197] ECHR, at Art.10

C. Freedom of Expression and the Right to Be Forgotten

In order to harmonize and bring into accordance the right to be forgotten and the right to freedom of expression, this thesis will make a number of suggestions. Proper codes of conduct and self-regulatory methods could give a positive boost to the right to be forgotten. This has also been proposed by Reding, who suggested that industry self-regulation is a good option in the area of data protection and privacy.[198] There can be no universal mechanism to fit every possible right to be forgotten case, but there has to be an analysis for everything.

There is no need to enumerate all the merits of media self-regulation here, but the following may be taken as a broad outline stated by the OSCE:

The OSCE explains that media self-regulation is a joint endeavor by media professionals. It works by setting up voluntary editorial guidelines and abiding by them in a learning process open to the public. By doing so, the independent media, that is concerned, accepts that they have a responsibility for the quality of public discourse in the nation, doing that they also fully preserve their editorial autonomy in shaping it.[199]

For media websites and organizations, the implementation of a self-regulatory mechanism is somewhat easier when compared to other actors like social media, but there are still a number of challenges. If the process of self-regulation could also be taken over by search engine operators and social media websites, to at least some extent, it would simplify the process concerning the right to be forgotten. Much depends on the rules that are implied for self-regulation and the mechanisms that assure they are followed. If it is possible to impose such self-regulatory bodies – which are actually effective – this would make a tremendous impact on the problem of data protection, because there would be less negative content to worry about in the first place.

It is not possible to ensure that self-regulatory mechanisms would be a reasonable alternative for the strict application of the right to be forgotten, and they should not be intended as such.

---

[198] V. Reding, *The Upcoming Data Protection Reform for the European Union*, 1, International Data Privacy Law, at 3 (2011)
[199] M. Haraszti *et al*, The Media Self-Regulation Guidebook, Organization for Security and Co-operation in Europe, at 9 (2008)

Multiple different mechanisms provide the best possible solution to the implementation of the right to be forgotten.

I. Freedom of Expression

Freedom of Expression is a fundamental basis for democracy and its attendant rights and freedoms, and it has roots reaching back to antiquity.[200] The right is essential for democracy to function and promote public participation in the decision-making process. It is not possible to take part in the process if one does not have access to information and ideas or is unable to express viewpoints. Thus the right is important for an individual's dignity, the participation process, accountability and democracy.[201] Given the essential importance of the right to freedom of expression, there exist concrete means to ensure that it is respected: specially constructed mechanisms, worldwide and regional, that protect freedom of expression.[202] There is no difference made between the medium used to fulfill that right, whether written or oral, including art and Internet, etc.[203]

Freedom of expression is recognized in Article 19 of the UDHR, where it is stated that:

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[204]

This is also accepted as international law by the International Covenant on Civil and Political Rights, where Article 19 states that freedom of expression is a universal right, which is nonetheless subject to some restrictions.[205]

---

[200] ECtHR, *Handyside v. the United Kingdom*, judgment of 7 December 1976, series A, No. 24.
[201] *Freedom of Expression*, Human Rights Education Associates http://www.hrea.org/index.php?base_id=147 accessed 09.2014
[202] Ibid.
[203] A. Puddephatt, *Freedom of Expression, The essentials of Human Rights*, Ed. Hodder Arnold, at 128 (2005)
[204] UDHR., at Art 19
[205] UN General Assembly, *International Covenant on Civil and Political Rights*, United Nations, Treaty Series, vol. 999, p. 171, (16 December 1966), at Art. 19

Concerning regional instruments, two basic documents apply within Europe. First there is the ECHR that covers freedom of expression under Article 10:

"Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."[206]

The most modern of these is the Charter of Fundamental Rights of the European Union which came into force in 2012.[207] The CFREU is strict about freedom of expression and information and states, in Article 11:

"Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. The freedom and pluralism of the media shall be respected."[208]

The legislation in place demonstrates that the right to freedom of expression is highly valued, but almost all of them specify some restrictions or exemptions. A broad overview of justified restrictions is analyzed in the Guidelines by the Council of the European Union.[209] This document states that any restriction that threatens freedom of expression must be legitimate, thus provided by law, and imposed on the grounds set in international law. It must be proportionate

[206] ECHR, at Art. 10
[207] CFREU
[208] Ibid., at Art. 11
[209] Council of the European Union, EU Human Rights Guidelines on Freedom of Expression Online and Offline, FOREIGN AFFAIRS Council meeting, Brussels, (12 May 2014)

and necessary to its aim – in order to assess proportionality, certain tests must be passed.[210] Restrictions of fundamental and human rights are not of small concern in international law and require concrete grounds in order to be justified. Two examples given in the Guidelines demonstrate those types of restrictions that violate the right to freedom of opinion and expression, and the second relates explicitly to the Internet.[211]

Censorship on the Internet usually is in the form of laws and regulations allowing for the total or partial banning of certain webpages. There are even circumstances in which, countries resort to the complete disconnection from the Internet. Actions like these isolate a whole country or region from the rest of the world.[212] "It is important to guarantee that the access to and free flow of information will not be subject to unjustified restrictions regardless of the medium."[213]

The right to freedom of expression applies not only to expressing oneself, but is relevant to the accessing of information. As the Universal Declaration of Human Rights[214] stipulates, freedom of expression is also about seeking, receiving and imparting information and ideas, through any media and regardless of frontiers. With that, it can be concluded that an individual has the right to access information. That right is thus in conflict with the right to be forgotten, and some might say that the right to privacy ought to prevail over the right to freedom of expression.[215]

II. Freedom of Expression and Case C-131/12

Moving on to the connection between freedom of expression and Case C-131/12, there are several opposing opinions on its effect. As Steven James says, there has been a dramatic impact of this decision on the right to access information. Until recently Internet users have believed the Internet to be something of a repository for all kinds of information – be it good or bad. Case C-

[210] Ibid., at Annex 1
[211] Ibid.
[212] Ibid.
[213] Ibid.
[214] UDHR
[215] S. James, *The right to privacy catches up with search engines: the unforgettable decision in Google Spain v AEPD*, 20 (5), Computer and Telecommunications Law Review, at 130-133 (2014)

131/12 is thus something that attacks its freedom to be that storage for information.[216] When the right to be forgotten, or erasure, as it is called in the new GDPR Proposal, allows individuals to remove certain information linked to their subjective understanding of what ought to be allowed and what not, it makes censorship of information possible or even more likely. This in turn makes the Internet a much less reliable and neutral medium.

Search engines, for that matter interact with the right to be forgotten in multiple different ways. Acting as mediators, search engines facilitate the possibility to receive information and by doing that they enhance and enable an individual's right to access and receive information. It could even be said that search engines are the primary tools used to find relevant content on the Internet. Interference with a search engine's activity in providing for that right thus poses a serious threat to these rights and needs a proportionate justification.[217]

Another potentially negative impact of Case C-131/12 on freedom of expression is that, forced to be so subjective in responding to erasure requests, search engines are likely to indiscriminately satisfy them. This is because search engines do not want to be found liable for breach of privacy, and compared to the administrative costs of analyzing each request, it is cheaper to simply remove the link in question automatically. Although there still exists the possibility that the information subject to the removal request could not be justified, or that there might be sufficient public interest to maintain it, this deliberation is too burdensome to be realistically expected of the search engine. This is based not on mere assumption but is evident in real trends in the present response to removal requests[218]. Once again it is clear that the freedom to access information and freedom of expression could suffer a serious setback from the implementation of this right. Removing content without sufficient analysis is not the correct means to protect individuals' rights, but it is the easiest and most likely option in this case.

The CJEU, in decision C-131/12, headed in another direction.[219] Paragraph 99 of the decision stated that it should be examined whether a data subject has such a right that the information at hand not be linked to his name.[220] On the contrary, the CJEU and the EU Commission, in its

[216] Ibid.
[217] Alsenoy, Kuczerawy, Ausloos (2013)
[218] James, at 130-133 (2014)
[219] European Commission Factsheet about data protection http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf accessed 09.2014
[220] Case C-131/12, *Google Spain and Google*, at para. 99

factsheet[221], claim that the right to be forgotten is not a right that trumps other fundamental rights like freedom of expression. The CJEU came to the conclusion that the right to be forgotten exists but it is not an absolute right, and it has limits that must be assessed on a case-by-case basis.[222]

The CJEU explained that the right to be forgotten only applies where the data at hand is no longer necessary or is irrelevant to the purposes for which the data was first collected. According to their view, removing irrelevant and outdated links to webpages is not the same as deleting any content.[223]

It was further established that neither the right to the protection of personal data nor the right to freedom of expression are absolute rights.[224] There is always a fine balance that should be struck between the legitimate interests of Internet users and an individual's fundamental rights to privacy.[225]

The European Commission also explained that:

"Freedom of expression carries with it responsibilities and has limits both in the online and offline world. This balance may depend on the nature of the information in question, its sensitivity for the person's private life and on the public interest in having that information. It may also depend on the personality in question: the right to be forgotten is certainly not about making prominent people less prominent or making criminals less criminal."[226]

The balancing test is clearly shown in Case C-131/12 where the CJEU ordered the search engine operator to remove search results but did not oblige the original publisher to remove the article in place[227]. With that the CJEU proved that there is a difference between a search engine's actions and its impact on the person concerned with the original existence of the information published. Case C-131/12 explained that search results have a significant impact on a person's privacy

[221] European Commission Factsheet about data protection European Commission Factsheet about data protection http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, accessed 09.2014
[222] Ibid.
[223] Case C-131/12, *Google Spain and Google*, at para. 86
[224] European Commission Factsheet about data protection http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf accessed 09.2014
[225] Ibid.
[226] Ibid.
[227] Case C-131/12, *Google Spain and Google*, at para. 88

because they help to compose a profile of an individual. Although the information will still be available to the public, it is enough to remove search results to protect individual privacy.

The strictest criteria for the balancing between privacy and freedom of expression were mentioned in paragraph 93 of Case C-131/12 where the CJEU stated that:

"…even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed."[228]

These criteria are essentially derived from Article 6 of the Data Protection Directive where it is stated that information should be collected for specified, explicit and legitimate purposes and only processed for said purposes alone. Processing for historical, statistical or scientific purposes is also compatible with the Data Protection Directive but there must be appropriate safeguards.[229]

The Article also confirms that the information must be accurate, kept up to date, relevant, adequate and not excessive in relation to its original purpose. In order to meet these criteria, all reasonable steps must be taken to remove or rectify inaccurate or incomplete data. Once again the article reiterates that appropriate safeguards should be implemented for historical and scientific collection and processing.[230]

Finally the Data Protection Directive leaves the implementation and assessment of the previously mentioned aspects to the controllers.[231]

The most problematic aspect thus remains giving an explicit meaning to the above criteria. If the controller and the assessor are the same agent, there is no oversight to ensure that assessments are conducted properly and that their results are in accord with those that might be reached by an impartial court. Imposing oversight on the assessment process could encourage controllers to

[228] Ibid., at para. 93
[229] Directive 95/46/EC (Data Protection Directive), at Art. 6
[230] Ibid.
[231] Ibid.

remove every result, and even if that is not the inclination of specific controllers, smaller organizations might not have access to adequate and professional personnel to carry out the assessment process.

Although it has been said that time is of great importance in these matters, Data Protection Directive and Case C-131/12 does not specify how to assess that importance. It is the vagueness of the right to be forgotten that is a problematic aspect.[232] Vagueness with regard to privacy in most cases trumps freedom of expression, and constitutes the biggest threat to that freedom.[233] Only with correct and concrete guidelines can data controllers act according to EU law, for without it they are likely to conduct only subjective analyses and to move towards a situation in which freedom of expression and access to information are negatively and indiscriminately affected.

If the GDPR is not approved, the Data Protection Directive still gives Member States different ways to regulate the right to be forgotten. This creates a far too burdensome and difficult situation for controllers, who are required to assess requests in accordance with every single legislative act that has been implemented with regard to the Data Protection Directive.

Case C-131/12 is important in the context of freedom of speech due to its classification of data controllers.[234] At first glance, there may not seem to be a significant connection to freedom of speech, but such a connection does exist and it is significant. With this judgment, search engine providers are held liable in to the provisions of the Data Protection Directive, meaning that they are required to ensure that the data they processed is adequate and relevant. There is no reasonable way for a search engine to assess data according to these criteria because they have no real connection to the data subject or to the original publishing of the data and the factual situation[235]. This makes these requirements overly burdensome for search engines, which, rather than undertaking to assess the adequacy and relevancy of the data in question, will be more willing to simply remove the result on request without any analysis.

---

[232] B. Thompson, A. Kates, *The Debate*, 9, Engineering & Technology, 8, at 26 (2014)
[233] P. Neroth, *Challenge of balancing privacy with censorship ends up in Google's lap*, 9, Engineering & Technology, 7, at 16 (2014)
[234] Case C-131/12, *Google Spain and Google*, at para. 33
[235] A. Proops, *Privacy but at what price?*, 4, Lawyer (Online Edition), Academic Search Complete, EBSCOhost, accessed 09. 2014.

It is significant that Case C-131/12 does not treat the balancing of different fundamental rights, especially freedom of expression and the right to privacy. Both of those rights are fundamental and thus of equal and fundamental importance. As discussed above, freedom of expression also entails the right to receive information. This is the right that individuals exercise when they search for information on the Internet.[236] The judgment in this case, however, somehow grants the right to privacy a dominant position with regard to freedom of expression and other rights.[237]

"Only if there is a 'preponderant interest of the general public'[238] in facilitating access to the information can the relevant web-pages continue to be subject to indexation. The effect of the judgment is therefore that individuals are now afforded a significant power to rewrite their e-history to suit their own interests."[239]

Once again there are no guidelines on how to objectively assess the existence of this 'preponderant interest of the general public'. This could in the worst case lead to automatic removal upon request, which as we have seen has a decidedly negative effect on freedom of expression.

It should be mentioned that some authors have argued that Case C-131/12 is not a freedom of speech issue, and that attempts to frame it as one are inaccurate if not mischievous. Furthermore, they claim that the right to speak, to publish and to be published is unaffected by this case.[240] As we have shown at the beginning of this thesis, this has proven to be an inaccurate conclusion. The indexing and appearance of information in search results helps to give an individual a detailed profile, and thus search engines' activities are an issue related to freedom of expression, as proven by the CJEU.[241]

---

[236] Ibid.
[237] Case C-131/12, *Google Spain and Google*, at para. 81
[238] Ibid., at para. 97
[239] A.Proops, *Privacy but at what price?*, 4, Lawyer (Online Edition), Academic Search Complete, EBSCOhost, accessed 09. 2014.
[240] F. Crehan, *Google Spain, What It Means and What It Doesn't,* Fergal Crehan BL (14 May 2014) http://fergalcrehan.com/2014/05/14/google-spain-what-it-means-and-what-it-doesnt accessed 09.2014
[241] Case C-131/12, *Google Spain and Google*, at para. 37

The new General Data Protection Regulation proposal includes a clause that obliges Member States to pass national legislation that reconcile data protection with freedom of expression and media.[242] Article 80 of the new GDPR states the following:

"Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organizations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression."[243]

Although the European Commission in its factsheet suggests that the new GDPR proposal empowers individuals to

"manage their personal data while explicitly protecting the freedom of expression and the freedom of media",[244]

serious critiques have arisen on this point. These have mostly to do with the inadequacy of the GDPR Proposal, which is said to be inadequate in the sense of protecting freedom of expression and freedom of the media and, without amendments, to give the right to be forgotten a superior status. This status, which supersedes other fundamental rights, will give the right to be forgotten the potential to shape history by deleting information from historical archives. This then affects news organizations and any other proponents of unfettered publication of information about matters of public concern.[245]There is certain to be a great deal of future debate on these issues, but at the moment it is the vagueness and subjectivity of the whole concept which comprises its most problematic aspects.

---

[242] Z. Akhtar, *Malicious communications, media platforms and legal sanctions*, Computer and Telecommunications Law Review, Sweet & Maxwell and its Contributors, at 184 (2014)
[243] GDPR Proposal, at Art. 80
[244] European Commission Factsheet about data protection http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf accessed 09.2014
[245] K. Larsen, *Europe's "Right to Be Forgotten" Regulation May Restrict Free Speech*, 17, First Amendment & Media Litigation, 1 (2012)

III. Historic Truth and the Alternation of Content

History can broadly be defined as the knowledge acquired by investigation of the past.[246] It tries to analyze objectively, based on patterns and other phenomena, the cause and effect of things that have happened.[247] In order to give an objective reflection of past events, one needs access to all the information available from the point in time under consideration. It is impossible to provide clear historic data if certain kinds of information are removed or repressed.

As established earlier in the thesis, freedom to access information is a part of freedom of expression, and the same is true of history – it is a category under freedom of expression. History, thus being a part of freedom of expression, cannot happen without the help of the Internet. With regard to freedom of expression and access to information, one cannot overlook the importance of the Internet and search engines[248], the Internet consists of billions of web pages that are spread across thousands of servers everywhere.[249]

With such a great amount of information available, a user must choose between two basic means accessing it. The first option is to know the exact address of the page and navigate directly to it, and the second is to use a search engine to locate pages relevant to a search query. In reality, users would have limited access to information without the use of search engines. The reason behind that is the relative impossibility of locating and accessing specific information, given the huge number of possible locations.[250]

One cannot assume that freedom of expression and access to information is really provided without a way to locate information. This is the where search engines become irreplaceable. The *raison d'être* of search engines is to locate and access Internet content. In performing this task, search engines have also become targets of censorship. Censorship or restriction of access is a

---

[246] B. Joseph (Ed.), R. Janda (Ed.), *The Handbook Of Historical Linguistics*. Blackwell Publishing, at 163 (2008)
[247] A. Munslow, *What Is History?*, History In Focus, *2*, University Of London (2001)
[248] S.A. Haynes, *Google Search Results: Buried If Not Forgotten*, 15, North Carolina Journal Of Law & Technology, 3, at 470 (2014)
[249] B. Faye, *Liability Of Internet Search Engines*, Hibernian Law Journal, at 181 (2006)
[250] Ibid., at 181

threat to freedom of expression and does not project a correct historical account.[251] Such censorship is made more likely due to the legal liability that has been placed upon search engines by recent court cases. As established earlier, in Case C-131/12, search engines are to be considered as controllers and are thus liable before EU law. This sets a challenge before freedom of expression because the amount of information available to search engines makes it impossible to analyze all – or even any – of it in depth. It is thus likely that a search engine operator will act by removing or withdrawing any possibly infringing information.[252] From a historical perspective, it would lead censorship of the past and the projection of a non-objective picture of it. The same is feared by AG Jääskinen in his opinion.[253]

Censorship is totally inconsistent with freedom of expression, and although people have a tendency to approve of it when it is used to censor certain things that they do not like, this is often dependent on political and legal trends and is thus easily changeable.[254] Trends in this case can change with certain guidelines and case-law, which can modify the right to be forgotten. Without legally binding concrete rules, it is unclear under which conditions the case can be invoked and against whom.[255] This uncertainty is yet another aspect that may drive search engine operators to be overly enthusiastic about removing and retaining information. While it is initially intended that the digital age should allow for some degree of forgiveness[256], this should not be allowed to conflict with the right to freedom of expression.

If a person is given the chance to abuse the right to be forgotten, or even to use it as intended, they have the possibility to erase certain aspects of history that would otherwise be made available to others. The information that is concerned, although not strictly of a specific concrete nature, can be anything that a person thinks is irrelevant or embarrassing.[257]

It must be clarified that:

---

[251] Ibid., at 182
[252] Y.F. Lim, Cyberspace Law: Commentaries And Materials, Oxford University Press (2nd Ed), at 335 (2007)
[253] Advocate General Jääskinen in Case C-131/12, *Google Spain and Google*, at para. 129
[254] L. Siegel, *Should The Internet Be Censored? No! No! No! No!*, 22, Update On Law-Related Education, 2, American Bar Association, at 12 (1998)
[255] Giurgiu, at 367 (2013)
[256] M.L. Ambrose, N. Friess, V.M. Jill, *Seeking Digital Redemption: The Future Of Forgiveness In The Internet Age*, 29, Santa Clara Computer & High Technology Law Journal (2012)
[257] J. Rosen, *The Deciders: The Future Of Privacy And Free Speech In The Age Of Facebook And Google*, 80, Fordham Law Review, 4, at 1534 (2012)

"Historical and cultural data are protected under freedom of information and for this reason must be transferred to archives dedicated to historical research and should be encouraged and treated as a valid way to retain data beyond their operational utility date."[258]

Even though some censorship is active for individuals, there are types of information that are still kept in specific archives that are exclusively available for historical research. It could be assumed that access to those archives, mentioned in the previous paragraph, is not made available to everyone, so this is not sufficient to protect freedom of expression.

Some censorship and shaping of history is thus bound to occur with the removal of information and search results, and this has been stated by Google's lawyer with regard to case C-131/12:

"...a fundamental shift of responsibility from the publisher to the search engine and amount to censorship."[259]

IV. The Deciders

The fact that private companies are to make ethical and other similar decisions is a question that should be dealt with. Case C-131/12 and the GDPR leave it to private actors to decide what history is made available. Although it is the individual who fills in the application and submits the request for removal, the final decision is still left to search engine operators and webpage owners. Search engine operators are the ones to decide what is inadequate, irrelevant or no longer relevant, and, if they do not, are subject to fines. This has thus been called a license to rewrite history.[260]

A quote from Jeffrey Rosen is appropriate at this time, when analyzing the actors to whom it is left to decide on history and free speech:

---

[258] P.S. Castellano, *The right to be forgotten under European Law: a Constitutional debate*, 16.1, Lex Electronica, at 27 (2012)
[259] S. Bodoni, *Google Cites Censorship Risk in EU Data Control Law Suit*, Bloomberg (2013) http://www.bloomberg.com/news/2013-02-26/google-cites-censorship-risk-in-eu-data-control-lawsuit.html accessed 09.2014
[260] Neroth, at 16 (2014)

"Until recently, the person who had more power to determine who may speak and who may be heard around the world was not a president or king or Supreme Court Justice. She was Nicole Wong, who was deputy general counsel at Google until her recent resignation. Her colleagues called her "the Decider."[261] Nicole Wong was the Decider, who was awoken in the middle of the night to decide what content goes up or comes down, not only on Google.com, not only on each of the national Google's that are operated around the world, such as Google.fr, Google.de, but also what goes up or comes down on YouTube, which Google bought in 2006."[262]

In a world that is so dependent on technology and the Internet, should such determination be left to a private actor? It could be assumed that even if the process is left up to private companies, these cannot be certain about what to remove and what not to remove because there are no binding rules that govern those choices. It is not objectively possible for Google to decide what is of public interest and what is not. The situation in the wake of Case C-131/12 and the GDPR is that it is the private actors that are to assess every single case. This thesis agrees with Jennifer Stoddart, who, in communication with lawyers, states that realistic guidance by regulators is increasingly important to this process.[263]

As it has been demonstrated that private actors cannot objectively decide what to remove and what not, it is time to propose a possible solution:

Linked to the chapter concerned with self-regulation, that is a positive step, there exists the possibility to create some kind of an international body, like a European Commission of Forgetfulness. This international body could evaluate every single case on a case-by-case basis and decide if a particular request should be granted approval or not.[264] A commission like that, with proper legal support and legitimacy could independently and more objectively give their proposal to search engines and websites. A solution like that would have many benefits, first of all being the objectivity and consequent approach, to say nothing of lessening the burden that is now put upon private actors and search engines.

---

[261] J. Rosen, *Google's Gatekeepers*, The New York Times (2008) http://www.nytimes.com/2008/11/30/magazine/30google-t.html?pagewanted=all&_r=0 accessed 12.2014
[262] Rosen, at 1536 (2012)
[263] J. Stoddart, *Privacy in the Era of Social Networking: Legal Obligations of Social Media Sites*, 74, Saskatchewan Law Review, at 270 (2011)
[264] Rosen, at 1533 (2012)

As mentioned earlier in the thesis, in the opinion of the author, the obligation and the burden upon search engines is too great. Although Google and Yahoo could potentially cope with that amount of responsibility, smaller service providers are not able to provide acceptable results because of their resources. With an international body, private actors would not be concerned with that obligation to analyze each request, and from a financial perspective, an international body would be more efficient at that task.

"...determining when, where, and to whom the right to be forgotten should be applied is an enormous challenge."[265]

This is a challenge that should not be left to the private sector, who themselves are held liable if they make an incorrect decision. For this reason, an international body is an important aspect of this legislation.

Some authors have also proposed different options for data that exists on the Internet. One example – which could prove technically impossible – is the implementation of a life span on certain information. This would result in a meta-tag that would, in due time, remove the data automatically.[266]

The aforementioned solution is not very accurate and is technically close to impossible.[267] There are many different file formats and software platforms that support different solutions, and that is why a universal technical solution could tend to be impossible to implement. Even if there were a way to implement a technical solution, there will always arise ways to bypass these restrictions.

[265] F. Muge, *Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet*, 3, International Data Privacy Law, 3, at 152 (2013)
[266] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, at 15 (2009)
[267] Ibid.

V. Unintended Backlash

Although the right to be forgotten is formed with good intentions in mind – that is, to help an individual remove old, inadequate, inaccurate, irrelevant or excessive information about them[268]– there are ways in which media has begun to turn that intention in the opposite direction. At this point in time, there are no scientific articles that touch upon this issue, but there are already some cases in which a serious backlash to privacy has occurred.

There are many different parties involved once a removal request has been submitted to Google, for example. It is not a minor matter, as can be seen further in the thesis, that Google is not the original publisher and has to inform the original publisher that a request has been filed for the removal of search requests. As has been seen, this communication not only involves the search engine and the individual who has made the request but also the publisher of the information.

There is a term that has been called the "Streisand effect"[269], which is derived from a recent privacy issue concerning Barbara Streisand.[270] With that effect, the media companies, who are the main target of the right to be forgotten, are turning the intention of the right in another direction.

In 2010 The Bolton News published a story about three soldiers who came under attack in a nightclub and feared for their lives.[271] After the publishing the article, a removal request was submitted to Google, asking the search engine to remove the search result that lead to the article. Google then removed the search result and informed Bolton News of the removal. Bolton News then made a move that completely turned the result around. They published a story about the

---

[268] A. Suuberg, *The View from the Crossroads: The European Union's New Data Rules and the Future of U.S. Privacy Law*, 16, Tulane Journal of Technology and Intellectual Property, at 282 (2013)
[269] The Streisand effect is the phenomenon whereby an attempt to hide, remove, or censor a piece of information has the unintended consequence of publicizing the information more widely, usually facilitated by the Internet.
[270] J. Parkinson, *The perils of the Streisand effect*, BBC (2014) http://www.bbc.com/news/magazine-28562156 accessed 12.2014
[271] *Soldiers feared for their lives in nightclub brawl*, The Bolton News (2010) http://www.theboltonnews.co.uk/news/8440496.Soldiers_feared_for_their_lives_in_nightclub_brawl/ accessed 10.2014

removal request in which they drew attention the article concerned in the removal request.[272] Bolton News is not the only institution that has used a similar approach of highlighting a removal request, and a similar approach has been taken by numerous press actors.[273]

This cannot in any case then co-exist with the reasoning behind the right to be forgotten. If the right is intended to facilitate forgiveness on the Internet, then this acts as a tremendous backlash and only draws greater attention to the issue that was meant to be forgotten.

VI. Privacy Re-conceptualization

From a more philosophical point of view, once could ask whether there is any privacy in the information and communication age, or if attempts to enforce and protect it are bound to fail.

"You have zero privacy anyway, get over it."[274] This is the sentence used by Scott McNealy, the CEO of Sun Microsystems, in 1999. 1999 was a long time ago but it could be said that the sentiment is still valid.

Nevertheless, the previous statement by Mr. McNealy's speaks some truth in that the conceptions of privacy that are used and carried over from the analog world have not aged gracefully.[275]

People around the world are giving privacy a new meaning. They are posting vast amounts of information about themselves, including their background, habits, interests, friends and family for others to view on different Internet platforms like social networks, blogs, and text

---

[272] C. White, *Bolton News story 'erased' from Google search results because of EU ruling*, The Bolton News (10 July 2014) http://www.theboltonnews.co.uk/news/11330343.Bolton_News_story__erased__from_Google_search_results_because_of_EU_ruling/ accessed 10.2014

[273] M. Masnick, *Google Alerts Press About Right To Be Forgotten Removals, Putting Those Stories Back In The News*, TechDirt (2 July 2014) https://www.techdirt.com/articles/20140702/12094027764/google-alerts-press-about-right-to-be-forgotten-removals-putting-those-stories-back-news.shtml accessed 10.2014

[274] P. Sprenger, *Sun on Privacy: 'Get Over it'*, Wired News, (1999) http://archive.wired.com/politics/law/news/1999/01/17538 accessed 10.2014

[275] W.T. DeVries, *Protecting Privacy In The Digital Age*, 18, Berkeley Technology Law Journal, 1, at 283 (2003)

messages.[276] Perhaps people and lawmakers ought to focus on preventing the misuse and abuse of information instead of enforcing privacy.

It could be agreed that the laws applicable are insufficient and too outdated to address today's consumers acting on the Internet.

Consumers of the Internet are often also overlooking the need for regulation, judicial recourse, and remedies because the Internet has a lot to offer, like many entrancing, commercial benefits available on new media, which make the temptation of an unregulated web, seem romantic and enchanting. With the Internet the ability to establish and maintain associations has multiplied.[277]

With that in mind, the lure of the Internet is understandable and there is no need to justify it anymore. There are specific positive and negatives sides of the Internet, like loss of privacy and growth of freedom of expression and connectivity.

The Internet is a positive environment for sharing ideas, knowledge, memories, creativity and all of its positive features can be agreed to be good from the viewpoint of an individual. The aspect that is most often overlooked concerns the Internet's dominant actors. These are the service providers, whose interest is in profiting from individuals' information.[278]

There are many different views and approaches concerning the notion of privacy. Daniel J. Solove proposes that there needs to be a change in its conceptualization:

"...if we merely seek to preserve those activities and matters that have historically been considered private, then we fail to adapt to the changing realities of the modem world."[279]

Alexander Tsesis proposes that different laws are necessary for maintaining privacy, and these not only have to be effective with regard to commercial exploitation but also have to set out

---

[276] A. Tsesis, *The Right To Erasure: Privacy, Data Brokers, And The Indefinite Retention Of Data*, 49, Wake Forest Law Review, at 460 (2014)
[277] Ibid.
[278] Ibid., at 461
[279] Solove, at 1142 (2002)

procedural rules for a fair trial.[280] There is no question about different approaches on privacy, because there are many of them.[281]

Tort law that is applicable today is also concerned with the misuse of information, so perhaps it could be held that a new conception of privacy is needed: a concept wherein the balance is shifted from away from privacy and toward information misuse. Ultimately, the approach to privacy must be practical and adapted to technological developments. Attention should be paid to helping people understand the amount of information they themselves provide, and to providing guidance to service providers on how and what information they use.[282]
A similar tort-law-centered approach is applicable in the United States of America. There is no right to be forgotten in the U.S and the closest civil action is that an individual could file a claim upon his invasion of privacy. This could appear because of publication of private facts or public disclosure.[283]

The Restatement of Torts[284] states the following:

"One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that
(a) would be highly offensive to a reasonable person, and
(b) is not of legitimate concern to the public."[285]

This thesis cannot propose an objective and ideal approach to privacy and it does not intend to do so. The intent behind this chapter is to give a broad overview of the different approaches to privacy that need to be taken into account in light of the subject matter at hand.

[280] Tsesis, at 461 (2014)
[281] Solove, at 1087 (2002)
[282] DeVries, at 311 (2003)
[283] McNealy, at 15-16 (2012)
[284] Restatement (Second) of Torts, cmt. b (1965).
http://lexinter.net/LOTWVers4/restatement_%28second%29_of_torts.htm accessed 12.2014.
[285] Ibid., at Section 652D.

D. Article 29 Data Protection Working Party[286] Guidelines

Following the ruling in case C-131/12, WP29 issued a press release on July25, 2014 describing the contents of a meeting that was held with representatives of Google, Microsoft, and Yahoo, the operators of the three largest Internet search engines. During the meeting, WP29 asked search engines about the practical implementation of the right to be forgotten, in order to compose their guidelines. With these guidelines, the WP contributed to the consistent handling of complaints.[287]

During the meeting the representatives of the three companies explained their views on the application of the right to be forgotten and answered some questions. The questions that were asked dealt primarily with the delisting process of search results.[288] After the meeting, the WP29 issued their guidelines on the application in autumn, 2014.[289]

The guidelines that were adopted on November26, 2014, have two parts: the first concerns the interpretation of the CJEU judgment, and the second is a list of common criteria for the handling of complaints by European data protection authorities.

I. Executive Summary

The WP29 has composed their own interpretation of the ruling. The guidelines clarified certain points from the C-131/12 CJEU ruling and an executive summary of them is as follows:[290]

---

[286] Article 29 Data Protection Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
[287] Article 29 Data Protection Working Party - PRESS RELEASE - Adoption of guidelines on the implementation of the CJEU's judgment on the "right to be forgotten" (25 July 2014)
[288] Ibid.
[289] Article 29 Working Party, *Guidelines on the Implementation of The Court of Justice of the European Union Judgment on "Google Spain and Inc V. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12,* (6 November 2014) (hereafter WP29 Guidelines)
[290] Ibid., at 2-3.

The guidelines are so new that there are no sources but this thesis intends to give a description on the content of these guidelines as it is relevant for the analysis conducted.

1) Search engines as data controllers

WP29 emphasizes upon the ruling that search engine operators are to be considered as data controllers because they are processing personal data and within the meaning of Article 2 of Directive 95/46/EC they are to be qualified as data controllers.[291]

"The processing of personal data carried out in the context of the activity of the search engine must be distinguished from, and is additional to that carried out by publishers of third-party websites."[292]

With this WP29 basically affirms the statement that was made in the C-131/12 ruling.

2) A fair balance between fundamental rights and interests

WP29 also acknowledges that a data subject's rights, as a general rule, prevail over the economic interest of search engines, and the public's right of access to information. They state that a balance of relevant rights and interests must be made on a case-by-case analysis and its outcome depends on the public interest and the nature of the data being processed. It is also stresses that the public interest is greater if the data subject is a public figure.[293]

3) Limited impact of de-listing on the access to information

With this, the WP29 argues that the impact of the right to be forgotten is limited with regards to freedom of expression and access to information. In each case an assessment of circumstances has to be concluded and the interest of the public has to be taken into account. If the interest prevails over the right to be forgotten, de-listing will not be justified.[294]

[291] Ibid., at 2
[292] Ibid.
[293] Ibid.
[294] Ibid.

4) No information is deleted from the original source

As in the C-131/12 ruling, WP29 confirms that no information shall be deleted from the original source. The right to be forgotten only applies to searches made on the basis of an individual's name and with that it is not required to delete the link from a search engine's indexes. The original information will still be available with different search terms or by direct access to the original source. Only the search results that include the individual's name are required to be removed.[295]

5) No obligation on data subjects to contact the original website

Individuals exercise their rights toward the search engines and thus, they have no obligation to contact the original publisher and they can directly contact the search engine as a data controller.[296] The original publisher actually has no relation to the right to be forgotten in case C-131/12 because the original information shall always be available on the website. The only information that will be removed is the search result of a search engine, so the data subject's name would not be related to the original information in the indexes.

6) Data subjects' entitlement to request de-listing

Although with regard to EU law, every individual has a right to data protection, in practice there should be a clear link established between the data subject and the European Union, for instance, the data subject has to be a resident or a citizen of the EU.[297]

7) Territorial effect of a de-listing decision

This point in the WP29 guidelines is of somewhat larger importance. They emphasize that the de-listing of a search result from a national domain is not enough to guarantee the protection of data subjects' rights. It is not justifiable to circumvent the EU law by limiting the de-listing to EU domains. All relevant domains should be influenced by the right to be forgotten and this

[295] Ibid.
[296] Ibid.
[297] Ibid.

includes, for example, .com domains.[298] It is argued that non-EU countries have four options in this case, they either (1) adopt the same right to erasure; (2)ignore the erasure claims; (3) comply with take down requests; or (4) establish a modified version of the right.[299]

8) Information to the public on the de-listing of specific links

The WP29 states that search engines should not inform the public about the incomplete nature of their search results. This practice is only acceptable when "users cannot, in any case, conclude that one particular individual has asked for de-listing of results concerning him or her."[300]

9) Communication to website editors on the de-listing of specific links

Data controllers should not inform the original publishers about the removal of search results related to them. In some cases search engines may want to contact the original publisher in order to obtain addition information about the removal request. EU law in itself does not require this communication.[301] With that the WP29 indirectly aims to prevent the Streisand Effect from occurring.[302]

As we have seen, the WP29 interprets case C-131/12 in a somewhat narrow manner and suggests that these guidelines should be followed.

In conclusion, the key messages that the WP29 addresses are as follows:

1) "The right only affects the results obtained from searches made on the basis of a person's name;
2) The right does not require deletion of the link from the indexes of the search engine altogether, meaning that the original information can still be accessible using other search terms, or by direct access to the source;

[298] Ibid.
[299] M. L. Ambrose, *Speaking of Forgetting: Analysis of Possible Non-EU Responses to the Right to be Forgotten and Speech Exception,* Telecommunications Policy TPRC 2013 Submission (2013)
[300] WP29 Guidelines, at 2
[301] Ibid.
[302] Parkinson (2014)

3) De-listing decisions must be implemented in such way that they guarantee the effective and complete protection of data subjects' right; and
4) The EU law cannot be circumvented by for instance limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains; it follows from this that in any case de-listing should also be effective on all relevant .com domains"[303]

II. Criteria for the Right to Be Forgotten

In addition to the interpretation of case C-131/12, the WP29 also, in addition to its guidelines, composed a list of 13 criteria to be used as a flexible working tool to help data protection agencies assess complaints on a case-by-case basis. The criteria were analyzed by WP29 upon complaints received from data subjects whose removal requests were denied.[304]
WP29 stressed that in most cases, more than one criterion will need to be taken into account to reach a correct decision and no single criterion in itself will be determinative.[305]

"Each criterion has to be applied in the light of the principles established by the CJEU and in particular in the light of the "the interest of the general public in having access to [the] information."[306]

The guidelines contain 13 criteria for data protection agencies to judge the merits of complaints. This list can also be used by data controllers upon reaching request refusal decisions.

Based upon the criteria, data protection agencies must analyze the following:

1) Does the search result relate to a natural person – i.e. an individual? And does the search result come up against a search on the data subject's name?

[303] P. Van Eecke, J. De Bruyn, *Europe: right to be forgotten guidelines adopted by WP29*, Lexology, (27 November 2014) http://www.lexology.com/library/detail.aspx?g=59dc3e68-bcc4-467b-aaf3-fbb53a25f469 accessed 12.2014
[304] WP29 Guidelines, at 12
[305] Ibid.
[306] Ibid.

The DPA[307] must analyze whether the search result relates to a natural person's name, including pseudonyms and nicknames that relate to an individual's real identity.[308]

2) Does the data subject play a role in public life? Is the data subject a public figure?

The WP29 states that is difficult to decide what constitutes a role in public life, but they outlined a simple illustrative rule:

"Try to decide where the public having access to the particular information – made available through a search on the data subject's name – would protect them against improper public or professional conduct."[309]

The same can be said of public figures: it is not easy to define one.

"In general, it can be said that public figures are individuals who, due to their functions/commitments, have a degree of media exposure."[310]

The WP29 also differentiates between a public figures' private and public lives with the help of the Von Hannover v Germany case.[311]

3) Is the data subject a minor?

The de-listing is more likely to be required if the data subject, at the time of the publishing, was under-age. The WP29 refers to Article 24 of the EU Charter of Fundamental Rights.[312]

4) Is the data accurate?

Here the WP29 clearly differentiates between a matter of fact and a matter of opinion. Accuracy has only to do with factual circumstances.[313]

---

[307] Data Protection Agency
[308] WP29 Guidelines, at 13
[309] Ibid.
[310] Ibid., at 14
[311] Von Hannover v Germany [2004] ECHR 294 (24 June 2004), European Court of Human Rights
[312] WP29 Guidelines, at 15

5) Is the data relevant and not excessive?

a. Does the data relate to the working life of the data subject?

b. Does the search result link to information which allegedly constitutes hate speech/slander/libel or similar offences in the area of expression against the complainant?

c. Is it clear that the data reflect an individual's personal opinion or does it appear to be verified fact?

The age of the data is most likely the key here and a difference should be made between an individual's personal and professional life.[314]

6) Is the information sensitive within the meaning of Article 8 of the Directive 95/46/EC?

7) Is the data up to date? Is the data being made available for longer than is necessary for the purpose of the processing?

The original purpose of the processing is the key element at this point.[315]

8) "Is the data processing causing prejudice to the data subject? Does the data have a disproportionately negative privacy impact on the data subject?"[316]

9) "Does the search result link to information that puts the data subject at risk?"[317]

10) In what context was the information published?

a. Was the content voluntarily made public by the data subject?

---

[313] Ibid.
[314] Ibid., at 15-17
[315] Ibid., at 17-18
[316] Ibid., at 18
[317] Ibid.

b. Was the content intended to be made public? Could the data subject have reasonably known that the content would be made public?

The WP29 bases its arguments on the data subject's consent. If at the time the data subject's consent was the only justification for the publication of data, and that consent is now revoked, the removal of search results is likely to be approved.[318]

11) "Was the original content published in the context of journalistic purposes?"[319]

12) "Does the publisher of the data have a legal power – or a legal obligation – to make the personal data publicly available?"[320]

13) Does the data relate to a criminal offence?

If the data relates to a criminal offence, national law governing the public availability of such information should be taken into account.[321]

Unfortunately, in these recently adopted guidelines, the concepts discussed are actually quite vague and this vagueness could become a problem in time. In order to give them more content, further case law should be written regarding the right to be forgotten. National legislation could also help with this issue, but the final decision-making will always be incumbent upon the CJEU. Although the guidelines with their list of criteria are of help to data protection agencies and data controllers, it should not be forgotten that they are not legally binding upon the EU law and courts. With the guidelines being very novel at this point in time, there are no scholarly articles or case-law that has analyzed them, and the issue of the right to be forgotten from this perspective. European law still gives each Member State the authority to determine the balance between freedom of expression and privacy.[322]

[318] Ibid., at 19
[319] Ibid.
[320] Ibid.
[321] Ibid., at 20
[322] GDPR Proposal, at Art. 80

Concluding Remarks

This thesis set out to explore the concept of the right to be forgotten with regard to forthcoming European data protection reform and the recent CJEU case C-131/12.

The right to be forgotten is a novel concept that has provoked debate because of the controversial C-131/12 case that supported application of the right. The CJEU based its judgment upon European Parliament Directive 95/46/EC, and on that of the Council of October 24th, 1995 – concerning the protection of individuals with regard to the processing of personal data, and the free movement of such data – which, by their reasoning, already contained the right to be forgotten.

Although the right is positive for an individual, aiming as it does to prevent lives from being influenced by the irrelevant actions of the past, it is nonetheless problematic in certain respects. The concept of the right is vague and brings with it many challenges to freedom of expression, censorship, and other issues such as historical documentation and historical truth.

As stated in the introduction, the aim of this thesis has been to identify the feasibility of actual implementation of the right to be forgotten, and to explicate the problematic aspects and critiques of the concept.

This thesis sought to find an answer to the following question:

Is the right to be forgotten compatible with other rights, and is the application of the right actually possible and proportionate?

The aim of the thesis was accomplished through a comprehensive analysis that thoroughly explored and explained the topic and issues surrounding the right to be forgotten, exploring its pros and cons.

As a new and broad concept, the right to be forgotten is a concept that needs clarification and analysis, and although the CJEU case C-131/12 answered some important questions, there will certainly be attempts to re-visit those issues in the future.

This thesis is divided into sections. The first contains a description of Internet privacy and the EU data protection law currently in place. It also analyses forthcoming data protection reform.

Privacy was broadly defined as the notion that an individual ought to have control over his personal life and the information related to it.

After defining what privacy is, the thesis introduced the two primary instruments for privacy and data protection in the EU: the Convention for the Protection of Human Rights and Fundamental Freedoms, and the European Charter of Fundamental Rights. The primary tool for protecting privacy is the 95/46/EC directive based upon the CFREU and the ECHR. Although the Data Protection Directive is a necessary tool, technological developments in the intervening years have raised new challenges and concerns for the protection of personal data. With the Data Protection Directive, Member States have achieved a result in which there are many divergences in the rules' enforcement. These are among the primary reasons that the EU is in need of a single, comprehensive regulation and a data protection reform. This thesis established that the biggest change regarding data protection reform is the distinction between the application of a directive and the application of a regulation that is directly applicable in each Member State.

This first section also gives a definition of the right to be forgotten, as stated in the Data Protection Directive and as it shall remain in the new proposed regulation.

The second section of the thesis highlighted European Court judgment C-131/12, which supported the right to be forgotten in the European Union.

This section highlighted the most important aspects of the C-131/12 case related to the right to be forgotten, and discussed AG Jääskinen's reasoning in his opinion.

The CJEU has stated that:

1) Search engines are to be considered as data controllers.

2) If a company has an establishment to which they are inextricably and economically linked, this is sufficient to make the company responsible under EU data protection law.

3) A search engine is responsible for the removal of search results under the European Data Protection Directive, because it is considered a data controller.

4) The right to be forgotten already exists in the Data Protection Directive.

The following sections of the thesis concern critiques of, and conflicts with, the right to be forgotten.
These sections include an analysis of the relation between freedom of speech and the right to be forgotten.

The thesis, after analyzing these issues, states that the right to be forgotten and freedom of expression are in conflict, because they are both equal rights and giving the right to privacy a superior status, superseding other fundamental rights, gives it the potential to shape history and limit freedom of expression. The vagueness and essentially subjective nature of the whole concept of the right to be forgotten is one of its most problematic issues.

Further on, I have analyzed the delegation of rights and privatization of the implementation of the right to be forgotten. The conclusion that was reached suggested that, due to the delegation of the implementation of the right to be forgotten, search engines might be keen on removing more than should be removed, because reaching a result later deemed wrong would make them liable. And with search engines as one of the most important modern means of finding information, the shaping of history becomes a concern. This thesis asserts that the right to freedom of expression holds in itself the right to access history.

Some unintended consequences of the right to be forgotten, as it is implemented at this time, are also discussed. Primarily, this thesis argues that the removal of a search result, while intended to give an individual the right to not be affected by actions performed in the past, could in fact have the opposite effect. As the original information remains online while search engine operators negotiate with the original publisher about removing results that are linked to their website, the original publishers have found ways to highlight the situation that was discussed in the original article and thus bring it a great deal of attention.

A new definition of privacy is also discussed. The re-conceptualization of privacy could be a solution with regard to the Internet that has so suddenly appeared. The balance could shift from privacy to misuse of information and should be adapted to technological developments.

Finally, this thesis discusses new guidelines for the application of the right to be forgotten, as adopted by the Article 29 Data Protection Working Party. Concluding the section, this thesis notes that these guidelines are vague and that this vagueness is due to become a problem. The guidelines and the criteria of the right to be forgotten need further case law that addresses the specifics of the issue. Some help could be provided by the national legislation of EU Member States, but it should not be forgotten that these are not legally binding upon EU law and courts, and the final decision-making will always be upon the CJEU.

The constraints of this thesis did not allow detailed consideration of every significant aspect of the right to be forgotten, and it concentrated primarily on the legal aspects of the right to be forgotten and data protection.

Limitations on the approach of this thesis also appeared due to the lack of scientific information composed on the topic. This issue is so novel that the amount of peer-reviewed scholarly information is limited. There is no significant case-law on the topic, and there are no scientific articles about the newly proposed WP29 guidelines.

This thesis is significant because of its comprehensive approach to the issue of the right to be forgotten. Novelty is another key factor that is of importance, given the topic. This thesis is novel and complements earlier works by different authors.

Further research should concentrate on the moral, ethical, and sociological aspects of the right that invite analysis by specialists in these respective fields. Also, after the implementation of the new General Data Protection Regulation and the development of some case-law, further analysis should be conducted on the issue of the right to be forgotten.

In conclusion and to answer the central question of this thesis:

The right to be forgotten poses a serious threat to freedom of expression in the Internet era. It has the potential to make Internet actors like Google and Yahoo liable if they are not able to

correctly remove data about individuals. Thus, there is a fine balance to be struck between the right to privacy and freedom of expression that, if not carefully considered, could lead to a less open Internet and a conflict of rights.

List of Sources

Books

Bender, David, A Guide to Cyberlaw and Data Privacy, Matthew Bender (2012)

Bermann, George, Goebel, Roger J., Davey, William, Fox, Eleanor, Cases and Materials on European Union Law 23, 3rd ed., Oxford University Press (2011)

Black, Gillian, Publicity Rights and Image: Exploitation and Legal Control, Hart Publishing (2011)

Garfinkel, Simson, Database Nation: The Death of Privacy in the 21st Century, O'Reilly Media Inc (2000)

Haraszti, Miklos, Baydar, Yavuz, Gore, William, Zlatev, Ognian, Maurus Véronique, The Media Self-Regulation Guidebook, Organization for Security and Co-operation in Europe, 9 (2008) Online at http://www.osce.org/fom/31497?download=true (Last visited 18 September 2014)

Joseph, Brian (Ed.); Janda, Richard (Ed.), The Handbook Of Historical Linguistics. Blackwell Publishing, 163 (2004)

Lim, Yee Fen, Cyberspace Law: Commentaries And Materials, Oxford University Press (2nd Ed) (2007)

Mayer-Schönberger, Viktor, Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, 15 (2009)

Puddephatt, Andrew, Freedom of Expression, The essentials of Human Rights, Ed. Hodder Arnold, 128 (2005)

Steiner, Josephine, Woods, Loma, Twigg-Flesner, Christian, EU Law, Oxford: Oxford University Press (2006)

Articles

Akhtar, Zia, *Malicious communications, media platforms and legal sanctions*, Computer and Telecommunications Law Review, Sweet & Maxwell and its Contributors, 179-187 (2014)

Ambrose, Meg, Leta,, Friess, Nicole, Jill, Van, Matre, *Seeking Digital Redemption: The Future Of Forgiveness In The Internet Age*, 29, Santa Clara Computer & High Technology Law Journal, 99-163 (2012)

Carter, Edward, L., *Argentina's Right to be Forgotten,* 27, Emory International Law Review, 23-39 (2013)

Castellano, Pere, Simón, *The right to be forgotten under European Law: a Constitutional debate*, 16.1, Lex Electronica, 1-30 (2012)
Online at http://www.lex-electronica.org/docs/articles_300.pdf (Last visited 20 October 2014)

Crowther, Hannah, *Remember to forget me: the recent ruling in Google v AEPD and Costeja*, 20 (6), Computer and Telecommunications Law Review, 163-165 (2014)

DeVries, Will, Thomas, *Protecting Privacy In The Digital Age*, 18, Berkeley Technology Law Journal, 1, 283-311 (2003)

Van Eecke, Patrick, De Bruyn, Julie, *Europe: right to be forgotten guidelines adopted by WP29*, Lexology, (27 November 2014)
Online at http://www.lexology.com/library/detail.aspx?g=59dc3e68-bcc4-467b-aaf3-fbb53a25f469 (Last visited 27 December 2014)

Faye, Bohan, *Liability Of Internet Search Engines*, Hibernian Law Journal, 181-228 (2006)

Giurgiu, Andra, *Challenges of Regulating a Right to Be Forgotten with Particular Reference to Facebook,* 7(2), Masaryk University Journal of Law And Technology, 361-378 (2013)

Haynes, Stuart, Allyson, *Google Search Results: Buried If Not Forgotten*, 15, North Carolina Journal Of Law & Technology, 3, 463-518 (2014)

James, Steven, *The right to privacy catches up with search engines: the unforgettable decision in Google Spain v AEPD*, 20 (5), Computer and Telecommunications Law Review, 130-133 (2014)

Koops, Bert-Jaap, *Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice,* 8, SCRIPTed, 3, 229-256 (2011)

Larsen, Katharine, *Europe's "Right to Be Forgotten" Regulation May Restrict Free Speech*, 17, First Amendment & Media Litigation, 1, 12-14 (2012)

McNealy, Jasmine, *The Emerging Right to be Forgotten: How a Proposal in Europe Could Affect the Sharing of Information,*12, Insights on Law and Society, 3 (Spring), 14-17 (2012)

Muge, Fazlioglu, *Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet*, 3, International Data Privacy Law, 3, 149-157 (2013)

Neroth, Pellel, *Challenge of balancing privacy with censorship ends up in Google's lap*, 9, Engineering & Technology, 7, 16 (2014)

Nys, Herman, *Towards a Human Right 'to be Forgotten Online'?,*18 (5), European Journal of Health Law, 469-475 (2011)

Reding, Viviane, *The Upcoming Data Protection Reform for the European Union*, 1, International Data Privacy Law, 3-5 (2011)

Rosen, Jeffrey, *The Deciders: The Future Of Privacy And Free Speech In The Age Of Facebook And Google*, 80, Fordham Law Review, 4, 1525-1538 (2012)

Rosen, Jeffrey, *The Right to be Forgotten,* 64, Stanford Law Review Online, 88-92 (2012)

Online at http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten (Last visited 27 December 2014)

Siegel, Loren, *Should The Internet Be Censored? No! No! No! No!*, 22, Update On Law-Related Education, 2, American Bar Association 12&14 (1998)

Shoor, Emily, *Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation*, 39, Brooklyn Journal of International Law, 1, 487-519 (2014)

Snijders, Chris, Matzat, Uwe, Reips, Ulf-Dietrich, *'Big Data': Big gaps of knowledge in the field of Internet*, 7, International Journal of Internet Science, *7*, 1-5 (2012)
Online at http://www.ijis.net/ijis7_1/ijis7_1_editorial.pdf (Last visited 14 September 2014)

Solove, Daniel J., *The End of Privacy?*, 299, Scientific American, 1, 100-106 (2008)

Spinello, Richard A., *The End of Privacy*, 176, America, 1/4, 1, (1997)

Stoddart, Jennifer, *Privacy in the Era of Social Networking: Legal Obligations of Social Media Sites*, 74, Saskatchewan Law Review, 263-275 (2011)

Suuberg, Alessandra, *The View from the Crossroads: The European Union's New Data Rules and the Future of U.S. Privacy Law*, 16, Tulane Journal of Technology and Intellectual Property, 267-286 (2013)

Thompson, Bill, Kates, Andrea, *The Debate*, 9, Engineering & Technology, 8, 26 (2014)

Tsesis, Alexander, *The Right To Erasure: Privacy, Data Brokers, And The Indefinite Retention Of Data*, 49, Wake Forest Law Review, 433-484 (2014)

Internet

Bodoni, Stephanie, *Google Cites Censorship Risk in EU Data Control Law Suit*, Bloomberg (26 February 2013)
Online at http://www.bloomberg.com/news/2013-02-26/google-cites-censorship-risk-in-eu-data-control-lawsuit.html (Last visited 20 October 2014)

Crehan, Fergal, *Google Spain, What It Means and What It Doesn't,* Fergal Crehan BL (14 May 2014) http://fergalcrehan.com/2014/05/14/google-spain-what-it-means-and-what-it-doesnt/ (Last visited 18 September 2014)

European Union, http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm, (Last visited December 2014)

Fisher, Owen, *Google Right to be Forgotten … but what about business data?,* Magnifica (20 August 2014)
Online at http://www.magnifica.co.uk/blog/google-right-to-be-forgotten-what-about-business-data (Last visited 12 September 2014)

Fleischer, Peter, *Foggy Thinking about the Right to Oblivion*, PETER FLEISCHER: PRIVACY ... ? (2011)
http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-tooblivion.html (last visited 29 December 2014)

Flower, Kevin, *Facebook page supporting Palestinian intifada pulled won,* Cable News Network, Turner Broadcasting System Inc. (29 March 2011)
Online at http://edition.cnn.com/2011/WORLD/meast/03/29/palestinian.facebook/index.html?_s=PM:WORLD (Last visited 27 December 2014)

Gibbs, Mark, *Freedom and Privacy, R.I.P.,* Network World (2011)
Online at http://www.networkworld.com/article/2179900/security/freedom-and-privacy--r-i-p-.html (Last visited 27 December 2014)

Freedom of Expression, Human Rights Education Associates
Online at http://www.hrea.org/index.php?base_id=147 (Last visited 18 September 2014)

Google Support page about search removal request
https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=en (Last visited 14 September 2014)

Khan, Shaan, *Taliban attack wounds teen activist blogger*, Cable News Network, Turner Broadcasting System Inc. (10 October 2011)
Online at http://edition.cnn.com/2012/10/09/world/asia/pakistan-teen-activist-attack/ (Last visited 27 December 2014)

Lowe, Josh, *What's wrong with the 'right to be forgotten'?,* Prospect (30 July 2014)
Online at http://www.prospectmagazine.co.uk/blogs/prospector-blog/whats-wrong-with-the-right-to-be-forgotten (Last visited 14 September 2014)

Masnick, Mike, *Google Alerts Press About Right To Be Forgotten Removals, Putting Those Stories Back In The News*, TechDirt (2 July 2014)
Online at https://www.techdirt.com/articles/20140702/12094027764/google-alerts-press-about-right-to-be-forgotten-removals-putting-those-stories-back-news.shtml (Last visited 20 October 2014)

Munslow, Alun, *What is History?*, History In Focus, *2*, University Of London (2001)
Online at http://www.history.ac.uk/ihr/Focus/Whatishistory/munslow6.html (Last visited 5 October 2014)

Open Rights Group
https://www.openrightsgroup.org/blog/2014/landmark-ruling-by-european-court-on-google-and-the-right-to-be-forgotten (last visited September 2014)

Parkinson, Justin, *The perils of the Streisand effect*, BBC (30 July 2014)
Online at http://www.bbc.com/news/magazine-28562156 (Last visited at 27 December 2014)

Plummer, Quinten, *Google, Microsoft, Yahoo meet EU data regulators to discuss 'right to be forgotten' ruling,* Tech Times (28 July 2014)
Online at http://www.techtimes.com/articles/11366/20140728/google-microsoft-yahoo-meet-eu-data-regulators-to-discuss-right-to-be-forgotten-ruling.htm (Last visited 14 September 2014)

Rosen, Jeffrey, *Google's Gatekeepers,* The New York Times (28 November 2008)
Online at http://www.nytimes.com/2008/11/30/magazine/30google-t.html?pagewanted=all&_r=0 (Last visited 27 December 2014)

Soldiers feared for their lives in nightclub brawl, The Bolton News (2010)
Online at http://www.theboltonnews.co.uk/news/8440496.Soldiers_feared_for_their_lives_in_nightclub_brawl/ (Last visited 20 October 2014)

Sprenger, Polly, *Sun on Privacy: 'Get Over it'*, Wired News, (1999)
Online at http://archive.wired.com/politics/law/news/1999/01/17538 (Last visited 20 October 2014)

White, Chris, *Bolton News story 'erased' from Google search results because of EU ruling*, The Bolton News (10 July 2014)
Online at http://www.theboltonnews.co.uk/news/11330343.Bolton_News_story__erased__from_Google_search_results_because_of_EU_ruling/ (Last visited 27 December 2014)

Wikileaks http://wikileaks.org/About.html (last visited 27 December 2014)

Other Sources

Alsenoy, Brendan Van, Kuczerawy, Aleksandra, Ausloos, Jef, *Search engines after Google Spain: internet@liberty or privacy@peril?*, ICRI working paper, 65 (2013)

Ambrose, Meg, Leta, *Speaking of Forgetting: Analysis of Possible Non-EU Responses to the Right to be Forgotten and Speech Exception,* Telecommunications Policy TPRC 2013 Submission (2013)

Article 29 Working Party, *Guidelines on the Implementation of The Court of Justice of the European Union Judgment on "Google Spain and Inc V. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12*, (6 November 2014)

Article 29 Data Protection Working Party - PRESS RELEASE - Adoption of guidelines on the implementation of the CJEU's judgment on the "right to be forgotten" (25 July 2014)

Backes, Michael, Druschel, Peter, Tirtea, Rodica, The Right to Be Forgotten – Between Expectations and Practice, European Union Agency for Network and Information Security (2012)
Online at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/at_download/fullReport (Last visited 27 December 2014)

Bender, David *A Guide to Cyberlaw and Data Privacy, §51.04 (rev. 2013); CDT Analysis of the Proposed Data Protection Regulation*, CTR. for Democracy & Tech." (2012) Online at https://www.cdt.org/files/pdfs/CDTDPR-analysis.pdf. (Last visited August 2014)

Council of the European Union, EU Human Rights Guidelines on Freedom of Expression
European Council, Brussels, EUCO 169/13, (25. October 2013) http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf (Last visited December 2014)

House of Lords, European Union Committee, *EU Data Protection law: a 'right to be forgotten'?* 2nd Report of Session 2014–15, London, (2014)

Merriam Webster website http://Merriam-Webster.com (last visited 6 August 2014)

Reding, Viviane, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, Transcription of the speech held at the Digital

Life Design conference (2012) Online and Offline, FOREIGN AFFAIRS Council meeting, Brussels, (12 May 2014)
Online at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF (last visited 29 December 2014)

Restatement (Second) of Torts, cmt. b (1965). http://lexinter.net/LOTWVers4/restatement_%28second%29_of_torts.htm (last visited 29. December 2014)

European Commission

European Commission, *Commission proposes a comprehensive reform of the data protection rules* http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm (Last visited August 2014)

European Commission, *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses* http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en (25 January 2012) (Last visited August 2014)

European Commission, *Data protection reform: Frequently asked questions*, (25 January 2012) http://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=en (Last visited August 2014)

European Commission Factsheet about data protection http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (Last visited 10 August 2014)

European Commission, How will the data protection reform affect social networks? http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf, (Last visited August 2014)

European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation),* Brussels, COM(2012) 11 final 2012/0011 (COD) (25 January 2012)

Legislative Acts

Council of the European Union, *Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,* Official Journal J L 350, (27 November 2008)

European Union, *Directive 2000/31 of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce),* Official Journal L 178, 17.07.2000, 1-16. (8 June 2000)

European Union, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,* Official Journal L 281 , 23/11/1995 P. 0031 – 0050, (24 October 1995)

Treaties and Conventions

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14,* (4 November 1950)

Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* CETS No. 108, (28 January 1981)

European Union, *Charter of Fundamental Rights of the European Union,* 2012/C 326/02, (26 October 2012)

European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, 2008/C 115/01, 13 December 2007

European Union, *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*, 2007/C 306/01, (13 December 2007)

UN General Assembly, *International Covenant on Civil and Political Rights*, United Nations, Treaty Series, vol. 999, p. 171, (16 December 1966)

UN General Assembly, *Universal Declaration of Human Rights*, 217 A (III), (10 December 1948)

Case Law

<u>EU Courts</u>

Judgment of 7 December 1976 in *Handyside v. the United Kingdom* series A, No. 24. European Court of Human Rights

Judgment of 6 November 2003 in case C-101/01, Bodil Lindqvist v Åklagarkammaren i Jönköping, CJEU

Judgment of 24 June 2004 in *Von Hannover v Germany,* 294, European Court of Human Rights

Judgment of 13 May 2014 in case C-131/12, *Google Spain and Google*, Google Spain SL, Google Inc. v. Agencia de Protección de Datos (AEPD),Mario Costeja González, CJEU

<u>Advocate General Opinions</u>

Advocate General Jääskinen in Case C-131/12, *Google Spain and Google*, Google Spain SL, Google Inc. v. Agencia de Protección de Datos (AEPD),Mario Costeja González

Canada

R v Duarte (also *R v Sanelli*) Supreme Court of Canada, 20542 (1990)

R v Edwards, Supreme Court of Canada, 24297 (1996)