The Right to be Forgotten As a New Challenge of Human Rights: Analysing its Functioning in the Personal Data Protection

Zihan Yan

E.MA MASTER'S DEGREE IN HUMAN RIGHTS AND DEMOCRATISATION

Academic year 2012-2013

SUPERVISED BY

KOEN LEMMENS

Katholieke Universiteit Leuven

Acknowledgement

I would like to express my gratitude to my supervisor, Professor Koen Lemmens, who is Director of the E.MA programme for Katholieke Universiteit Leuven helped me carry out the research. I take immense pleasure in thanking Michaël Merrigan, teaching assistant at the KUleuven Institute for Human Rights and Critical Studies and the whole staff of Faculty of Law in KUleuven which hosted me during the second semester. Without their help this research would not have been possible. Finally, I wish to express thanks to the whole E.MA staff and masterini crew for the wonderful year together.

Abstract:

Rapid technological developments have brought new challenges for the protection of personal data. The right to be forgotten as an element of personal data protection has been debated hotly and controversially for the past few years, especially in Europe. The scale of data sharing and collecting has made personal information publicly and globally available, therefore it is necessary to provide a legal mechanism to persons to remove their personal data from online databases.

This thesis seeks to address how important the right to be forgotten will be as a new human right to protect personal data information in the digital age. The right to be forgotten needs better definition to avoid negative consequences since it is not very clear yet. Individuals should have the right to control over their personal information and remove it effectively after a certain time elapsed. Among the development of this right, there is an emerging dispute between European countries and United States, it is discussed in conflict with the right to freedom of expression. In such an information age, the criticism of the right to be forgotten also focus on internet environment in particular. Hence it is a urgent problem that how to implement the right to be forgotten in practice, both legal framework and technical measures should be taken into consideration. Furthermore, in order to improve its efficient function in society and create a more friendly online environment, we need to find sufficient and possible methods both from legal view and technical view to balance the public interests and personal privacy on the application of the right to be forgotten.

Acronyms:

AEPD	*Agencia Española de Protección de Datos* (Spanish Data Protection Agency)
BDSG	*Bundesdatenschutzgesetz* (Federal Data Protection Act)
CNIL	*Commission nationale de l'informatique et des libertés* (French Data Protection Agency)
DNT	Do Not Track
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
ENISA	European Network and Information Security Agency
EU	European Union
HTTP	Hyper Text Transport Protocol
TFEU	Treaty on the Functioning of the European Union
US	United States of America

Table of Contents:

Introduction:

The right to be forgotten belong to the most intimate sphere of individual's life. It is a form of privacy right. In recent years, a number of people have realised the challenges of collecting, storing and using personal information in light of technology. Recent developments in the European Union (EU) which have highlighted the potential challenges for the development of a "right to be forgotten". Because if you posted your information on the Internet, it becomes very hard to truly erase that information from Internet, the right to be forgotten represents an urgent problem in the digital age.

The Directive 95/46/EC,[1] was a milestone in the data protection history and currently it is a central legislative instrument for the protection of personal data in Europe. The right to be forgotten in the context of digital memory and data retention was only recently proposed as a fundamental right. In November 2010, the EU Commission took up the idea of introducing a right to be forgotten in the context of the ongoing revision of the Data Protection Directive 95/46/EC.[2] There was a reform for the EU's data protection rules which included the right to be forgotten in the proposed Regulation published by the European Commission in January 2012. It has created a new legal framework on the right to be forgotten gradually. Additionally, some Member States are building some mechanisms to implement the personal data protection in practice.

However, European Union and United States of America (US) have diametrically opposed approaches on the application of the right to be forgotten. In Europe, the roots

---

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 Octorbor 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

[2] European Commission, 'A Comprehensive Approach on Personal Data Protection in the European Union' (Communication) COM (2010) 609 final, 4 November 2010.

of the right to be forgotten can be found in French law, which recognises *le droit à l'oubli* or the "*right of oblivion*". It is a right that allows a convicted criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction and incarceration. In US, they have opposite views, many US experts and commentators accused EU regulator of "foggy thinking".[3] They insisted the fundamental US values, they think the right to be forgotten violate other rights, such as the right to freedom of expression and free speech.

As a new fundamental right, there is no clear interpretation about how the right to be forgotten could actually be enforced or how the deletion could be done in practice so far. Numerous possible legal and technological limits must be taken into account in this situation. Enforcement must depend on a combination of technical and international legal provisions. The European framework has already offered quite a comprehensive protection, but looking at the future, it is important to focus on enhancing the effectiveness of the existing framework in practice, to balance the personal data privacy and public interests. The main objective should always be to give individuals a balanced control over their personal data. An adequate implementation of the 'right to be forgotten' will make contributions to personal data protection system, and to the benefit of individuals in the information society have a friendly privacy system in the future.

Outline

This paper has been organised in the following way. While the Chapter one at hand meant to describe the definition of the proposed new right to be forgotten, include the background, the scope of the right and try to distinguish the difference between the right

[3] Fleischer, Foggy thinking about the Right to Oblivion, 9 March 2011, available at http://peterfleischer.blogspot.be/2011/03/foggy-thinking-about-right-to-oblivion.html (consulted on 28 March 2013).

to be forgotten and *droit à l'oubli* (the right to forget). In Chapter two, I will identify the right to be forgotten as an expression of right to privacy from a human right perspective. In Chapter three, I will look at the legal framework which protect personal information in international, regional level and national level. In Chapter four, it seeks to address that how conflicting opinions between EU and US on the right to be forgotten and criticisms which focus on challenges of the righ to freedom of expression and internet environment. In Chapter five, I will discuss what difficult practical implementation arising from legal and technical view. In Chapter six, I will explain what the mitigative and feasible measures to implement the right to be forgotten to protect the personal data privacy at present. I will conclude with Chapter seven in which I will anticipate the future of friendly online privacy system to promote data protection during the information age.

Research Questions and Methodology

The EU countries have a long history on personal data protection and privacy rights. Recent developments in the field of information-based society have led to an increasing interest in the right to be forgotten. Even though, European countries have played a key role in privacy area, such a new right need to be explained and evaluated on the basis of proper data protection framework. Insofar, the right to be forgotten need to be evolved both in theoretical and practical aspects. Hence this thesis seeks to deal with the following research questions:

How does the right to be forgotten as a new proposed fundamental right play the role of protect personal data privacy? What the dilemmas does it face to during the proceeding of implementation?

Methodology

This thesis will mainly use legal methods, literature researches, case studies and official documents in order to clarify the content of the right to be forgotten in present proposed Regulation and practical difficulties. Accordingly try to find expectations and recommendations to promote and improve the development of the right to be forgotten.

At the primary stage of the research I will focus on legal documents, which comprise publications, reports, international and domestic framework etc. Comparing with regional process and national experience on personal data protection, focus on EU data protection system particular and take cases which in EU jurisprudence for examples to talk about the necessity of introducing this new right. Then I will use standpoints which are from scholars, universities and authoritative organisations on the data protection. Concerning contrary opinions, I will lead in comparative method to account for today situations in different nations on the right to be forgotten. In addition, some relevant advocate and criticism materials can be found in websites are useful to address this issue.

1. Definition:

To understand the new proposed right to be forgotten, it is important and necessary to first go through the definition of this right in the current debate, to know the background of this right and the meaning of the conception on the right to be forgotten. Furthermore, distinguish the right to be forgotten from the other similar right to forget, in order to realise the development of the right to privacy during the process.

1.1 Background

The data protection is based upon the understanding of the right to privacy, at a word that "*knowledge about me is my property"*.[4] One hundred years ago, Louis Brandeis, an American lawyer and Associate Justice on the Supreme Court of the US stated the famous sentence: "*Publicity is justly commended as a remedy for social and industrial deceases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.*"[5] In 1890, Louis Brandeis together with Samuel Warren, a Boston attorney addressed the right to privacy in their famous law review article "The Right to Privacy".[6] They are the first people to propose the right to privacy. The conception in their words was created to protect the confidentiality of an individual,[7] in particular, mostly the right to privacy was understood as the "*right to be let alone*".[8] They exemplified that a common law of the right to privacy exist that guarantee individuals have right to determine, include their thoughts, feelings, perceptions.[9]

---

[4] Ramsay H., 2010, p. 288.

[5] Louis D., 1914, p.92.

[6] Samuel D. &/Louis D., 1890, pp.193-220.

[7] Solove & Rotenberg & Schwartz, 2006, p.11.

[8] Olmstead v United States, 277 US 438, 478 (1928)

[9] Ibidem footnote 3, p. 198.

Originally, this right focuses on commercial matters, business methods generally, and also on governmental actions.[10] Some years later, Brandeis referred in an opposite opinion that subtler and far-reaching methods have become available to invade personal privacy.[11]

However, the general legal perspective of Warren and Brandeis did not lead to legislative actions immediately. At that time, the meaning of data protection did not include the right to be forgotten, it was mainly directed against data collections which were undertaken by governmental agencies and large corporations.[12] Only after the Second World War and the first economic recovery in Europe, the national governments began to realise that data protection issues must be taken into account. Then the personal data protection was gaining recognition by countries and the government began to lay down laws to ensure the protection of personal data.[13]

From the historical development view of the right to privacy, along with data protection laws have developed over the last 50 years, lack of precise laws on the autonomy of the individual on their personal data will make individuals are short of management of their data. Hence the security of information access has become an obvious issue, people noticed that the privacy protection should be improved with the time changes.[14] The existing laws or regulations are not enough to protect individual privacy rights on the area of personal data. Consequently, in this circumstance, it is necessary to bring in the proposed implementation of a new right to be forgotten. The recent process on this right is assessed by European Commission, in a communication on "A comprehensive approach on personal data protection in the European Union", the Commission clarified that considering the rapid technological developments, bringing

---

[10] Kaufmann & Weber, 2010, p. 779.

[11] Gindin, 1997, pp. 1153-1154.

[12] Richards, 2010, pp. 1295-1296.

[13] Whitman, 2004, pp.1151-1194.

[14] Xanthoulis, 2013. p. 86.

more challenges for protection of personal data.[15] In the movement, the scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal data on an unparalleled scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Therefore, EU needs a more comprehensive and coherent policy on the fundamental right to personal data protection.[16] In order to strengthen the individual's control over their personal data and guarantee the free movement of personal data, it is time to build a much stronger and more consistent personal data protection framework in the EU. One of the subjects is to introduce a right to be forgotten to put individuals in control of their personal data. In Commission's point of view, the right in attempt to be identified as "to ensure that when an individual do not want their personal data to be processed any more, and if there is no legitimate reason for keeping it, it should be removed"[17]

1.2 The Scope Of the Right to Be Forgotten

To address this new rising fundamental human rights, the right to be forgotten, primordially must take the three primary groups of actors who are implicated by the right to be forgotten into account: data subjects, data controllers, and third-party websites.[18] The first group includes people who are the subjects of data posted, stored, or collected online. The second group is content creators, which covers persons who post data online that qualifies as protected speech, such as blog posts, pictures on

---

[15] Ibidem footnote 2.

[16] European Commission, 'A Comprehensive Approach on Personal Data Protection in the European Union' (Communication) COM (2010) 609 final, 4 November 2010.

[17] Reding, "EU data protection reform and social media: Encouraging Citizens' Trust and Creating New Opportunities Economist conference "New frontiers for Social Media Marketing" Paris, Tuesday 29 November 2011, available at http://europa.eu/rapid/press-release_SPEECH-11-827_en.htm (consulted on 20 March 2013).

[18] Conley, 2010, p. 53.

Facebook, videos on YouTube, product comments in online stores, etc. The third category contains websites that display or link to material created by others, like search engines and aggregators.

In a speech in Paris on 25 November 2010, Neelie Kroes, European Commission Vice-President and EU Commissioner for the Digital Agenda, expressed herself to support a "right to be forgotten" as follows: "In my view, the issue is not merely about deleting all data. Just like in real life, when you present yourself on the net, you cannot assume no records exist of your past actions. What matters is that in those cases any data records are made irreversibly anonymous before further use is made of them."[19]

Subsequently, Vivian Reding, the European Commissioner for Justice, Fundamental Rights, and Citizenship, in favor of the new privacy right. She proposed the European Parliament to adopt this right as a European Union-wide regulation.[20] On 25th January, 2012, the European Commission issued legislative proposals for data protection. One of the proposals is 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), which includes a right to be forgotten extending to the personal data of all persons. It is a most authoritative document for the right to be forgotten. In the first place, in Article 17 of proposed Regulation articulated that four situations of the data subjects 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."[21] "(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise

[19] Gridnev, Security & Resilience in Governmental Clouds: Making an informed decision-(OT European Network and Information Security Agency), January, 2011, available at http://www.slideshare.net/gridnev/security-resilienceingovernmentalcloudsenisa (consulted on 27, Febuary, 2013).

[20] Kuner, 2012, p.1.

[21] European Commission, 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final, 2012.

processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) (data subject has give consent to the processing of their personal data), 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 (right to object); (d) the processing of the data does not comply with this Regulation for other reasons." Therefore, in a nutshell, the right can be invoked when (a) the data is no need for existed; (b) consent is withdrawn or the storage period has expired; (c) data subjects object to disseminate data; (d) the reason for processing of data does not comply with this Regulation.

In the second place, the proposed Regulation gives a right to data subjects to delete their data when the data controller referred to above mentioned has made the personal data public. At the meantime, the data controller shall take " all reasonable steps " to inform third parties which are processing such data and erase any links or copy or replication of that personal data according to the data subject requests.[22] Therefore, the data controller is responsible for the publication of third parties. From the provision, the data controllers' obligation to notify the third parties includes three elements: First of all, just because of the data controller made the personal data public, if it is not the data controllers who made the data public, they will not be responsible; Second of all, the data controller is obliged to inform only that third parties who process the data. Finally, the data controller shall take " all reasonable steps", but not " all steps".[23]

In the third place, the limitations are provided for the right to be forgotten in the proposed Regulation. Upon request, website operators are required to "carry out the erasure without delay",[24] but there are some limitations, firstly, the retention of data is

---

[22] Ibidem art 17(2).

[23] Smętek & Warso, 'The right to be forgotten-step in the right direction?' Helsinki Foundation for Human Rights, 22 Octorber 2012, available at http://www.europapraw.org/en/policy-papers/policy-paper-prawo-do-bycia-zapomnianym-wzmocnienie-autonomii-informacyjnej-czy-wprowadzenie-cenzury-w-internecie (consulted on 29 May 2013).

[24] Reding, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data

"necessary" for exercising "the right of freedom of expression", secondly, for reason of "public interest in the area of public health", thirdly, "for historical, statistical and scientific research purposes" and fourthly "for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject".[25] In addition, although the controllers have to restrict the processing of it, personal data can also be retained when (a) their accuracy is contested by the data subject; (b) for purposes of proof; (c) the data subject opposes the erasure and request to restrict use of the data instead; and (d) for data portability purposes.[26] Although the applications of all these limitations are not clear, they draw a basic-bounded line for the deleted information and retained information. It is necessary to balance the right to be forgotten with other fundamental rights.

The European Data Protection Supervisor (EDPS) welcomed the proposal and considered that the right to be forgotten could be proved very useful in the context of information society services. "An obligation to delete or not further disseminate information after a fixed period of time makes sense especially in the media or the internet, and notably in social networks".[27] The opinion of EDPS is that the right to be forgotten is a useful conception. It could be worthwhile to include them in the legal instrument, but probably for the electronic environment, it would be not effective.

From the short overview, it showed that EU commissioners Kroes and Reding have different views on this right. While Kroes stresses the point that because it is not realistic, the right to be forgotten is not about deleting all data, but about making them irreversibly anonymous. Reding puts central the right to withdraw consent for further processing of data and the obligation of the processor to prove the need to keep data

---

Protection Rules in the Digital Age Innovation Conference Digital, Life, Design, 24 January 2012, available at http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm (consulted on 31 March 2013).

[25] Ibidem footnote 21 art. 17(3).

[26] Ibidem art. 17 4.5.

[27] Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — 'A comprehensive approach on personal data protection in the European Union', OJ C181/01

rather than deleting it. However, for the EDPS, the passive role of the person concerned and the obligation of the data processor to delete data on his own initiative seems to be the core of the right to be forgotten.[28] These different opinions did not produce a substantial contribution to what the exactly scope is and presented vagueness of the proposed right, however, at least, it formulates the essential range for the right to be forgotten primordially.

1.3 The Right to Be Forgotten and the Right to Forget

There are some difference between the right to be forgotten and the similar term "*the right to forget*" (*droit à l'oubli*). The term right to be forgotten has been created just recently, but "the right to forget", which also called the right to oblivion was already debated a decade ago.[29] They are not identical, the right to be forgotten should not be confused with the right to forget as happens frequently in discussions: The "right to forget" refers to the already intensively reflected situation that a historical event should no longer be recovered as the time goes by since its occurrence, it is the right for individuals and nations to forget their past. The right to be forgotten reflects that an individual have a right to request certain data be deleted so that third persons can no longer trace them.[30] Therefore, the right to be forgotten is based on the autonomy of an individual becoming a rightholder in respect of personal information, the longer the origin of the information goes back, the more likely personal interests prevail over public interests.

In the context of digital age, the internet handles a number of personal information, this information is easy to disclose, disseminate, share, download and repost in various ways. To distinguish the "right to forget" and the right to be forgotten, it is necessary to

[28] Nys, 2011, p.471.
[29] Streich, 2002, p. 525.
[30] Weber, 2011, p.120.

examine internet privacy, which is important to address the two rights. The meaning of privacy in the internet situation is not to be just regard as 'intimacy' or 'secrecy', the concept should be understood more broadly and refer to the dimension of privacy, this dimension can be considered as information automony or information self-determination.[31] From this view, it means the individuals have autonomy to control over their information online. Informational self-determination means individuals have right to control over their personal information, to decide which information about themselves will be disclosed, to whom and for what purpose. The informational self-determination has been recognised as a right of personal data protection in Europe.[32] It represents the information automony or informational self-determination attempt to change personal information from public to private area.[33]

It may become confusedly and faintly if the two rights do not be distinguished. The former one, the right to forget is based on protection against violate to dignity, personality reputation and identity, it used to apply in the cases related to individual who has served a criminal sentence and wishes to no longer be linked to the criminal actions. It is a right to protect individual to leave from his criminal past and prevent the public from accessing their past information which may have an effect on their present lives. The latter one, the right to be forgotten is a right that providing erasure of information when individual ask for deletion.[34] In such a context, it is unclear on the right to be forgotten in the proposed Reguation, in the literature of Meg Ambrose and Jef Ausloos, the authors explain that a more accurate description for the right to be forgotten would be a "right to erasure". They maintain that more research have the right to erasure will support for the less clear concept of the right to be forgotten.[35] By comparing two rights, as can be seen obviously the right to be forgotten has been

[31] Ausloos, 2012, p.144.
[32] Terwangne, 2012, p.109.
[33] Rouvroy & Poullet, 2009, p.45.
[34] Ibidem footnote 30.
[35] Ambrose & Ausloos, 2013, p.14.

evolved, it includes both deletion and oblivion, it can get more control over personal information, that means this right will entrust more protection to individuals' privacy.

According to the Center for Democracy and Technology, the difference between oblivion and be forgotten is "passive or transactional data sharing when a service collects and uses personal data in the context of a commercial transaction, active or expressive data sharing when content is authored or disseminated by users themselves."[36] Time factor is the significant aspect that distinguish the two rights. A right to oblivion means if oblivion, it will not allow to access the information as time goes on, however, the right to be forgotten do not necessarily include the time element, it related to the consent of individuals, individual has right to withdraw their consent to the processing of their personal data at any time. According to the distinction aforementioned, the separation of two rights depend on whether the information has been disclosed to the public or individual give consent to delete it. The right to forget is based on information privacy as a personality, identity and self-determination as the "search engine society" phenomenon.[37] The right to be forgotten is based on information privacy as a control method, it intend to get efficiently control over the personal data in such information era.[38] But unquestionable, both of the two rights have an influence on the present information society, whereas they can not be merged or treated similarity.

---

[36] Center for Democracy & Technology, Comments to the European Commission in the Matter of Consultation on the Commission's Comprehensive Approach on Personal Data Protection in the European Union, 15 January 2011, available at https://www.cdt.org/files/pdfs/CDT_DPD_Comments.pdf (consulted on 1 March 2013).

[37] Halavais, 2009, p. 221.

[38] Ibidem footnote 35, p.1.

2. The Right to Be Forgotten from Human Rights Perspective

Through analysing the new right to be forgotten, it is always proposed as a right.[39] It is discussed by some methods through laws, regulations or other managing mechanisms. However, there are some other opinions of this point, because being forgotten is presented as a natural functioning of the human brain,[40] it is also addressed by other scholars that this right can be seen as an ethical, virtue, social value, interest worthy of protection or a policy goal.[41] For example, from Rouvroy's point of view, she has a formulation of "a 'right ' or rather a 'legitimate interest to forget and to be forgotten'".[42] This means not just the forgetfullness from psychologically, but also has social and legal intrusions. In this paper I will emphasis on the right to be forgotten as a legal right. Thus on grounds of the right to privacy, the right to be forgotten could be treated as a human right to protect personal information.

2.1 The Right to Be Forgotten as a Right

The actual difference between rights and just individual's interests is based on the content and its obligations.[43] Griffin argued that to some extent, a right must bear duties, otherwise it would not be a right.[44] In other words, if we want to bring the right to be forgotten in this area, the main point is whether the right to be forgotten protects individual interests and create obligations to make sure this right take effect. In spite of the broad definition of the right to be forgotten in this information world, one thing the

---

[39] Ibidem footnote 11 and 12, p. 8.
[40] Blanchette & D.G., 2002, p. 33.
[41] Mayer-Schönberger, 2009, pp. 16-50.
[42] A Rouvroy, Forgetting Footprints, Shunning Shadows. A Critical Analysis of The "Right To Be Forgotten" In Big Data Practice, 24 December 2011, available at http://script-ed.org/?p=43 (consulted on 15 February 2013).
[43] Gtiffin, 2008, p.97.
[44] Cranston M., 1983, pp.1-17.

proposed right aims by principle to grant an individual control, not only for that data which related to negative past events, but also individuals' digital footprints and data shadows. The digital footprints mean data subjects themselves leave behind, data shadows mean the information related to them which generated by others.[45]

In fact, the right to be forgotten related to personal data protection, it is built on the right to a private life. In current society, with high speed development of information, we have more and more concerned about losses of our privacy. In EU level, it formulates the relationship between data protection and the right to privacy. "where as data-processing systems are designed to serve man; where as they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals"[46]

2.2 The Right to Be Forgotten as a Form of Right to Privacy

In essence, the right to be forgotten is a consequent element of right to privacy. The right to privacy has a multi-dimensional conception, several authors have discussed that privacy should be regarded as a "cluster concept".[47] According to Lisa Austin, she exemplified that "technology creates privacy issues that appear to fall outside the bounds of our traditional concerns regarding privacy in order to respond to these new situation."[48] As a result, a multi-dimensional approach is arising.

There are five forms of privacy analysed by Hayden Ramsay lately. The first privacy element is not only individuals could control over the flow of their information, and also extend to the risk of invasion of privacy. The second privacy element refers to the

---

[45] M Dodge & R Kitchin, 2007, p. 431.
[46] Ibidem footnote 1.
[47] Hugl U.,2010, p. 120.
[48] Austin, 2003, p.164.

freedom from interference and violation. The third one is the basis of the moral good to respect the value of persons and maintain people from infringement. The fourth privacy element comprises the point which provided by Warren and Brandeis. The fifth privacy element can be defined as keep personal life secret, asking for safety from observation and invasion.[49] In view of many elements are included in the privacy, requiring data protection take these elements into consideration and create a full-scale conception.[50] Such a "cluster concept" includes the information, access and expressions, these three aspects need to be combined. Informational privacy refers to control over information, accessibility privacy focuses on central observations, and expressive privacy protects a realm for expressing one's self-identity.[51]

Having addressed how privacy can be regarded as a multi-dimensional concept, in consideration of a new "right to be forgotten," the relevant aspects of this cluster need to be identified, analysed, and condensed into a rights structure. Bert-Jaap Koops identified three perspectives of the right to be forgotten in his literature paper. The first stressing that personal data should be deleted in due time. Secondly, it is " clean slate", also called Fresh Slate, which means the outdated negative information should not be used against people. Thirdly, people should without fear of future consequences and not be restrained of expressing themselves anywhere, it means that the right to only be connected to current information.[52] These three aspects of the right to be forgotten are conceived by Koops are complementary which fall under the multi-dimensional of the right to privacy that talked above.

The first approach refer to the proposed right which focus on restrict informational access of the third parties to certain personal information. It falls under the information dimension and constitutes one of the dimensions of the right to privacy. The second

---

[49] Ramsay, 2010, pp. 288-297.
[50] Hugl, 2010, p. 4.
[51] Ibidem.
[52] Koops, 2011, p.254.

point refers to protect an individual's freedom to determine his social relationships with the third parties, it falls under the social dimension of the privacy. And the third perspective is linked to individual self-development and personal identity protection, it subjects to guarantee individual autonomy and dignity, it fall under both psychological dimension and social dimension of privacy.[53] Having discussed the right to privacy has a multi-dimension, the right to be forgotten aims to protect individuals' interests and value, it can be considered that this right against the threat of personal interests or value.[54] In this way it should be regarded as a human right request.

To sum up, in term of present research what we have, it proves that the right to be forgotten can be put in the broad understanding of the right to privacy, it is a form of the multi-dimension right to privacy and also a human right. From this human rights based approach, it is useful to develop this right, such as to further define the scope, the limitation and the implementation challenges of this right.

[53] Ibidem, p. 253.
[54] Gordon & Gemmell, 2009, pp. 14-46.

3. Legal Framework

Overview, as such a new fundamental human right, the right to be forgotten need to evolve on the basis of appropriate framework, the most important support is depend on the legal protection framework. In this section, it seeks to address the legal framework in the regional level and domestic level, although there is no clause regulate the right to be forgotten in current law directly, we can find the roots and sources in International documents, also the national practices have the strong support to bring the right to be forgotten into legislative purpose.

3.1 International and Regional Framework

The protection of personal data has developed over decades, especially in European level, the EU played a leading role in building more comprehensive and specific framework to the Member States.

The right to personal data protection is established by Article 8 of the Charter of Fundamental rights of the EU, which the Lisbon Treaty turned into a binding instrument, not only for the EU institutions and bodies, but also for the Member States when implementing Union law. It enshrines protection of personal data as a fundamental right. In this Article, it sets that data must be processed fairly for specified purposes and based on the consent of the person or legitimate reasons. And everyone has the right of access to their data and rectified.[55] The Lisbon Treaty also created a horizontal basis for rules on data protection in all EU policies in Article 16 Treaty on the Functioning of the European Union (TFEU). In Article 16(1) of TFEU, it establishes the principle that everyone has the right to protect their personal data which relating him or her. Moreover,

[55] Charter of Fundamental Rights of the European Union (adopted 7 December 2000, entered into force 1 December 2009) art 8.

with Article 16(2) of TFEU, the Lisbon Treaty introduced a specific legal basis for the adoption of rules on the protection of personal data.[56] This provision is also the basis for the current reform of the EU legal framework for data protection.

Furthermore, the Council of Europe played a pioneering role in formulating the basic concepts and principles of data protection in European Convention on Human Rights (ECHR) in 1981, which since then has been ratified by more than 40 European countries, including all EU Member States. In Article 8 of the ECHR, it formulates that 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."[57] It is also one of the legal basis for the current reform of the EU legal framework for personal data protection.

Currently, the center point of the existing EU legislation on data protection is 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.[58] This current Data Protection Directive has two objectives in mind. Firstly, to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States. Secondly, it was complemented by Framework Decision 2008/977/JHA as a general instrument at Union level for the protection of personal data in the areas of police co-operation and judicial co-operation in criminal matters.[59] In Article 1(1) of Directive 95/46/EC which provides the aim of this Directive is Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to privacy with respect of the processing of personal data.

---

[56] The Treaty on the Functioning of the European Union (Treaty of Rome, as amended)

[57] European Convention on Human Rights (adopted 4 November 1950, entered into force 3 September 1953)

[58] Ibidem footnote 1.

[59] 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 [2008] OJ L350/60

The 95/46/EC Directive has already given EU citizens certain rights control over their data. Organisations can process data only with consent, and only to the extent that they need to fulfil some legitimate purposes. Although the current Directive does not provide for a detailed or general concept of "the right to be forgotten", it can be regarded as the root and inspiration for the right to be forgotten, some existing provisions can be interpreted as implied the right to be forgotten.[60] For example, in Article 6(1)(e) of the Directive, narrates that personal data can be kept "for no longer than is necessary for the purposes for which the data were collected or for which they are further processed." Moreover, the consent elements in Article 7 declares the situations that when personal data can be processed. The Article 29 is about the opinion on consent of Working Party, it has emphasised that individuals should always be allowed to withdraw their consent. The most relevant provisions refer to the right to be forgotten is Article 12(b) and Article 14 in the current Directive. In Article 12(b) it analyses the limit of apply for this right"when the processing does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data."[61] In Article 14, it provides that the data subjects have the right to object to the processing of personal data relating to them, but also states some limitaions. "object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data".[62]

As clarified by the Court of Justice of the European Union (ECJ), the evolution on the right to personal data protection must be considered in relation to its function in

---

[60] Smętek & Warso, 'The right to be forgotten-step in the right direction?' Helsinki Foundation for Human Rights, 22 Octorber 2012, available at http://www.europapraw.org/en/policy-papers/policy-paper-prawo-do-bycia-zapomnianym-wzmocnienie-autonomii-informacyjnej-czy-wprowadzenie-cenzury-w-internecie (consulted on 29 May 2013).

[61] Ibidem footnote 1.

[62] Ibidem.

society.[63] Therefore, under this situation, the proposed Regulation go further than the 95/46/EC Directive, it reflects the tendency of 95/46/EC Directive. Because from the objectives of current Directive, it can be divided into two main contents. On the one hand is try to strengthen the individual's control over their personal data. And on the other hand is try to provide legal certainty and to minimize administrative burdens for businesses. One of the methods to gain the first objective is to introduce a "right to be forgotten" into the proposal.

From the new proposed Regulation, in the EU level, it is considered to be the most adequate legal instrument to define the framework for the the right to be forgotten. At least it has two progresses on personal data protection. Firstly, it reinforces the protection of the data subject. In Article 79 c (5), it gives each supervisory authority power to conduct administrative sanctions. If the data controllers intentionally or negligently do not abide by the right to be forgotten or do not take all necessary steps to inform third parties that a data subjects request to erase their personal information which regulates in Aricle 17, the supervisory authority should impose a fine up to 500,000 Euro, or an enterprise up to 1% of its annual worldwide turnover.[64] This referral of administrative sanctions would make the enforcement of the right to be forgotten more realisable by urge the data controllers to comply with the rules laid down in the proposed Regulation.

Secondly, it is a further step of legislation on personal data protection to guide the existence of a great deal of different national systems to the right direction.[65] In Article 288 of TFEU, it formulates that "A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States."[66] Hence in accordance with this article, the direct applicability of a Regulation will reduce legal

---

[63] European Commission, Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century. COM (2012) 9 final.
[64] Ibidem footnote 21, art. 79 c (5).
[65] Ibidem footnote 23.
[66] Ibidem footnote 56, art. 288.

fragmentation and provide much greater legal certainty by introducing a harmonised set of core rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the internal market. Not just limited to the level of Member States, the proposed EU legislative actions hope to be more effective than similar actions at the level of Member States. This proposal is also a basis to reduce the current diversity and complexity of data protection law, mainly due to the implementation of one legal framework into different national versions of the such same concepts and principles. The Commission's proposal for a directly binding Regulation is the appropriate answer to make the present legal safeguards on the right to be forgotten more effective in practice.[67]

3.2 Domestic Framework

When referring the right to be forgotten, EU is always more active. Many countries in Europe reflect that they agree with this right and have taken actions to prove that they are exercising this right to be forgotten in national level. I will take France and Germany for examples to give an account of the development of the right to be forgotten in domestic framework.

France

Among European countries, as the first country to provide *"droit à l'oubli",* France has a non-ignorable standard on this issue. It represents the historical origin of this

[67] European Economic and Social Committee Conference " Towards a more responsible use of the internet-The European civil society perspective" 6 March 2013, available at http://www.eesc.europa.eu/?i=portal.en.events-and-activities-internet-responsible-use (consulted on 30 March 2013).

concept in the late 1970s from the French *le droit à l'oublie*.[68] However the*"droit à l'oubli"* did not have a proper English translation, in most cases, it is translated into the right to oblivion, someone translate it as the right to forget, the right to delete, the right to erase etc.[69]

In France, it introduced a legislation called "*un chartier sur le droit a l'oubli*", it is a charter on *droit à l'oubli,*[70] which intends to implement to "*droit à l'oubli*".[71] In Octorber 2010, several internet companies except two major internet companies Google and Facebook, subscribeb together with the French government a Charter *«Droit à l'oubli dans les sites collaboratifs et les moteurs de recherche».* The aim of the Charter is to improve transparency of the personal information, protect the minors online privacy and promote the implementation of "*droit à l'oubli.* This reflects an important foundation for the approbation of the right to be forgotten.[72] Based on the French experience, it is a good example for European Commission to find ways to do their utmost to exercise the right to be forgotten effectively.

In 2010, a first legislative project was developed in France that envisaged the creation of a "right to be forgotten" online to secure the right to be forgotten on the Internet. [73] The initiative was taken by the French State Secretary for the digital agenda, Nathalie Kosciusko-Morizet. It is remarkable and should not be overlooked as it may have important consequences for the development of the right to be forgotten in France.[74] The project was completed and resulted in the adoption of two codes of good practice. First is Code of Good practice on Targeted Advertising and the Protection of

---

[68] Ibidem footnote 29.
[69] Ibidem footnote 3.
[70] Miller, We May Not Have a 'Right to Be Forgotten' Online, 14 March 2011, available at http://www.internetevolution.com/author.asp?section_id=1047&doc_id=204757 (consulted on 20 March 2013).
[71] Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure numérique, Novembre 2009.
[72] BEUC, 'A Comprehensive Approach on Personal Data Protection in the European Union' European Commission's Communication, 2011.
[73] Charte du droit à l'oubli numérique dans les sites collaboratifs et les moteurs de recherche, 13 October 2010.
[74] Bril NV., 2011,p. 469.

Internet Users.[75] In this Code, it includes eight recommendations refer to reinforce data protection and Internet users' rights, especially the Code intends to limit the retention of cookies for the purposes of behavioral advertising. The other is Code of Good Practice on the Right to Be Forgotten on Social Networks and Search Engines.[76] The Code attempt to protect Internet users's right to control over their data when it is posted online and request the network companies have responsibility to give Internet users prior inform of processing or using their data. The French approach is trying to educate Internet users about the risks of their privacy, at the meantime, it develops more enhanced way to cultivate the right to be forgotten and personal data protection at national level.[77]

In recent years, internet legislation seems to be a hot topic in France, France has transposed the 95/46/EC Directive to national law,[78] and a proposed law about creating an online "right to be forgotten " will play an important role on regulate network order. The right to be forgotten intends to push forward online and mobile companies to dispose of E-mails and text messages after an agreed upon length of time or on the request of the person concerned.[79] Under the European context, the proposed French law put the right to be forgotten which in proposed EU Regulation into reality. It built a bridge to connect EU law with national law.

The French Data Protection Agency, the *Commission nationale de l'informatique et des libertés* (CNIL), which is an independent French administrative authority that refer

---

[75]CHARTE SUR LA PUBLICITE CIBLEE ET LA PROTECTION DES INTERNAUTES, http://www.huntonfiles.com/files/webupload/PrivacyLaw_Charte_publicite.pdf

[76] CHARTE DU DROIT A L'OUBLI DANS LES SITES COLLABORATIFS ET LES MOTEURS DE RECHERCHE, http://www.huntonfiles.com/files/webupload/PrivacyLaw_Charte_du_Droit.pdf

[77] Hunton & LLP, French Government Secures "Right to Be Forgotten" on the Internet, 21 October 2010, available at http://www.huntonprivacyblog.com/2010/10/articles/french-government-secures-right-to-be-forgotten-on-the-internet/ (consulted on 25 March 2013).

[78] European Commission, Thirteenth Annual Report of the Article 29 Working Party on Data Protection, 14 July 2010, No LX-46 01/190.

[79]Reid, France ponders right-to-forget law, 8 January 2010, available at http://news.bbc.co.uk/2/hi/programmes/click_online/8447742.stm (consulted on 28 March 2013).

to the data privacy and enacted into law on 6 January 1978.[80] The mission of the CNIL is to ensure the data privacy law is applied to the collection, storage and use of personal data.[81] The CNIL recognises that the proposed regulation provides substantial improvements that were excepted and necessary. They welcome the proposed EU regulation on data protection and claimed they will pursue its efforts to ensure the draft regulation are reflected in the final EU regulation. At the same time, CNIL noticed that the proposed regulation is not consummate, the risks between European citizens and their national authorities will not ensure an effective implementation of the right in practice.[82] Thereby, the CNIL industriously through numerous to establish a legal framework for the right to be forgotten and also CNIL declared that they will continue to promote the right to be forgotten is read-in their obligations.[83]

Lately, on 30th May 2013, the CNIL launched a public consultation on the right to be forgotten, on the CNIL's website it says, " The draft European Regulation would establish the principle of a digital 'right to be forgotten' which would allow us to better control our online life…In this context, the CNIL has launched an online consultation about this right, which is often cited but whose contours remain unclear. In parallel, the CNIL also will consult professionals concerned with this issue."[84] The CNIL proposed some questions to let individuals choose to answer, the result of the public consultation will be published on the CNIL's website. By this means, I think it is a good way for authority to know how the community think about this right, get more communication

---

[80] CNIL, available at http://www.cnil.fr/english/ (consulted on 30 March 2013).
[81] CNIL, Mission and Power, available at http://www.cnil.fr/english/the-cnil/operation/ (consulted on 1 April 2013).
[82] CNIL, Draft EU Regulation on data protection: the defense of data protection driven apart from citizens, 31 January 2012, available at http://www.cnil.fr/linstitution/actualite/article/article/draft-eu-regulation-on-data-protection-the-defense-of-data-protection-driven-apart-from-citizens/ (consulted on 2 April 2013).
[83] CNIL, CNIL satisfied with draft European Parliament report on the Regulation proposed by the European Commission, 16 January 2013, available at http://www.cnil.fr/english/news-and-events/news/article/cnil-satisfied-with-draft-european-parliament-report-on-the-regulation-proposed-by-the-european-comm/ (consulted on 30 March 2013).
[84] The Privacy & Information Security Committee, French DPA Launches Public Consultation on Right to Be Forgotten, 10 June 2013, available at http://thesecuretimes.wordpress.com/2013/06/10/1137/ (consulted on 15 June 2013).

with individuals and will achieve more recognition from public.

Germany

At the beginning of the process of the right to be forgotten, even as a pioneer on issue of personal data protection, the German government against the proposed right to be forgotten.[85] German Interior Minister Friedrich argued that the current German law has already offered an excellent model for this, he does not want the proposed EU Regulation to apply to data processing which carried on by govermental authorities. He declared that he supported to the individuals self-regulate, trying to avoid the negative effect on themselves as much as possible and he thought the idea of the proposed right is mainly interested in expanding the European Commission's power.[86]

As media start to bring a number of data to online environment, the way in which individuals intend to control over the information has become diverse and contradictory. Therefore take a look at how recent developments of a right to be forgotten in Germany may affect other countries to carry on the data protection. In Germany, individuals who have been commit crimes, served their sentence and paid their debt, have right to get protection of their privacy. While the Internet may record their crimes, indicate their identities, show their offense. At that time, the media has the right to freedom of expression and public has the right to know. However, as time passes by, the online publisher who releases the information refer to individuals should delete such information. Basically speaking, the individuals obtain a right to be forgotten.[87]

In the past decades, German Courts have dealt with some cases about criminal

---

[85] US Government and Internet Giants Battle EU over Data Provacy Proposal, 17 Octorbor 2012, available at http://www.spiegel.de/international/business/us-government-and-internet-giants-battle-eu-over-data-privacy-proposal-a-861773.html (consulted on 25 April 2013).
[86] Ibidem.
[87] Siry & Schmitz, 2012, p. 1.

offenders after be executed or published, they sued the data controller to take down their information from internet or delete their full name that mentioned in the online archives. The most famous case is Wolfgang Werlé and Manfred Lauber.[88] They are two half-brothers, they were convicted of robbed and murdered Walter Sedlmayr, who is a famous actor in 1993. But the two defendants denied the accusations, afterwards, in 1999, they sued a constitutional complaint to Constitutional Court to against their convictions and want to overturned the situations. The Constitutional Court held their complaint and judge that their complaint to be not admissible. Then further applications for re-litigation was also unsuccessful. This case caused more public attention at that time. The offenders were known widely in Germany, and the news broadcast referring to the accused and always mentioned their full names which made the Wolfgang Werlé and Manfred Lauber more notable. With the development of the Internet, the news broadcasts is spreading into online environment. As the offenders were released on parole, they were worried about the news broadcast may have a side effect on their life, in order to prevent to be stigmatised, in 2007 they filed a lawsuit against website providers request to remove their full names from all articles which somehow connect them to the crimes that they had already served in prison. After a long time of litigation, the full names of two murders were deleted from news broadcast in German websites and German Wikipedia also removed their full names from the articles which refer to victim Sedlmayr. Nevertheless the two half-brothers also trying to remove their names from English-language version of Wikipedia is at question. Many legal professionals in US think that the action of Wikipedia is protected under the US constitution and the judgement of German Federal Court of Justice has no jurisdiction on US. Thereby they rejected to delete the murders' names.[89]

From the German case, it indicates that it is difficult to decide whose judgement has

---

[88] The "right to be forgotten," Germany, and the Wikimedia case, 4 February 2011, available at http://www.pogowasright.org/?p=20228 (consulted on 15 May 2013).
[89] Ibidem footnote 87, p. 4.

priority in US or EU countries. As the world is becoming smaller in the Internet environment, the interests is not only direct against domestic area, but also against non-domestic area. It will become more interconnected and universal, and more cooperation are needed. In that case, from the German standpoint, the right to be forgotten has been applied in society. This is a evidence to emphasise the right to be forgotten is an important way to protect indiviuals' privacy. From legal perspective, German has a law support on the personal data protection field. The main legal source of data protection in Germany is the Federal Data Protection Act (*Bundesdatenschutzgesetz*) (BDSG), which implements Directive 95/46/EC on data protection. In addition, in Germany, each state has a data protection law of its own.[90] In principle, the state's data protection acts aim to protect personal data from processing and use by public authorities of the states. The BDSG is aimed at protect personal data from disseminating and using unofficially by federal public authorities and private bodies. Personal data is regulated and includes any information concerning the personal circumstances of an identified or identifiable individual. In the Section 20 of the Federal Data Protecion Act,[91] It has a provision about rectification, erasure and blocking of data, right to object, it is similar as the right to be forgotten. It provides that data subjects can ask the data controller to rectify, complete, update, block or delete his personal data if it is sensitive, inaccurate, incomplete, ambiguous, expired, or its collection, usage, disclosure or storage is prohibited. Compare Article 20 in BDSG and Article 17 in proposed EU Regulation, we find a mainly difference between these similar provision. In the former one, it depicts that if the personal data processed in an unlawful way, it shall be erased. And also when the data accuracy can not be verified, it shall be blocked.[92] However, the difference in Article 17 is the data subjects have right to ask

---

[90] Ibidem footnote 85.

[91] Federal Data Protection Act (BDSG) adopted on 14 January 2003, entered into force on 1 September 2009 last amended by Article 1 of the Act on14 August 2009.

[92] Ibidem.

data controller to stop disseminating their information. It means even the data is correct, when the data subject withdraw the consent on the data, the data controller should remove such data in the light of data subjects' demands.

4. From Theory to Practice

The right to be forgotten is still in the forming stage, since the proposal does not clarify clearly how this right could be enforced, it is arising some problems when this right turn into practice. The most two obvious disputes are the US conflict with EU perspective on the right to be forgotten, and in this digital age where internet is very necessary, whereas also the uncertain right would face more challenges on the Internet environment.

4.1 EU and US Perspectives

Reding declared that once the proposed Regulation is promulgated, it will instantly become law throughout the EU, currently there is a safe harbor agreement in place, if EU withdraws from it, the European framework could be imposed on US companies doing business in Europe as well.[93] Since there are different privacy traditions and discussions between EU and US for long time, when Americans and Europeans speak of privacy, they are often talking about very different things.[94]

European privacy laws are primarily intended to safeguard an individual's dignity and public image, rather than to protect against governmental intrusions. In contrast, In the US, where privacy is normally couched in the language of liberty, public policy is primarily concerned with protecting a citizen's "reasonable expectations of privacy" against impermissible government intrusion.[95] This tradition shows that European Courts tend to be less preoccupied with protecting free speech rights from government

---

[93]The Economist, Private Data, Public Rules, 28 January 2012, available at http://www.economist.com/node/21543489 (consulted on 2 April 2013).

[94] Ibidem footnote 13.

[95]The Free Dictionary, Search and Seizure, available at http://legal-dictionary.thefreedictionary.com/Reasonable+expectation+of+privacy (consulted on 1 June 2013).

interference than American Courts, and more willing to restrict speech if necessary to protect the dignitary rights of citizens.[96] Even the two opinions are exclusive, this does not mean that Americans have no regard for their public reputation, or that Europeans are not concerned with the powers of the State. In Europe, the general trend is the States intervene the public society to protect citizens' privacy, whereas in the US, public authorities pay more attention to promote personal liberty and free expression. Therefore, European rules that protect public reputation through government action would meet significant obstacle in First Amendment doctrine if imported to the US.[97]

4.1.1 EU Response

Under the context of EU data protection environment and the proposed right to be forgotten, recently some European countries have experiences on the right to be forgotten in practice. For instance, Switzerland is a good example of the development of the right to be forgotten. It has very strict privacy laws to prevent publication of individuals' photo without their consent. In Swiss law, "publishing the name of someone with a criminal record may be allowed after time has elapsed since conviction only if the information remains newsworthy…"[98] So far, the Court practice also has already acknowledged the criminals have right to delete the information which related to their convinced crimes.[99] In early 2010, moreover, an Italian Court found several Google executives permitted a video to disseminate online, this video displayed a disabled boy who was abused, the Court defined that it violated Italian privacy law.[100]

---

[96] Black's Law Dictionary, 2009, p. 522. Dignitary Definition, Merriam-Webster.com Dictionary, available at http://www.merriam-webster.com/dictionary/dignitary (consulted on 2 May 2013).
[97] Von Hannover v Germany (App no 59320/00) ECHR 24 September 2004
[98] Werro, 2009, p. 291.
[99] Hendel, In Europe, a Right to Be Forgotten Trumps the Memory of the Internet, 3 February 2011, available at http://www.theatlantic.com/technology/archive/2011/02/in-europe-a-right-to-be-forgotten-trumps-the-memory-of-the-internet/70643/ (consulted on 27 March 2013).
[100] Sullivan, Italian Court Finds Google Execs Guilty of Violating Privacy Code, 24 February 2010,

These developments suggested to have wide and comprehensive understanding of "right to be forgotten". To further address how exactly an EU Member State would enforce the right to be forgotten, it might be useful to consider Spain's recent request to hide personal information against Google.[101]

Although later than the French and Italian Data Protection Agency, the Spanish Data Protection Agency, *Agencia Española de Protección de Datos* (AEPD) has recognised the right to be forgotten build on data protection principles, basically on data quality, collection limitation and purpose specification principles. Moreover, the AEPD has been a pioneer by extending and defining the new right to be forgotten. The AEPD considered that individuals have the right to delete personal data published if he or she does not consent, they also have the right to object data processing performed by search engines. The AEPD claimed that if the information does not have a current public relevance, even it is about public or legitimate information as official journals of government, it could be ask to cancel.[102]

There are many cases in Spain refer to the so-called the right to be forgotten. Therefore, in early 2011, AEPD issued decisions demanding that Google to remove news articles from online certain links on grounds that the articles contained information which infringed the privacy of Spanish citizens, arguing that the company was in breach of the right to be forgotten as acknowledged in the laws of Spain.[103] The specific case related to an official notice of foreclosure, it derived from an outstanding debt with the Social Security, which appeared in La Vanguardia (a Catalan newspaper) in 19 January 1998. The debt was later on paid by the debtor and the foreclosure had

---

available at http://searchengineland.com/italian-court-finds-google-execs-guilty-of-violating-privacy-code-36813 (consulted on 31 March 2013).

[101] Sibble, 2011, p. 12.

[102] Simón Castellano, 2012, p. 22.

[103] BBC News, Google fights the Spanish privacy order in court, 20 January 2011, available at http://www.bbc.co.uk/news/technology-12239674 (consulted on 2 May 2013).

never took place. However, if you type the name of the concerned person on Google, the first result links to the page of the newspaper's archive showing that old notice of foreclosure. The affected person appealed to the AEPD, asking for an prohibition against both the newspaper and the search engine. The AEPD dismissed the claim against the newspaper who was under the legal obligation of publishing the official notice, and issued an injunction against Google Spain SL. to delete the data from the search engine's index.[104]

There are a number of similar situations existed in Spain that individuals wanted Google not to connect their names with negative events which had occurred many years ago, in addition, they also do not want their information which were published in the online editions of newspapers and regional official gazettes is available online.[105] According to the Google Transparency Report, Just between July and December 2011, Google received 14 petitions. "We received 14 requests from the Spanish Data Protection Authority to remove 270 search results that linked to blogs and sites referencing individuals and public figures. The Spanish Data Protection Authority also ordered the removal of three blogs published on Blogger and three videos hosted on YouTube. We did not comply with these requests."[106]

Spain allows its citizens to sue to force companies to erase information held about them under the Spanish Data Protection Authority.[107] So AEPD issued decisions

---

[104] ISP Liability, Spain asks the ECJ whether Google must delete links to personal data, 2 March 2012, available at http://ispliability.wordpress.com/2012/03/02/spanish-court-asks-the-ecj-whether-google-must-delete-links-to-personal-data/ (consulted on 8April 2013).

[105] Escribano, Preliminary ruling on the right to be forgotten may be requested by Spanish Courts. The Google case, 7 March 2011, available at http://blogs.olswang.com/datonomy/2011/03/07/preliminary-ruling-on-the-right-to-be-forgotten-may-be-requested-by-spanish-courts-the-google-case/ (consulted on 5 April 2013).

[106] Law & the Internet, Spain demands the right to oblivion for its citizens, 30 March 2011, available at http://www.blogstudiolegalefinocchiaro.com/wordpress/2011/03/spain-demands-the-right-to-oblivion-for-its-citizens/ (consulted on 12 March 2013).

[107] Anderson, Spain asks: If Google search results make your business look bad, can you sue?, 27 February 2012, available at

demanded Google to delete the certain links. Google states that information made available by third parties is public and its removal should be considered as a problem of someone else. In particular, Google believes that Spanish and European law should based on the content of publisher who holds the material.[108] To be precise, Google consider that requiring intermediaries like search engines to censor material published by others would have a potential threat on freedom of expression. The US company insist that they will not eliminate links to information published by third parties "because it originally belongs to those websites". For these reasons Google faced off against AEPD decisions and refused to conceal information on grounds that this would constitute "censorship". while the AEPD considers that the search engine should observe the "*derecho al olvido*" or "right to be forgotten", which recognises a person's right to block information affecting his or her privacy or dignity.[109] Then generally, the issue between the AEPD and Google is whether individuals have the right to oblige search engines to erase or block search results that point to personal information. Therefore, Google appealed this issue to the Spanish National Court, *Audiencia Nacional*, the highest Court in Spain. Probably it takes time for *Audiencia Nacional* to response because more than 130 cases are pending before it, in which Google is appealing injunctions issued by the Spanish Data Protection Authority against the search engine.[110]

In 2012, the Spanish Audiencia Nacional referred to the ECJ nine questions in the

---

http://arstechnica.com/tech-policy/2012/02/spain-asks-if-google-search-results-make-your-business-look-bad-can-you-sue/ (consulted on 28 March 2013).

[108] Fleischer, 'The Right to be Forgotten', seen from Spain, 5 September 2011, available at http://peterfleischer.blogspot.nl/2011/09/right-to-be-forgotten-seen-from-spain.html (consulted on 3 April 2013).

[109] El Pais, Google defies Spanish requests to hide personal information, 21 June 2012, available at http://elpais.com/elpais/2012/06/21/inenglish/1340280978_188515.html (consulted on 8 April 2013).

[110] ISP Liability, Spain asks the ECJ whether Google must delete links to personal data, 2 March 2012, available at http://ispliability.wordpress.com/2012/03/02/spanish-court-asks-the-ecj-whether-google-must-delete-links-to-personal-data/ (consulted on 8April 2013).

framework a process between AEPD and Google.[111] In summary, the questions what the the Audiencia Nacional wants to know is whether Google is restrained by Spanish European law on data protection. if it is responsible for the damages that dissemination of personal data may cause to citizens. And whether the individuals concerned can exercise their rights before the regulatory Spanish body and the Spanish tribunals, or if they have to go to Court in the US. The Audiencia Nacional also wants to know the scope and contents of the rights to erasure and to block to be clarified, it means whether an individual may apply for a search engine to stop indexing information about him or her published or included on the websites by third parties, even if its reservation at the site of origin is lawful, but the applicant considers that its appearance in search results threatens their privacy, dignity or right to be forgotten.[112] The oral hearings took place 26th February 2013 at the New Great Courtroom Advocate General and the Jääskien's opinion will be published on 25 June, the ECJ sentence might be ready by the end of this year.[113]

The ECJ's answer will prove a instructive suggestion as to the boundaries of the right to be forgotten, especially with respect to search engines like Google, whose search results include news articles. It might also indicate how the EU will apply this right to organisations, like Google, Facebook, YouTube, etc. The upcoming decision of the ECJ will have a great significance, restricting not only the Spanish Courts but also all of the national Courts of the European Member States. In the near future we will see how the ECJ defines, interprets and understands the right to be forgotten and the limits of this right. It is really likely that the final result will be influenced on the new framework in data protection and the modification of EU Data Protection Directive. And it is also have an indicative recommendation in which the European Commission is

---

[111] Número de Identificación Único: 28079 23 3 20100004781,Procedimiento:PROCEDIMIENTO ORDINARIO 725 /2010,Sobre: EN LA AGENCIA DE PROTECCION DE DATOS (in Spanish)

[112] Ibidem footnote 110.

[113] Case C-468/11 Commission v Spain OJ C 340

going to address this matter.

4.1.2 US Response

Now the main arguments in US on the right to be forgotten is whether the right to compel the removal of personal information from the internet would infringe upon the First Amendment rights. This produces two questions: (1) Would granting data subject have the right to require a creator to remove the offending information from the website which violate the promulgator's free speech rights; and (2) would granting the right allow the data subject to compel that their information be removed from third-party websites.

Many US commentators, when confronted with the suggestion of development of a "right to be forgotten," accused the EU regulator of "foggy thinking", and the American lawyers and professors also oppose to this right.[114] They think the proposed European legislation will seriously alter the structure of the Internet, damage many companies like Google, Yahoo, Facebook etc. They have predicted that if the right to be forgotten were adopted in the US, it would violate the freedom of expression which was written in the First Amendment and will represent the biggest threat to individuals' free speech.[115]

In US, The First Amendment to the US Constitution plays an important role in US Court practice. It states that restriction to the right of free speech would be prejudicial to public interests. On grounds of the First Amendment, the American privacy rights have two values, "the value of the free press, and the value of the free market."[116] The laws in US protect this values, the obligation of media in US is "discover the truth and report it, not merely the truth about government and public affairs, but the truth about

---

[114] Ibidem footnote 3.

[115] Mayes, We Have No Right To Be Forgotten Online, 19 March 2011, available at http://www.guardian.co.uk/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet (consulted on 10 April 2013).

[116] Ibidem footnote 13.

individuals."[117] Since the freedom of expression was tied to the constitutional scrutiny, it is difficult to bring the right to be forgotten into this standard.[118] Therefore, for that reason, when privacy interfere with the freedom of expression, the freedom always take over the first place, and the privacy trend to become losing.

According to the meaning of the First Amendment, there is no doubt that the embarrassing, inaccurate personal informations fall within the scope of the right to be forgotten. And also In the US there is the Privacy Act of 1974 which would be the most analogous to the right to be forgotten. The Act shows that the government is prohibited from disclosing information about individuals without their consent while individuals are given a right to access records about themselves and make changes if there are errors.[119] For European level, the Commission provided that data may not be deleted when it is necessary for "the right to freedom of expression". However, the main point which arising dispute has a different understanding of the freedom of expression in American law. In American law, truthful publications of lawfully obtained information may be constrained only when the restriction is "narrowly tailored to a state interest of the highest order."[120] This directly conflicts with the core of the right to be forgotten. It means that just in view of the State interest of the highest order, the right of freedom speech could be restricted, but for the reason of individual's privacy rights, it can not be invoked. "Absent exceptional circumstances, reputational interests alone cannot justify the proscription of truthful speech."[121] Thus, by extension, it reflects that the right to be forgotten could only be applied by a data subject against a content creator under "exceptional circumstances" of the "highest order" of state interest. Personal privacy and reputational harm are not in such interests.

Since Europe and US have diffierent understanding of the right to privacy, which

---

[117] Ibidem.
[118] Smith v Daily Mail Publishing Co., 443 U.S. 97 (1979)
[119] Ibidem footnote 93.
[120] The Florida Star v B. J. F., 491 US 524 (1989)
[121] Butterworth v Smith, 494 U.S. 624, 634 (1990)

influences the application of the right to be forgotten. Hence, coordinating international data protection law to make them more reconciliatory should be a trend in our present society.[122] The Federal Trade Commission, a national data protection agency in US. The development represents an incresing advance for privacy regulation.[123] The privacy in the US has been received more and more attention these years. The Federal Trade Commission has already engaged in over three hundred enforcement actions concerning privacy so far. And a project which implements " Do Not Track" System is also underway.[124] Furthermore, not all US commentator oppose the right to be forgotten, as some operative features of the right can be separated out from the European legal and cultural context and applied to the US without offense the constitutional right, they agree with a more acceptable way which has a limited application of the right to be forgotten. [125] For example, they suggest that just children should have the ability to erase information that posted improvidently, because the children lack of judgement.[126] Thus it may be possible to implement a circumscribed version that will avoid less controversy about freedom of expression and privacy rights.

Even if the US argues apply the right to be forgotten would be unconstitutional, the First Amendment does not prevent all rights of data deletion.[127] In the First Amendment, it not only grants Internet users a right to speak, but also the right not to speak. The "individual freedom of mind"can have a widely concept, both the right to speak and the right to avoid speaking, they are complementary components[128] Moreover, the First Amendment does not compel anyone to speak, nor does it forbid voluntary agreements

---

[122] Messenger, 2012, p. 29.
[123] Bamberger & Mulligan, 2011, p. 285.
[124] Federal Trade Commission, FTC Testifies Before the Senate Commerce Committee on Privacy, 16 March 2011, available at http://www.ftc.gov/opa/2011/03/privacy.shtm (consulted on 11 April 2013).
[125] Sykes, 1999, p.221; Zittrain, Rosen, 2010, p.25.
[126] Bennett, 2012, p. 166.
[127] Pop, EU To Press For "Right To Be Forgotten" Online, 4 November. 2010, available at http://euobserver.com/social/31200 (consulted on 20 April 2013).
[128] Sedler, 'The First Amendment Right of Silence', Wayne State Univ. Law School Research Paper Series No. 07-39, 20 November 2007, available at http://papers.ssrn.com/sol3/papers.cfm?abstract-id=1031505 (consulted on 18 April 2013).

not to speak.[129] Therefore, people have the right to express their opinions on the websites, also has a right to stop speaking by removing the data. From this point of view, where a user submits her or his own personal data to a website and then want to remove, it should be deleted according to the personal willingness. As a consequence, the limited version of the right to be forgotten, a right to delete voluntarily submitted data would not offend the First Amendment.[130]

4.2 Criticisms of the Right to Be Forgotten

Although the right to be forgotten has been proposed in Europe, it may affect companies or organisations outside of Europe. Since open questions of the right to be forgotten was put forward, this right has become very controversial. Concerning the right to be forgotten may be in conflict with other fundamental rights, especially to that rightholders who refer to this issue. This part seeks to address the two mainly critical questions about the right to be forgotten.

4.2.1 The Interplay Between the Right to Freedom of Expression and the Right to Be Forgotten

According to Viviane Reding's speech, it is obvious that the right to be forgotten is not an absolute right. It is not a right that can totally erase the personal data or take precedence over freedom of expression.[131] Furthernore, in Article 80 of proposed Regulation provides an provision about processing of personal data and freedom of expression, in order to cohere with the right to freedom of expression. It defines the

---

[129] Cohen v. Cowles Media, 501 U.S. 663, 672 (1991)
[130] Walker, 2012, p. 257.
[131] Ibidem footnote 17.

exemption and derogation 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.”[132] Nevertheless, this exemption does not mitigate the worry of opponent scholar and legal professionals, because in the proposed Regulation, it does not explain what criteria should be used, how to balance the interests between privacy right and the right to freedom of expression and what is the clear scope of the exemption and derogation.[133] The exemption in the proposed Regulation is not clear and still have vague conception. And in addition, since the EU are very in favor of this right, the scholars are worried about that EU would give priority to the privacy when deal with the right to be forgotten, and ignore the freedon of expression.[134] This dispute is particular discussed between privacy advocates and free speech defenders. How to balance the interests of these two right is still underway. There is a case about the deletion of personal data in social networks refer to the relationship between the right to freedom of expression and the right to be forgotten.

Stacy Snider, a 25-year-old girl, she is working as a student-teacher at Conestoga Valley High School. Only some days before her graduation in May 2006, Millersville University in Pennsylvania discovered a photo on Stacy’s “MySpace” page, titled "Drunken Pirate," in the picture, Snyder can be seen wearing a pirate hat and drinking from a plastic cup. So the university accused Stacy Snyder of inducing minor drinking. This photo which posted in the website became the root of her problems to get her teaching degree. First, her supervisor found this photo and the title, so the supervisor ask her to off state considering her behaviour was unprofessional. Secondly, the director of Millersville University School of Education, where Stacey was enrolled in, said she had encouraged juvenile people and her underage students to drink. Although her action

---

[132] Ibidem footnote 21, art 80.
[133] Hendel, 2012, p.88.
[134] McNealy, 2012, p. 123.

was indirectly, the university argued it is the same as instigation and it has serious negative influence to minors. For all those reasons the university denied to issue her teaching degree. Stacy, definitely disagreeing with this decision. She maintained that the photo was taken at a costume party that off campus and after school hours. In allusion to the university refused to issue her a teaching degree, Snyder sued siting violation of her First Amendment rights. Francine McNairy, who was the president of Millersville University said "this was not about First Amendment rights, it was about performance, and she clearly did not do what was necessary in order to earn a degree in education."

However, the District Court for the Eastern District of Pennsylvania decided in favor of the university, the judge who heard the case rejected the arguments pointed out by Stacy in the lawsuit.[135] They argued that the First Amendment only protects public interests and does not protect individual who was in trouble due to post information in the social networkings even they came from a public employee. So, in conclusion, the federal court is not the appropriate forum in which to review the wisdom of a personnel decision taken when a public employee speaks upon matters of a personal interest. The case shows fully the negative consequences that can be caused, because the shared information in social networks is easy to become publicly and visible to others. Nevertheless, do citizens have the right to remove the shared personal data on the social networks before they affect their reputation? According to Stacy Snider's case, if that case happened in EU, will the result be different as in US?

The concept of data protection rights in this case are conflict with Europe, where has a huge scope of privacy rights, it is laid down especially in 95/46/EC Directive. In Europe, it is generally examine that individuals have a right to revoke or withdraw their contents to the disseminating of their personal data by others. With the European data

---

[135] Stacy Snyder v Millersville University, J. Barry Girvin, DR. Jane S. Bray and DR. Vilas A. Prabhu Case 2:07-cv-01660-PD

protection environment, individuals have the right to prevent or control another party's use of data which is personally identifiable to the individual, whether or not sensitive or confidential, that was lawfully obtained by the other party. Therefore data protection gives individual far broader rights to control uses of personal information by third parties. The European principles for data protection protects an individual's interests, not just public interests which relating to collection, processing, or other use of information identifiable with that person. Because the right to be forgotten is almost approved in Europe, people could claim cancellation and rectification of information against the publication of image, video, comments in social networks when it contains personal data that may injure the reputation of people.[136] If under EU condition, Stacy Snider could have the right to delete her image that posted in the website, and have the right to make sure that behaviour did not have retroactive force. Then she could get her degree normallly.

EU hold a opinion that the right to be forgotten and the right to freedom of expression are not contradictory. And the right to be forgotten will not take precedent on the freedom of expression and free speech. It would be a solution for achieve both two rights. And also European countries are following the EU perspective on this point currently. For instance, in Spain, the data protection law, *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (LOPD) stated specifically the right to withdraw their consent. With preciseness Article 6.3 of *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* provides the right to withdraw the consent when it has justified or well-grounded reasons, with no retroactive effects attributed.[137] So in conclusion the individuals have the opportunities to withdraw their consent and ask the person who is responsible for social network to delete their personal data.

Therefore, to summarise, as the hotly discussing in EU and US whether the right

[136] Meg Leta & Friess & Matre, 2012, p. 101.
[137] UOC-Huygens, 2011, p. 401.

to be forgotten will infringe the right to freedom of expression. How to balance these rights. The commentors question there exist a risk of right to freedom of expression if the right to be forgotten is made in the law.[138] Although they recognised that the privacy interests are let individuals leave from public eyes, the true information is necessary to keep at the aim of freedom of media no matter how the accuracy of the data is.[139] And proponents of the right to be forgotten assume that due to wide data retention and search capacities, we can not keep our personal data going which may have negative effects on ourselves when we move on our lives.[140] For this kind of situations, The most practical problem is if the headquarter of publisher which does not recognize the protection of personal right, such as US, even if the EU suggests implement the right to be forgotten, the opponents refuse on the grounds that jurisdiction.[141] Is there a way for both the individuals' privacy and freedom of expression come true? If we do not find trade-off between them, it would be an obstacle and controversy for enforcing this right in practice.

From my perspective, I think the right to freedom of expression and the right to be forgotten are not conflicting. As analysis above, indeed, people have right to post pictures, videos, comments, articles etc to the social websites. They can speak everything that they want. However, if the data that posted injure their interests or reputation, or will have negative effects on their study or work. They have the right to request take down these information, not only the information which published by content creators and the third parties websites, but also the data owners. The right to freedom of expression as a prior right, and the right to be forgotten as ex post facto right could avoid the negative effect on the individual's privacy. If the information is not possible to bring adverse effect to people, it of course no need to use the right to be forgotten, the right to be forgotten just as a remedy and additional right of the personal

[138] Ibidem footnote 54.
[139] Ibidem footnote 120.
[140] Bernal. 2011, p. 12.
[141] Ibidem footnote 87.

data protection.

4.2.2 Challenges in the Internet Field

As shown, the environment for the development of a new proposed right to be forgotten is complicated. As a modern media for today's society, the Internet is a necessary way to disseminate the information rapidly, but the shortcoming is the information which were posted in the public forum, even personal homepages, it is possible that have been seen, copied or downloaded by global user easily. The European Network and Information Security Agency (ENISA) issued comments on the proposed data regulation recently. ENISA declared that generally the right to be forgotten is adaptive and rational at a theoretical level, but it is difficult to implement in the Internet area.[142] Because in online environment, where data is disseminated in seconds, once data is published, it can be copied and disseminated by third parties in a very short time. If the data subject want their data to be deleted, then the social networking would face difficulties to control over these third parties to let them based the request of individuals and delete the information fully and efficiently. In this condition, it may have negative effect on the data subject's future.[143]

The Ways of Personal Information Dissemination

Due to the technical advanced, the personal information can be used in variety forms, people notice that their personal data should be user-friendly at any time. Lack of protection makes consumers hesitate to trust the website and buy online or adopt

---

[142] Info Security, Problems with the EU's proposed 'right to be forgotten,' 20 November 2012, available at http://www.infosecurity-magazine.com/view/29412/problems-with-the-eus-proposed-right-to-beforgotten (consulted on 10 April 2013).

[143] Ibidem footnote 94..

new services. This risk show the threaten to the online personal data. The individuals wish that just the data which need to use be collected, not anything more, so they should be aware of what they are signing in to and make sure data collect minimisation, that means data protection measures are necessary to be done to ensure efficient use of the data. However, in current conditions, there is not easy to avoid the misuse of personal data. Hereby I will address three factors which bring treat to the individuals data dissemination.

Firstly, for example, usually public authorities use personal data for numerous purposes, such as tracing individuals because of an outbreak of disease, for preventing from terrorism and crime, to administer social security projects or for taxation purposes, etc. And the growing use of procedures allowing automatic data collection, such as electronic transport ticketing, road toll collecting, the individual information, such as name, phone number, home address, even the number of credit card is easier to be disclosed. Nowaday, the geo-location devices make it more open, it could find the location of individuals just because people use a mobile device.

Secondly, not only the public data authorities, also the private sector collects a amount of information. For instance, Google stores all individual search queries in great detail: "literally, Google knows more about us than we can remember ourselves".[144] Facebook collects a large number of personal data through cookies, not only Facebook users themselves but also include non-members who just visit a page of Facebook, even without saying something.[145] Mobile phones also continuously produce location data, which are stored by European telecom providers for each communication. This may be stored on the device itself and downloaded on users' computers without their content. [146]

---

[144] Ibidem footnote 41, pp. 1-15.
[145] Roosendaal, 2011, p. 1.
[146] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications sevices or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive) [2006] OJ L105/54

Last but not the least, not only public organisations and search engines trace personal data, also individual themselves are generating data related to other people, through blog and tweet posts, tag someone's name to a photo on a social networking site, so that the photo can be automatically linked to this person's own page. With millions of photo uploaded daily and many millions of Facebook users, there is a important likelihood that anyone can be traced and tagged unsuspecting.[147] In a nutshell, it is clear that we live in a digital world of big data, particular related to the right to be forgotten is the result of information age and the way to deal with the data from different times and places to protect the privacy of personal data.

Controversial Problems

The objective of the right to be forgotten is give individuals the right to access, objection, rectification and cancellation of personal data which could make sure that the citizens have the right to control the transmission of their information and guarantee that after deleting, it has no retroactive effects, avoid their personal data disseminating in a negative effect in the future.[148] However, as aforementioned, on the Internet environment, it is not effortless to achieve an efficient protection of individuals' privacy. At least, there are three controversial problems in question.

The first question is who has the right to demand that a data item should be forgotten requires interpretation. "if I post something, and someone else copies it and re-posts it on their own website, do I have the right to request delete it?" According to the proposed right to be forgotten by EU, the answer is yes. For instance, a picture in the website showing that Anna and Tony took part in the same party at the same time, and they did drinking. Anna wished the photo to be forgotten, while Tony insisted it

---

[147] Kincaid "facebook users uploaded a record 750 million photos over new year's" , 3 January 2011, available at http://techcrunch.com/2011/01/03/facebook-users-uploaded-a-record-750-million-photos-over-new-years/ (consulted on 16 April 2013).

[148]BBC news,''Apple 'Not Tracking 'iphone users' 27April 2011, available at http://www.bbc.co.uk/news/technology-13208867 (consulted on 13 April 2013).

could be remained. So whose wishes should be respect? And if numerous people appear in a group photo, who can decide whether this picture be taken down? Another example, Tony incorporate part of the twitter that he received from Anna into his own blog or facebook etc. Afterwards, Anna wants to remove her twitter, what effect will this have on the status of Bob's blog post? Does Bob have to remove his entire blog post? Or does he have to remove Alice's tweet from it and rewrite his own post again? What criteria should be used to decide appropriate in practice? This is a very simple instance, but extending the meaning, the question is how the right to be forgotten could be balanced against the public interests on politics, journalism, history and scientific inquiry on the internet? Should the politician or government be able to request to remove the embarrassing report, or the journalists request to withdraw the news reports in the media which may produce adverse impact. What principle should be adopted to judge, and who has the authority to make decision?[149]

The second question is who has the right to decide remove the data that requests by individuals? According to Article 17(1) in the proposal, the data controller are obliged to delete the information immediately when receive the request from data subject.[150] However, it will put more burden and challenge on Internet companies like Facebook, Google, Yahoo, and also may increase the expenditure of the companies. Because it demand the companies must prove to a European Commission authority that the information which were requested to delete is included in the limitation of proposed right.[151] Now that the proposed Regulation endows an obligation to the data controller, , do the search engines have the right to decide which kind of data belong to these limitations? If the search engines make a decision that the information is part of exceptions and should not be forgotten, but the data subject object the determinations, how to deal with that?

---

[149] Curren & Kaye, 2010, p. 401.
[150] Ibidem footnote 21.
[151] Ibidem art. 17.

The third question is what constitutes in a “forgetting” data item? Europeans have a long tradition of introducing abstract privacy rights in theory but the proposed Regulation did not define specific obligations for data controller what type of information and use what kind of modalities to provide to data subject. For example, in Article 17(1)(a), the data subjects have the right to ask data controller erase “the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed”, so how to define “the data are no longer necessary”. Concerning the question of what kind of information forms should be deleted. This is included in the definition of personal data as “any information relating” to data subjects, regardless of its source.[152] Nevertheless, there have different interpretation of what “ any information relating to data subjects ” is. Currently, there are two opinions on that, on the one hand, a strict interpretation proposed in European Regulation examines include that information posted by other parties, the information posted by the data subjects own, and also identically constitutes the information then have been copied by others. Moreover, there are some problems and difficulties to take down all derived copies in the actual implementation. On the other hand, the weaker but more possible interpretation would allow encrypted copies of the data survive, because it is not easy to deciphering by unauthorized parties and will have small chance appear in public query results and search engines.

[152] Ibidem art 4(2).

5. Difficult Practical Implementation

Even though the right to be forgotten has been discussed much more controversial, it was written in the European proposed Regulation. It seems a development trend of personal data protection. The proposed definition is on the forming stage, it is inevitable that there are still many difficult problems around the right to be forgotten, in order to solve the problems, in this section, we try to find what difficult practical dilemmas are.

5.1 From the Legal View

The right to be forgotten used to be a political notion. Now the European Commision has proposed to make this notion into the law, to create a integrated framework for the right to be forgotten. It will be a big challenge to turn this notion from theory to practice. The criteria of implementing the right is the key elements under current condition.[153] However, as mentioned in last section, in light of the scope of the right to be forgotten in the proposal is vagueness, it does not define clearly who has the right to decide the deletion of the information, what constitute the right to be forgotten. The clearly definition and legal clarification will be subject to the interpretation, in order to make sure this right can be properly implemented. Otherwise, without the present provisions by law and prior cases, it will be up to the Courts to interpret this right, that gives more margin of appreciation to the judges to deal with the cases. In this way, it will produce different criterions. From the current proposed Regulation, there are three uncertainties surrounding the right to be forgotten.

Firstly, the dilemma is the functioning of the data controller, which formulates in the second paragraph in Article 17. It is the source of dominating dispute. Based on the current draft, this paragraph gives a right to the data subject when the data controller

[153] Leszczewicz, 2012, p. 32.

make the personal information public, this means at the same time, it also grants an obligation to data controller. The most vagueness in this paragraph is " take all reasonable steps" to inform the third parties. Such an obscurity has been brought to the forefront by the EDPS who highlights the need to clarify the specificity of the right to be forgotten's scope.[154] The EDPS clarified that the Article 17 imposes the obligation upon data controller, it potentially reflects that the data controllers should not assert it to be impossible.[155] The author thinks that every right has double-edged, both rights and obligations, the current provision give obligation to data controller but does not formulate the data controller's rights. And how to sort out the obstacles when the data controller are dealing with the demands of data subjects. There are no provisions about this question. Without the support or cooperation of other parties, it will be difficult for data controller to carry out their mission.

More similar, at the end of this paragraph, it defines the data controller " shall be considerde responsible for that publication". This means the data controller have the responsibilities for the publication of personal data by a third party when they have authorized it. But then the underlying problem is how a publication be 'authorized'? And what does the responsibility of data controller entail in line with the article?[156] At this point of view, it leaves a great deal open to the interpretation of the obligation of data controller.

In addition, in Article 17.9 of proposed Regulation, it endows an admissible power to the European Commission to adopt the delegated acts. One of the object to adopt delegated acts is to further specify criteria and conditions as referred to in second paragraph, and it will be also good for having criteria and requirements for the application of the right in specific sectors and situations.[157] On the one hand, this seems

---

[154] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012.
[155] Ibidem.
[156] Ibidem footnote 21.
[157] Ibidem.

to take the rapid changing of information environment into consideration and seems a solution for cover current shortage. However, on the other hand, depend on the Article 290 of TFEU, the delegated acts are non-legislative acts, it should as a supplement or amend to the legislative acts. The essential elements of a field should be written in the legislative acts, shall not be subject to the delegated acts.[158] Therefore, the question is whether the European Commission reserves the right to adopt delegated acts within legitimate.

Secondly, the lack of transparency. According to Article 17 of the proposed Regulation, the data subjects have the right to control their information whether retain or delete, the data controller should basis on the wish of data subjects. This means the individuals have the right to exercise control over their own data and obtain effective protection of personal data. Therefore it is necessary that individuals are timely and clearly informed in a transparent way. To apply to the online environment, the basic idea of transparency is let people know and understand if personal data are being collected, by whom, for what purpose and how it is processed. However, we can not find any relevant provisions on the current "right to be forgotten and to erasure" in proposed Regulation, such as how and by whom their data are collected and processed, for what reasons, for how long and what their rights are if they want to access, rectify or delete their data are not sufficient. It is also very important for individuals to be informed when their data are destroyed, lost, altered, accessed by or disclosed to unauthorised persons accidentally or unlawfully.[159]

At present, the control of data subjects on their own data is very weak. Even sometimes people even do not know such information exist online before they are injured for their online information. So when and why this right can be invoked still waiting for supporting from law. For example, the case of Andrew Feldmar, which

[158] Ibidem footnote 56.
[159] Ibidem footnote 12.

explained by Mayer-Schonberger Viktor in his book.[160] Andrew Feldmar is a Canadian psychotherapist living in Vancouver in his late sixties. In 2006, he went to Seattle-Tacoma International Airport to pick up his friend, he attempted to cross the boarder between US and Canada since he did many times before. However, this time, a boarder guard asked to a Internet search engine for Andrew. One of the searching results is an article written by Andrew in 2001 in an interdisciplinary Journal, in this article, he mentioned that he had taken LSD which is a kind of very powerful illegal drugs in the 1960s, but he also examined that he has not taken this drug since 1974. Even if it was already more than thirty years past, he was detained for four hours, fingerprinted and signed statement that indicate because of he has violated the law when he taken drug, he was prohibited to further entry into the US. For Andrew, he did not know his information was still online and would have negative effects on him. Because of the digital technology, the information that long time ago has not been forgotten, the data controller disclose people's data without knowing. Under this context, like the situation of Andrew, if the people even do not know their information online, so with the content of data subject will become meaningless. Consequently, the European Commission need to consider that introduce a general principle of transparent processing of personal data in the legal framework as a kind of supporting and guidance to the right to be forgotten executing in realistic society.

Thirdly, how to bring the rule of law to online environment.[161] On the seventh annual internet governance forum which aim is protecting the rule of law in the online environment, there is a common understanding that human rights should apply to online environment.[162] Obviously, the right to be forgotten is a new human right. Giuseppe Vaciago, who is a lawyer and Local Education Authorities Expert, said that the proper

---

[160] Ibidem footnote 41.
[161] Interview with Navi Pillay, United Nations High Commissioner for Human Rights, Office of the United Nations High Commissioner for Human Rights, Leuven, 21 May 2013.
[162] Organisation for Security and Co-operation in Europe, Seventh Annual Internet Governance Forum, 7 November 2012, available at http://www.osce.org/fom/94222 (consulted on 1 April 2013).

application of rule of law in online environment basically require detailed definition of conception. Like some limitation of fundamental rights should be narrowly defined and prescribed clearly by law. Inject the rule of law into the online environment could useful to precise interpretations of some fundamental rights or principles.[163] Then based on the particular definition, the stakeholder can not use the deficient provisions as an excuse to get rid of the obligation. Otherwise either the stakeholder or judges is confusing with the unclear system. The ambiguous and vague wordings will most likely make the ECJ a very difficult task which will arise criticism on the enforcement of the right to be forgotten. Ultimately, although the new EU proposal try to make the theoretical regulation to practical level, the root cause of the puzzling conception is the absence of systematic legislative initiative, it is still difficult to come into play if the online environment lacks the rule of law in functioning.

5.2 From the Technical View

The more variety ways of data's using, collecting, storing and processing in technical development, the more efficient guarantees need for individuals to enjoy effective control over their personal data. There are a number of approaches to implementing a right to be forgotten, however, the technical measures are the one of most convictive safegaurds to perform the right to be forgotten in practice. Hence the technical limits must be conscious in the implementation of the right to be forgotten. The Commission also believes that we need further research to enhance the security features of the technologies.[164] Finding what technical problems exist is good for

---

[163] Internet Governance Forum, IGF 2012 Workshop Proposal, (No: 111)Protecting the rule of law in the online environment, 21 April 2012, http://wsms1.intgovforum.org/content/no111-protecting-rule-law-online-environment (consulted on 31 March 2013).

[164] Spies, Reform of the EU Data Protection Directive: 'Right to Be Forgotten'-What Should Be Forgotten and How?, 19 December 2011, Privacy and Security Law Report.

improving and solving the dilemmas, prevent the right to be forgotten from losing function, so as to use technical tools and measures as a backup to support the right to be forgotten enter into force in reality.[165]

5.2.1 Realistic Conditions

Nowadays, data is not what is was in decades years ago, social networking had not such universal and communicative beforetime. Today there are hundreds of millions of members use the social networking and social websites.[166] We must aware of technology indeed bring lots of advantages to our lives, we hardly leave it from our daily life. It allows individuals to share their information about their behaviour and comments easily and make it publicly and globally. The social networking is available on an unprecedented powerful scale. But at the meantime, it is undeniable that this development actually has both sides, methods of collecting personal data have become increasingly diversely and less easily perceivable. It result in the instability of data subjects control over their personal information.

A recent study confirmed that there seems to be Data Protection Authorities, business associations and consumers' organisations have an increasing risk on the protection of personal data in online environment.[167] Neelie Kroes, the European Commission Vice-President for the Digital Agenda, said in her speech On 25th November 2010 that "cloud computing may indeed become one of the backbones of our digital future."[168] Therefore we must pay more attention to how to improve and promote technical measures to answer the digital age. I will take the cloud computing

---

[165] Conley, 2010, p. 53.
[166]Social Networking Statistics, 11 December 2012, available at http://www.statisticbrain.com/social-networking-statistics/ (consulted on 1 May 2013).
[167] London Economics, 2010, p. 14.
[168]Kroes, "Cloud computing and data protection", 25 November 2010, available at http://europa.eu/rapid/press-release_SPEECH-10-686_en.htm?locale=en (consulted on 18 April 2013).

for an example to address this question. “Cloud computing”, an internet-based software that can share resources and information on remote servers in the cloud. This bring potential threat to the right to be forgotten, because it may produce the loss of individuals’ control over their information when they store their data with programs hosted on someone else’s hardware.[169] Due to the right to the protection of personal data is a fundamental right in the EU, also data protection features should be served the same role in cloud computing. If a cloud computing without efficient data protection is not the kind of cloud that we need. So we need to consider what sort of technical measures we can use to deal with the right to be forgotten in cloud computing era.

5.2.2 Technical Challenges

In the report of ENISA pointed that there are four fundamental technical challenges in enforcing the right to be forgotten: Firstly, allowing a person to identify and locate personal data items stored about them; Secondly, tracking all copies of an item and all copies of information derived from the data item; Thirdly, determining whether a person has the right to request deletion of data; Fourthly, effecting the erasure or deletion of all original or derived copies of the data when an authorized person exercises the right.[170]

In practice, it is divided into two systems, open system and closed system. In an open system, like many existing public websites today, anyone can make copies of the public data and store them at somewhere else places. Comparatively speaking, the feasible means to enforce the right to be forgotten is in closed system, where all parties could stay in a jurisdiction of the right to be forgotten, the dissimination of the data

---

[169] ENISA, Privacy considerations of online behavioural tracking, 19 Octorber 2012, available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking (consulted on 10 May 2013).

[170] European Network and Information Security Agency, The right to be forgotten—between expection and practice, 18 Octorber 2011, available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten (consulted on 27 February 2013).

must be authorized and in this way the responsible people could be linked to natural people and organisation in real world.[171]

in open system

In an open system it is difficult to remove all the information, such as the public internet. On the one hand, public data can be accessed by any people with cyber identities. These participant are capable of further distributing the information to other untrusted parties, possibly resulting in a massive replication of data. On the other hand, in such a system, there is difficult to find generally available, technical approach to enforce the right to be forgotten. Therefore, the right to be forgotten is impossible to implement fully in an open and global system. And also the challenge is unauthorized copying of personal information is impossible to prohibit by technical measures. For example, Anna saw some personal information about David from a computer screen. Anna can take a picture of the screen using a camera, copy or note down these information. It is impossible to prevent Anna from doing so in technical place, even recognise that Anna has gained a copy of David's personal data. When David ask to delete his information, all known copies of his information on the website are deleted, and he also thinks that his right to be forgotten has already fully enforced, however, Anna still has a copy of the information and maybe he will put it on the website afterwards and spread at random.

This situation is common in the online environment, when personal data is being included in social networking sites, homepages, blogs, tweets, etc. It becomes hard to under the control of the users who originated the information. The reason is that data can be copies at any time, stored and published in any locations, in various ways, for different purposes.[172] Such digital copying can not be prevented by technical means,

---

[171] Ibidem.

[172] Ministry of Justice, 'Summary of Responses, Call for Evidence on Proposed EU Data Protection Legislative Framework', 28 June 2012.

unless one is able to make very strong assumptions about the underlying software and hardware. A potential solution maybe useful to avoid the unauthorized copying of data would be to expand data with an executable program that enforces the right to be forgotten.[173] For instance, communicate with some servers to properly display the data, like images or videos could be equipped with a program that when the original information been deleted, the copied information can not be viewed and become disabled subsequently. However, this technique also faces some limitations and dilemmas in practice. Because such solutions would often request additional communication with external servers, which would arise additional security challenges.[174] Such programs that mentioned would produce a new way for the entrance of viruses on the individual's computers and devices. To functioning appropriately, the program and measures should enforce more fully permission, which would raise new problems like malicious code.[175] For this reason, such solution is also difficult to implement by public, industry and company.

It can be seen that under online environment, the digital dissemination is not easy to prevent in an open frame. Even use technical means, there is still hard to prevent, the replayed information is very easy to reinserted in the internet. Since the information exist in variety of different forms, both in various digital places and non digital place, like newspaper, book or press releases, etc. There is difficult to use technical way to make such a variety of data be forgotten.[176]

in closed system

A closed system is one that can process, transmit or store personal information, all participants, include data subject and data controller can access to personal information.

---

[173] Amborse, 2012, p. 23.
[174] Mayer-Schönberger, 2007, p. 181.
[175] Ibidem footnote 173.
[176] European Commission, 'EU study on the Legal analysis of a Single Market for the Information Society, New rules for a new age?' November 2009.

It can be trusted or held responsible for respecting applicable laws and regulations concerning the use of the private information. The closed system is capable of the processing, storage and dissemination of all information and could prevent the dissemination of data from the places that the right to be forgotten can not be implemented.[177] In this circumstance, where personal data is processed, transmitted and stored exclusively by data processing hardware or software owned and operated by the company. In such a network implementing the right to be forgotten is feasible in technical means, but also have its challenges. For instance, when the data subject invoke the right to be forgotten, ask to delete all copies of the information and any duplicated information, including copies which stored on the local disks of computers, backup copies stored on archival storage, etc.[178] It is being a technically challenging and require clearly functioning.

In theory, the right to be forgotten can be controlled and managed more conceivable and feasible in such a system, because it is closed. In this closed system, the user and operator of data access to the personal information are held accountable for comply with the law, all personal information under the jurisdiction of this system. However, in practice, it is necessary to notice, when company shares personal information, how to make sure that it will not conflict with the personal privacy rights. For example, some health care companies, like health providers, insurance companies and health care billing companies share patient records. They are responsible for holding the personal information in accordance with the law or regulations. These participating companies or industries are trusted and responsible for using the personal information with properly reasons. From the professional speaking, the healthcare departments have right to know personal information, like their illness and physical condition about patient.[179] Thereby during the process of sharing patients' information, technical method plays a decisive

[177] Ibidem footnote 170.
[178] Rosen, 2012, p. 90.
[179] Flaherty, 1992, pp. 389-420.

role to protect that will not infringe privacy of patient.

6. Mitigate Drawbacks of the Right to Be Forgotten

By support of the legal provisons, the right to be forgotten has a general and basic framework. However, in the current system, especially in the open Internet environment, the personal information is fundamentally impossible to delete or even perceive just based on the legal framework, a possible solution will be cooperate by legal authorities and technical methods to enforce the right to be forgotten.[180]

6.1 the Role of Data Protection Working Party

The European Data Protection Authorities, the Article 29 Working Party on the Protection of individuals with regard to the Processing of Personal Data Protection Working Party, which is an independent advisory body on data protection and privacy, laid down in the Article 29 of 95/46/EC Directive.[181] It is constituted by representatives from the national data protection authorities of the EU Member States, the EDPS and the European Commission. Its tasks are described in Article 30 of Directive 95/46/EC and the Article 15 of Directive 2002/58/EC. The Article 29 Working Party is able to address any question that related to the data protection. It carries on the mission by issuing recommendations, opinions and working documents.[182]

Vice President Reding prefer to have a high and sufficient level of data protection and give Data Protection Authorities more power so that they can effectively protect people's privacy. In her speech, she explained how important role of the Article 29 Working Party plays. In order to have a better framework of enforcement. "Three conditions must be met to make this possible. The first is that there must be one single

---

[180] Walker, 2000, p. 37.
[181] Ibidem footnote 1.
[182] European Commision, Refrom of data protection legislation, 25 January 2012, available at http://ec.europa.eu/justice/data-protection/index_en.htm (consulted on 17 March 2013).

lead authority responsible for action in a particular case. The second is that other authorities from other Member States should have the means to require the leader to act, to accept joint actions, and to discuss the remedy. The third is that the Article 29 Working Party must play an important role in this mechanism."[183]

For the Article 29 Working Party, it made positive reaction to the Data Protection reform, on 23th Matrch, 2012, it adopted "the opinion 01/2012 on the data protection reform proposals by Article 29 Working Party", it serves as the national data protection authorities contribution to the legislative process before the European Parliament and the European Council.[184] One of the elements is they will try to have all necessary tools to ensure an actual right to be forgotten.[185] The Opinion also provides a number of advices for explaining and identifying some certain aspects of the right to be forgotten, such as this right should be narrowed to take into consideration cases in which the data is in the possession of a third party or the data controller no longer exists or can not be identified, especially in the Internet context.[186] The Article 29 Working Party also highlighted that to comply with deletion request of individuals, it need regulate mandatory provision to third parties.[187]

As mentioned in last section, the definition of the right to be forgotten, like the scope of personal data, a clarification of who has the right to ask for the deletion of personal data and under which circumstances are not included in the data protection

---

[183]Reding, 'Independent Data Protection Authorities: Indispensable Watchdogs of the Digital Age Meeting of the Article 29 Working Party', avaiable at http://europa.eu/rapid/press-release_SPEECH-11-863_en.htm?locale=en (consulted on 1 May 2013).

[184] Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, 23 March 2012, available at http://ec.europa.eu/justice/data-protection/index_en.htm (consulted on 10 February 2013).

[185]Data Protection Working Party, Release Press, 29 March 2012, available at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/ (consulted on 3 April 2013).

[186] LLP, Article 29 Working Party Opines on Proposed EU Data Protection Law Reform Package, 30 March 2012, available at http://www.huntonprivacyblog.com/2012/03/articles/article-29-working-party-opines-on-proposed-eu-data-protection-law-reform-package/ (consulted on 29 April 2013).

[187] Article 29 Data Protection Working Pary, 83th plenary meeting, 13 December 2011.

legislation.[188] Article 29 Data Protection Working Party should work together with Data Protection Authorities, the European Data Protection Supervisor etc. to clarify these issued to guide the implementation. In the paper of ENISA, as a complementing of implement this new right, it recommended that the Data Protection Authorities and relevant stakeholders in this field should aim to improve user awareness relating to their rights which originate from the data protection legislation and on the possibilities offered to them by the legal system to exercise these rights, such as by complaining in cases of overmuch collection and storage of personal data.[189]

6.2 Feasible Measures for the Right to Be Forgotten

In order to have the acceptable and effective ways on the deletion of personal data, within the definitions of the right to be forgotten, technique provides a more possible pragmatic approach to support comprehensive measures.[190] However, we need to notice that for any reasonable interpretation of the right to be forgotten, a fully deletion of the personal data is impossible.[191] At present, there are three visible approaches on the right to be forgotten that let personal information to be deleted.

6.2.1 Delete the Expired Data

In general, since it is difficult ro delete personal data fully while it was published, from another perspective, it is possible to limit the accessibility of data. On this point, expiry data is one feasible measure on how to implement the right to be forgotten which

[188] Larsen, 2013, p. 13.
[189] Ibidem footnote 170.
[190] Ibidem footnote 180.
[191] Mayer-**S**chönberger, 2010, p. 1872.

essential recognised by existing techniques.[192] Victor Mayer- Schönberger, who has presented very extensive research of the right to be forgotten in his academic literature. He proposed that tag sensitive data with an expiration date, and require all data controllers abide by the expiration dates. His main proposal is to find the balance between memory and forgetting, he narrated that "introduce the concept of forgetting in the digital age through expiration dates for information."[193]

The expiration of data is a data that individuals could have a right to delete such data in due time. The right to remove expired data which may mean, when the data are no longer relevant after use or when an expiry date elapses, or when the defects of the data retention start surpassing the advantages, the data subject can invoke this right to against the data controller. Delete data which in due time can make sure that people will not worry about their information is disclosed any more and to have a new start of their information.

X-pire! system

The expired date are linked to personal data which is implenented by encrypting the data and restricting access to these data. First of all, X-pire! is a system that allow users to set an expiration date for images in social networkings.[194] It requsts to encrypt the images before uploading to the websites and stores the corresponding keys on a dedicated key server in a suitable way. If a Internet users want to view this image, a browser on this individual's machine requests the corresponding decryption key from that key server. If this data has not expired, the images could be decrypted and showed on the people's screen.[195] To some extent, the X-pire! imitates the traditional expiration of data as paper-based world by developing a digital expiration date that could corresponding to the requirement of the current information age.

---

[192] Ibidem footnote 41, pp. 128-169.
[193] Ibidem.
[194] Backes & Duermuth & Gerling *et al*, 2012, p.1.
[195] Perlman, 2005, p. 76.

Filter the data

Usually, people find and view the information on the Internet by issuing queries to a search engine or using social networkings, sharing or tagging. Since it is difficult to remove data from website completely, limit the access ability of enter into the personal data seems a more visible way to protect information from attack. Filter the data is using this way.[196] It limits the accessibility, let data are not identified by a search engine or shared, to prevent data's appearance in the results of search engines and to filter it from the severs like Google, Facebook. And under the meaning of this measure, the authorities of Member States could ask search engine operators and servers to filter the relevant information to expiration data. As a consequence, such expiration data would be very difficult to find and then become disappearance permanently.

Automatic Deletion of Data

The right to automatic deletion means give data subjects an automatic right to be forgotten after the expiration of a certain period of time. It has been proposed particularly by the EDPS. The right to be forgotten should be extended to ensure that information automatically disappears after a certain period of time, even if the data subject does not take action or even the individuals are not aware data which were stored.[197] This automatic data deletion could improve individuals' control of their own personal data. This is very important in a context of the internet where a number of data processing outside of the data subjects' sensation.[198] In this process of automatic deletion, one is necessary to ensure is a certain period of time.[199] For example, for that data stored on terminal equipment such as mobile devices or computers, data would be automatically deleted or blocked after the certain period of time if the initial owner does

[196] Ibidem footnote 31, p. 149.
[197] Ibidem footnote 169.
[198] Scheuer, & Schweda, 2011, p. 8.
[199] Ibidem footnote 52, p. 238.

not belong to equipment.

6.2.2 Do Not Track

Do Not Track (DNT) is a technology and policy proposal which was originally proposed in 2009 by researchers Christopher Soghoian, Sid Stamm and Dan Kaminsky.[200] It enables individuals users to opt out of tracking or cross-site tracking by all websites they do not visit, including social networking, advertising websites, business websites etc. Now it is currently being exercised by the Tracking Protection Working Group.[201] The mechanism of DNT is direct, the operation is when a web browser requests content or send data using Hyper Text Transport Protocol (HTTP), which is a kind of communication protocol online, it can include extra information optionally in one or more items called "headers". The header is sent out with every web request, this includes the page the user wants to view, when the user wish to opt out of tracking,[202] DNT adds a tag indicate that the user does not want to be tracked to a header. The enforcement of this DNT can only be implemented on the part of the HTTP server, so its enforcement is applied effectively using the honor system, which is a philosophical way of running a variety of endeavors based on trust, honor and honesty.[203] This measure seems more from computer realm, however, the background originated from the right to privacy, the aim of DNT is to protect Internet users can control over their own data effectively, provide a simplified and self-regulation system to prevent the data from tracking by third parties.

---

[200]Soghoian , The History of the Do Not Track Header, 22 February 2012, available at http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html (consulted on 4 May 2013).

[201]W3C Tracking Protection Working Group, 22 February 2012, available at http://www.w3.org/2011/tracking-protection/ (consulted on 29 May 2013).

[202] Ibidem footnote 169.

[203] Galperin, How to Turn on Do Not Track in Your Browser, 14 June 2012, available at https://www.eff.org/deeplinks/2012/06/how-turn-do-not-track-your-browser (consulted on 10 March 2013).

Under the context of digital information, One could request "personal data" to be deleted on one site, but meanwhile the information might have been copied already and sent to the third parties. It is quite difficult to trace all these potential third parties to delete the information that are from the primary material.[204] To address this issue, one important advantage of the DNT is the control of the information could be implemented by individual themselves, it does not need to rely on the search engines, third parties or other data controllers, the individuals will get more initiative right. In this way, it will give more control power to individual and also will be more feasible for data subjects to protect their peosonal information.[205] Under the system of DNT, when the individuals want their information be deleted, it will be much easier to enforce the right to be forgotten, because the DNT rule will not let personal data being put on other websites. However, one point we need to notice is the functioning of DNT does not prevent all internet tracking, some internet companies accept that they will not track the users' data of insurance, medical industry, but there are still maybe used in the the market research and product development.[206]

The EU try to make contributions to assessing what a right to be forgotten could and should do in practice sufficiently. It sketches out the current feasible measures to solve the obstacles of implement the right to be forgotten in this digital age must rely on a combination of technical and legal protection. Advocating that a right to be forgotten must clarify narrower and create a more comprehensive, user-control-based framework to delete both individuals' digital footprints and data shadows for the sake of a fresh start of personal data.[207]

---

[204] Ambrose, 2013, p. 409.
[205] Zhang, Do Not Track, 24 February 2012, available at http://www.ifanr.com/74499 (consulted on 18 May 2013).
[206] Ibidem.
[207] Koops, 2011, p. 229.

7. The Future of Privacy Online

Along with the increased developing tendency which makes personal information more public, especially in online environment. The individuals feel that their personal privacy is on the line.[208] The European proposed a new right to be forgotten, which manifests the determination of EU to improve the personal data protection framework, however, the most important point is to promote and advance the whole existing online data privacy mechanism to enhance the effectiveness of right implementation to comply with current situations. In order to achieve this aim, there will be a large amount of things to do in every aspects including public interests exception, third parties sharing and data authorities etc.[209]

Aim at the right to be forgotten, it is a kind of personal privacy protection. The Commission stressed the importance of strengthening individuals' control over their data as a primary objective, the right to be forgotten falls under the meaning of Commission's perspective.[210] Look at the future, firstly, it is clear that the right to be forgotten must be complemented with legal documents to guide individuals on data protection principles, and together with the adequate legal guidelines. A specification of the right to be forgotten may be achieved by more reified codes of conduct.[211] Futhermore, it would be effective if technical measures to be introduced much faster than legal instruments, and it is better that technical measures have a global scope of application that is not limited by geography.[212] Moreover, if merely based on the legal system and technical measures, it is not adequate for the right to be forgotten, because some situations would be out of reach of the legal framework and technical enforcement,

---

[208] Information Commissioner's Office, The future of data protection in Europe, 28-29 March 2012, Dexter House, London.

[209] Ibidem footnote 2.

[210] Ibidem.

[211] Weber, 2011, p. 128.

[212] Ibidem.

like it would be impossible to prevent an employee from using his phone or camera to take pictures of personal information on his or her office computer screen and the disseminate this digital form online out of the company.[213] It is also necessary to take the influence of norms, the market and code into account, because they are complementary with each other, accountable mechanisms need to be introduced and available procedures should be established on basis of the cooperative efforts.[214]

People more and more concern about their personal information and wish to have a friendly privacy online environment in the future.[215] It will be an atmosphere that individuals have the right to be able to make personal decision which is effective and be provided a more balance system than current one between individuals' privacy, businesses success and governments security.[216] The proposed new right will produce the key effect for future law in online privacy protection.[217] Dr Paul Bernal, who is specialising in internet human rights and privacy, spoke at a conference on 12th April, 2013, he maintained that a privacy-friendly internet may be possible in the future.

Firstly, although some people argue that when methods are proposed to maintain individuals' privacy against intrusive technologies or activities, it seems unworkable and will destroy the Internet. In the contrary, Dr Paul Bernal has a very confident opinion on the privacy-friendly internet. He assumed a series of internet privacy rights which are both theoretical and achievable. The rights that he put forward includes, a right to surf the internet with privacy, a right to monitor those what are monitoring us, a right to delete personal data, a right to identity, comprising right to create, claim and protect that identity, etc. Secondly, he described that the implementation of those rights might impact on the internet. He outlined how businesses might functioning within a

---

[213] Ibidem footnote 170.
[214] Bennett & Raab,2006, p.16.
[215] Science Daily, Is There a Future for a Privacy-Friendly Internet? 11 April 2013, available at http://www.sciencedaily.com/releases/2013/04/130411194657.htm (consulted on 15 June 2013).
[216] Tene & Polonetsky, 2012, p. 68.
[217] Atagana, The right to be forgotten: A path to the future, 16 May 2012, available at http://memeburn.com/2012/05/the-right-to-be-forgotten-a-path-to-the-future/ (consulted on 31 March 2013).

privacy-friendly internet and provided a number of possible new business models, including strategy, mechanisms, social networking platforms and online retail activities which inserted privacy norms and values. Thirdly, Dr Paul Bernal emphasised the obligations of authorities. The government can not relieve their responsibilities from privacy-friendly environment. Their role in building legal mechanisms not only work out the dilemmas in the present privacy framework, but also explore ways to improve and promote the mechanism, to encourage the companies respect the values of privacy as their legal operation objective.[218]

Ultimately, through all the efforts what we are doing, it is convinced that a much better online privacy system will come about in the near future.[219] More than that, to create a privacy-friendly internet environment also could evolve and promote the right to be forgotten to be implemented successfully, we need to face up to the defects that there are also some significant and urgent obstacles and barriers to be solved. We hope that within the exploring and striving, we will have a "whole gorgeous picture" of friendly online environment and personal data protection.

---

[218] Bernal, Is there a future for a privacy-friendly internet?, 12 April 2013, available at http://www.uea.ac.uk/mac/comm/media/press/2013/April/privacy-internet-rights (consulted on 1 June 2013).

[219] Young, European Data Protection Supervisor Calls For Clearer and More Privacy-Friendly Rules On Internet Intermediary Liability, 21 September 2012, available at http://www.insideprivacy.com/international/european-union/european-data-protection-supervisor-calls-for-clearer-and-more-privacy-friendly-rules-on-internet-in/ (consulted on 13 May 2013).

Conclusion:

To summarise, this thesis focuses on the new proposed right to be forgotten as a form of right to privacy to protect personal data information. It is a new field, which only gets attention from the international community, especially in EU level recently. With the development of technology in digital age, the individual privacy has become vulnerable and at risk. Because once personal information was published online, it will be not easily and fully deleted, people are increasing aware of it is pivotal to protect their personal data. On 25th January 2012, a new proposed Data Protection Regulation which include the right to be forgotten was published. In this proposed Regulation, it examines what the right to be forgotten is, constitute of the scope, limitations, obligations of data controllers, etc. Then in the light of the multi-dimensional understanding of right to privacy, the right to be forgotten could be regarded as a human right to protect personal data. Under this situation, many countries and social communities have begun to pay more attention on the right to be forgotten. Therefore, this thesis tries to pursue how the right to be forgotten will be in the future by explaining the process of the right to be forgotten and the functioning in current circumstance.

The propose Regulation is the only direct source for the right to be forgotten, however, the roots can be found in the legal framework. Originally, it was from French law "*droit à l'oubli*", which represents people have right to control over their own data. In the international conventions and treaties, there are some provisions about personal data protection and individuals' privacy rights. These legal materials can be the foundation for the right to be forgotten is written in the law in the near future. In domestic level, with the legal framework, some countries are in favor of the right to be forgotten and have had experiences to improve and advance the processing of this right in national level.

Although the EU provides a framework to the right to be forgotten in theory, the enforcement of such a right could prove to be quite problematic, especially bring challenges to those companies who operating on the Internet. To addressing this controversial issue, the EU and US have conflicting views on the application of a right to be forgotten. For example, from EU perspective, Spain Google case will be a good example to show their opinion, they maintain that individuals could invoke this right to ask their information be deleted, the ECJ's answer will be an indication which influence on the new framework in data protection. The US holds an opinion that the right to be forgotten will violate the right to freedom of expression which was written in the First Amendment and threaten the online environment.

Concerning the controversial issues discussed above in the paper, the definition of right to be forgotten is not clear to solve the practical problems. There are still a series of difficult problems around the right to be forgotten, such as what constitute of being forgotten data, who has the right to decide remove the data and under what circumstances, etc. The current system provides both legal and technical methods try to mitigate the drawbacks of the right to be forgotten in implementation. Nevertheless, it is not easy to find a sufficiently and appropriately way to carry out this challenging right in such high-speed dissemination of information. All in all, the good thing is the reform for personal data protection has began to bring more positive thinking to current situation. Although the right to be forgotten is a complicated issue and there is still further work to be done, the proposed right to be forgotten is a milestone in the path towards a structured data privacy protection and seems will make contributions to building a friendly privacy online system in the near future. We perceive the coming years to be particularly crucial whether the right to be forgotten will be seen as an incredible success on personal data protection field.

Bibliography:

Books:

Bennett, Colin J. & Raab, Charles D., *The Governance of Privacy. Policy Instruments in Global Perspective*. London: Cambridge Mass, 2006.

Brandeis, Louis D., *Other People's Money: And How the Bankers Use It.* New York: Frederick A. Stokes Company, 1914.

Flaherty, David H., *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chaper Hill: The University of North Carolina Press, 1992.

Gordon, Bell & Gemmell, Jim, *Total Recall: How the Ememory Revolution Will Change Everything.* New York: Dutton, 2009.

Griffin, James, *ON HUMAN RIGHTS.* Oxford: Oxford University Press, 2008.

Halavais, Alexander Halavais, *Search Engine Society*. Cambridge: Polity, 2009.

Lopez-Tarruella, Aurelio, *Google and the Law, Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models Copyright.* The Hague: T.M.C. Asser Press, 2012.

Mayer-**S**chönberger, Viktor, *The Virtue of Forgetting in the Digital Age.* New Jersey: Princeton University Press, 2009.

Rouvroy, Antoinette & Poullet, Yves, *Reinventing Data Protection?*. New York: Springer, 2009.

Solove, Daniel J. & Rotenberg, Marc & Schwartz, Paul M., *Privacy, Information, and Technology*, New York: Aspen, 2006.

Sykes, Charles J., *The End of Privacy: The Attack on Personal Rights at Home, at Work, On-Line, and in Court.* Wisconsin: St. Martin's Press, 1999.

Zittrain, Jonathan, *The Future of the Internet--And How to Stop It.* London: Yale University Press, 2009.

Articles in Journals:

Ambrose, Meg Leta & Ausloos, Jef, ' The Right To Be Forgotten Across the Pond', pp. 1-23, in *Journal of Information Policy,* vol.3, 2013.

Ambrose, Meg Leta, ' It's About Time: Privacy, Information Life Cycles, and the Right to be Forgotten', pp. 369-422, in *Stanford Technology Law Review*, vol. 16, no. 2, Winter 2013.

Austin, Lisa, 'Privacy and the Questions of Technology', pp. 119-166, in *Law and Philosophy*, vol. 22/2, 2003.

Ausloos, Jef, "' The Right to be Forgotten'-Worth remembering?", pp. 143-152, in

Computer Law & Security Review, vol. 28, 2012.

Bamberger, Kenneth A. & Mulligan, Deirdre K., 'Privacy on the Books and on the Ground', pp. 274-316. in *Stanford Law Review*, vol. 63, 2011.

Bernal, Paul A., 'A Right to Delete', pp. 1-18, in *European Journal of Law and Technology,* vol. 2, no. 2, 2011.

Blanchette, Jean-Fran¸cois & Johnon Deborah G., 'Data Retention and the Panopic Society; The Social benefits of Forgetfulness', pp. 33-45, in *The Information Society,* vol. 18, no. 1, 2002.

Curren, Liam & Kaye, "Revoking consent: A 'blind spot' in data protection law? ", pp. 273-283, in *Computer Law & Security Review*, vol. 26, issue 3, 2010.

Cranston M., 'Are There Any Human Rights?', pp. 1-17, in *HUMAN RIGHTS*, vol. 112, No. 4, 1983.

Dodge, Martin & Kitchin, Rob, 'Outlines of a World Coming into Existence': Pervasive Computing and the Ethics of Forgetting, pp. 431-445, in *Environment and Planning B: Planning and Design*, vol.34, 2007.

Gindin, Susan E., 'Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet', pp. 1153-1154, in *San Diego Law Review*, vol. 34, 1997.

Hugl, Ulrike., 'Approaching the Value of Privacy: Review of Theoretical Privacy Concepts and Aspects or Privacy Management', pp. 120-130, in *AMCIS 2010*

PROCEEDINGS, Paper 248, 2010.

Hayden, Ramsay, 'Privacy, Privacies and Basic Needs', pp.288-297 in *The Heythrop Journal,* vol. 51, Issue 2, 2010.

Kaufmann, Christine & Weber, Rolf H., 'The Role of Transparency in Financial Regulation', pp.779-780, in *Journal of International Economic Law*, Vol. 13/3, 2010.

Koops, Bert-Jaap, 'Forgetting Footprints, Shunning Shadows, A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice', pp. 229-256, in *Scripted*, vol 8, Issue 3, 2011.

Leaton, Gray J., 'A Right to Be Forgotten: The Far-Ranging Implications', pp. 14-16, in *Data Protection Law & Policy* , vol.8, no.5, 2011.

LESZCZEWICZ, KATARZYNA CIUĆKOWSKA, ' The Right to Be Forgotten. European Approach to Protection of Personal Data', pp. 27-36, in *UWM Law Review*, vol. 4, 2012.

Larsen, Katharine, ' Europe's " Right to Be Forgotten" Regulation May Restrict Free Speech', pp. 12-14, in *First Amendment & Media Litigation*, vol. 17, no. 1, Winter 2013.

Messenger, Ashley, 'What Would A "Right to Be Forgotten" Mean for Media in the United States?', pp. 29-38, in *Communication Lawyer*, vol. 29, Issue 1, 2012.

McNealy, Jasmine E., 'The Emerging Conflict Between Newsworthiness and the Right

to Be Forgotten', pp. 119-135, in *Nothern Kentucky Review*, vol. 39, no. 2, 2012.

Meg Leta, Ambrose & Friess, Nicole & Matre, Jill Van. 'Seeking Digital Redemption: The Future of Forgiveness in the Digital Age', pp. 99-163, in *Santa Clara Computer & High Technology Law Journal,* vol.29, no. 1, 2012.

Meg Leta, Ambrose, ' You Are What Google Says You Are: The Right to be Forgotten and Information Stewardship', pp, 22-30, in *International Review of Information Ethics,* vol. 17, 2012.

Mayer-**S**chönberger, Viktor, ' Beyond Copyright: Managing Information Rights with DRM', pp. 181-198, in *Denver University Law Review*, vol. 84, 2007.

Mayer-**S**chönberger, Viktor, ' Beyond Privacy, Beyond Rights-Toward a "Systems" Theory of Information Governance', pp. 1854-1996, in *California Law Review*, vol. 98, 2010.

Nys, Herman, Towards a Human Right ' to Be Forgotten Online', pp. 469-475, in *European Journal of Health Law*, vol. 18, issue 5, 2011.

Perlman, Radia, 'File system design with assured delete', in *Proc. 3rd IEEE International Security in Storage Workshop*, 2005.

Richards, Neil M., 'The Puzzle of Brandeis, Privacy and Speech', pp. 1295-1296, in *Vanderbilt Law Review*, vol. 63, 2010.

Ramsay, Hayden, 'Privacy, Privacies and Basic Needs', pp. 288-297, in *The Haythrop*

Journal, vol. 51, 2010.

Roosendaal, Arnold, 'Facebook tracks and traces everyone: Like This!' pp. 1-10, in *Tilburg Law School Legal Studies Research Paper Series*, no.03/2011, 2010.

Rosen, Jeffrey, ' The Right To Be Forgotten', pp. 88-92, in *Stanford Law Review Online*, vol. 64, 2012.

Reding, Viviane, 'The upcoming Data Protection Reform for the European Union', pp. 1-3, in *International Data Privacy Law Advance Access,* no. 17, 2010.

Streich, Gregory W., 'Is There a Right to Forget? Historical Injustices, Race, Memory, and Identity', pp. 525-542, in *New Political Science*, vol. 24/4, 2002.

Siry, Lawrence & Schmitz, Sandra, 'A Right to Be Forgotten?-How Recent Developments in Germany May Affect the Internet Publishers in the US', pp. 1-12, in *European Journal of Law and Technology*, vol.3, no.1, 2012.

Steven C., Bennett, 'The "Right to Be Forgotten": Reconciling EU and US Perspectives', pp. 161-195, in *Berkeley Journal of International Law*, vol. 30, 2012.

Sibble, Joshua, 'Recent Developments in Internet Law', pp. 12-16, in *Intellectual Property & Technology Law Journal,* vol. 23, no. 4, 2011.

Simón Castellano, Pere, ' The right to be forgotten under European Law: a constitutional debate', pp. 7-30, in *Lex Electronica*, vol. 16, Winter 2012.

Scheuer, Alexander & Schweda, Sebastian, ‘ The Protection of Personal Data and the Media’, pp. 1-24, in *iris plus*, 2011.

Terwangne, Cécile de, ‘Internet Privacy and the Right to Be Forgotten/Right to Oblivion’, pp. 109-121, in *Revista de Internet, Derecho y Política*, no. 13, 2012.

Tasioulas, John, ‘Taking Rights Out of Human Rights’, pp. 647-678, in *Ethics*, vol. 120, Issue, 4, 2010.

Tene, Omer & Polonetsky, Jules, ‘Privacy In the Age Of Big Data: A Time For Big Decisions’, pp. 63-69, in *Stanford Law Review Online*, vol. 64, 2012.

UOC-Huygens, ‘Net Neutrality and other challenges for the future of the Internet’, pp. 391-406, Barcelona, in *Universitat Oberta de Catalunya*, 2011.

Warren, Samuel D. & Brandeis, Louis D., ‘The Right to Privacy’, pp. 193-220 in *Harvard Law Review*, vol. IV, no. 5, 1890.

Werro, Franz, ‘The right to inform v the Right to be forgotten: A transatlantic Clash’, pp. 285-300, in *Liability in the Third Millennium,* Research Paper no. 2, 2009.

Whitman, James Q., ‘The Two Western Cultures of Privacy: Dignity Versus Liberty’, pp. 1151-1194, in *The Yale Law Journal*, vol. 113, 2004.

Walker, Robert Kirk, ‘The Right to Be Forgotten’, pp. 257-284, in *Hastings Law Journal*, December, 2012.

Walker, Kent, ‘ Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange’, pp. 1-50, in *Stanford Technology Law Review,* vol. 2, 2000.

Weber, Rolf H., ‘The Right to Be Forgotten, More Than a Pandora’s Box?’, pp. 120-130, in *jipitec,* vol. 2, 2011.

Xanthoulis, Napoleon, ‘The Right To Oblivion In the Information Age: A Human-Rights Based Approach’, pp. 84-98, in *US-CHINA LAW REVIEW,* vol. 10, 2013.

International Law Sources:

Treaties:

Charter of Fundamental Rights of the European Union (adopted 7 December 2000, entered into force 1 December 2009)

European Convention on Human Rights (adopted 4 November 1950, entered into force 3 September 1953)

The Treaty on the Functioning of the European Union (Treaty of Rome, as amended)

EU Legislation and other instruments:

Communication from the Commission to the European Parliament, the Council, the

European Economic and Social Committee and the Committee of the Regions 'A Comprehensive Approach on Personal Data Protection in the European Union' (Communication) COM (2010) 609 final, 4 November 2010.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century. COM (2012) 9 final.

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 [2008] OJ L350/60

Directive 95/46/EC of the European Parliament and of the Council of 24 Octorbor 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications sevices or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive) [2006] OJ L105/54

European Commission, 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final, 2012.

Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — 'A comprehensive approach on personal data protection in the European Union', OJ C181/01

Member States Law:

Charte du droit à l'oubli numérique dans les sites collaboratifs et les moteurs de recherche, 13 October 2010.

Federal Data Protection Act (BDSG) adopted on 14 January 2003, entered into force on 1 September 2009 last amended by Article 1 of the Act on14 August 2009.

Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure numérique, Novembre 2009.

Publications by International Organisations, NGOs, State Authorities and Online Media:

Article 29 Data Protection Working Pary, 83th plenary meeting, 13 December 2011.

BEUC, 'A Comprehensive Approach on Personal Data Protection in the European Union' European Commission's Communication, 2011.

BBC News, Google fights the Spanish privacy order in court, 20 January 2011, available at http://www.bbc.co.uk/news/technology-12239674 (consulted on 2 May 2013).

BBC news, Apple 'Not Tracking' iphone users, 27 April 2011, available at http://www.bbc.co.uk/news/technology-13208867 (consulted on 13 April 2013).

CNIL, Mission and Power, available at http://www.cnil.fr/english/the-cnil/operation/ (consulted on 1 April 2013).

CNIL, Draft EU Regulation on data protection: the defense of data protection driven apart from citizens, 31 January 2012, available at http://www.cnil.fr/linstitution/actualite/article/article/draft-eu-regulation-on-data-protection-the-defense-of-data-protection-driven-apart-from-citizens/ (consulted on 2 April 2013).

CNIL, CNIL satisfied with draft European Parliament report on the Regulation proposed by the European Commission, 16 January 2013, available at http://www.cnil.fr/english/news-and-events/news/article/cnil-satisfied-with-draft-european-parliament-report-on-the-regulation-proposed-by-the-european-comm/ (consulted on 30 March 2013).

CHARTE SUR LA PUBLICITE CIBLEE ET LA PROTECTION DES INTERNAUTES, http://www.huntonfiles.com/files/webupload/PrivacyLaw_Charte_publicite.pdf

CHARTE DU DROIT A L'OUBLI DANS LES SITES COLLABORATIFS ET LES MOTEURS DE RECHERCHE, http://www.huntonfiles.com/files/webupload/PrivacyLaw_Charte_du_Droit.pdf

Data Protection Working Party, Release Press, 29 March 2012, available at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/

(consulted on 3 April 2013).

Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, 23 March 2012, available at http://ec.europa.eu/justice/data-protection/index_en.htm (consulted on 10 February 2013).

European Commission, 'EU study on the Legal analysis of a Single Market for the Information Society, New rules for a new age?' November 2009.

European Network and Information Security Agency, The right to be forgotten—between expection and practice, 18 Octorber 2011, available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten (consulted on 27 February 2013).

ENISA, Privacy considerations of online behavioural tracking, 19 Octorber 2012, available at http://www.enisa.europa.eu (consulted on 15 May 2013).

European Economic and Social Committee Conference " Towards a more responsible use of the internet-The European civil society perspective" 6 March 2013, available at http://www.eesc.europa.eu/?i=portal.en.events-and-activities-internet-responsible-use (consulted on 30 March 2013).

European Commission, Thirteenth Annual Report of the Article 29 Working Party on Data Protection, 14 July 2010, No LX-46 01/190.

European Commision, Refrom of data protection legislation, 25 January 2012, available at http://ec.europa.eu/justice/data-protection/index_en.htm (consulted on 17 March

2013).

Federal Trade Commission, FTC Testifies Before the Senate Commerce Committee on Privacy, 16 March 2011, available at http://www.ftc.gov/opa/2011/03/privacy.shtm (consulted on 11 April 2013).

Information Commissioner's Office, The future of data protection in Europe, 28-29 March 2012, Dexter House, London.

Internet Governance Forum, IGF 2012 Workshop Proposal, (No: 111)Protecting the rule of law in the online environment, 21 April 2012, http://wsms1.intgovforum.org/content/no111-protecting-rule-law-online-environment (consulted on 31 March 2013).

London Economics, 'Study on the economic benefits of privacy enhancing technologies', July 2010, available at http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf (consulted on 12 April 2013).

Law & the Internet, Spain demands the right to oblivion for its citizens, 30 March 2011, available at http://www.blogstudiolegalefinocchiaro.com/wordpress/2011/03/spain-demands-the-right-to-oblivion-for-its-citizens/ (consulted on 12 March 2013).

Organisation for Security and Co-operation in Europe, Seventh Annual Internet Governance Forum, 7 November 2012, available at http://www.osce.org/fom/94222 (consulted on 1 April 2013).

Science Daily, Is There a Future for a Privacy-Friendly Internet? 11 April 2013, available at http://www.sciencedaily.com/releases/2013/04/130411194657.htm (consulted on 15 June 2013).

The Privacy & Information Security Committee, French DPA Launches Public Consultation on Right to Be Forgotten, 10 June 2013, available at http://thesecuretimes.wordpress.com/2013/06/10/1137/ (consulted on 15 June 2013).

The Economist, Private Data, Public Rules, 28 January 2012, available at http://www.economist.com/node/21543489 (consulted on 2 April 2013).

W3C Tracking Protection Working Group, 22 February 2012, available at http://www.w3.org/2011/tracking-protection/ (consulted on 29 May 2013).

Websites:

Atagana, Michelle, The right to be forgotten: A path to the future, 16 May 2012, available at http://memeburn.com/2012/05/the-right-to-be-forgotten-a-path-to-the-future/ (consulted on 31 March 2013).

Anderson, Nate, Spain asks: If Google search results make your business look bad, can you sue?, 17 February 2012, available at http://arstechnica.com/tech-policy/news/2012/02/spain-asks-if-googlesearch- (consulted on 12 April 2013).

Bernal, Paul, Is there a future for a privacy-friendly internet?, 12 April 2013, available at http://www.uea.ac.uk/mac/comm/media/press/2013/April/privacy-internet-rights (consulted on 1 June 2013).

Backes, Julian & Backes, Michael & Dürmuth, Markus & Gerling, Sebastian & Lorenz, Stefan, X-pire! - A digital expiration date for images in social networks, 12 December 2011, available at http://arxiv.org/abs/1112.2649 (consulted on 20 May 2013).

Black's Law Dictionary, 2009, p. 522. Dignitary Definition, Merriam-Webster.com Dictionary, available at http://www.merriam-webster.com/dictionary/dignitary (consulted on 2 May 2013).

Conley, Chris, 'The Right to Delete', in *ACLU of Northern California*, 23 March 2010, available at http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1158 (consulted on 27 February 2013).

David, Reid, France ponders right-to-forget law, 8 January 2010, available at http://news.bbc.co.uk/2/hi/programmes/click_online/8447742.stm (consulted on 28 March 2013).

Escribano, Blanca, Preliminary ruling on the right to be forgotten may be requested by Spanish Courts. The Google case, 7 March 2011, available at http://blogs.olswang.com/datonomy/2011/03/07/preliminary-ruling-on-the-right-to-be-forgotten-may-be-requested-by-spanish-courts-the-google-case/ (consulted on 5 April 2013).

El Pais, Google defies Spanish requests to hide personal information, 21 June 2012, available at http://elpais.com/elpais/2012/06/21/inenglish/1340280978_188515.html

(consulted on 8 April 2013).

Fleischer, Peter, Foggy thinking about the Right to Oblivion, 9 March 2011, available at http://peterfleischer.blogspot.be/2011/03/foggy-thinking-about-right-to-oblivion.html (consulted on 28 March 2013).

Fleischer, Peter, The Right to be Forgotten', seen from Spain, 5 September 2011, available at http://peterfleischer.blogspot.nl/2011/09/right-to-be-forgotten-seen-from-spain.html (consulted on 3 April 2013).

Galperin, Eva, How to Turn on Do Not Track in Your Browser, 14 June 2012, available at https://www.eff.org/deeplinks/2012/06/how-turn-do-not-track-your-browser (consulted on 10 March 2013).

Hendel, John, In Europe, a Right to Be Forgotten Trumps the Memory of the Internet, 3 February 2011, available at http://www.theatlantic.com/technology/archive/2011/02/in-europe-a-right-to-be-forgotten-trumps-the-memory-of-the-internet/70643/ (consulted on 27 March 2013).

Hendel, John, Why Journalists Shouldn't Fear Europe's 'Right to be Forgotten, The Atlantic, 25 January 2012, http://www.theatlantic.com/technology/archive/2012/01/why-journalists-shouldnt-fear-europes-right-to-be-forgotten/251955/ (consulted on 25 April 2013).

Hunton & LLP,Williams, French Government Secures "Right to Be Forgotten" on the Internet, 21 October 2010, available at

http://www.huntonprivacyblog.com/2010/10/articles/french-government-secures-right-to-be-forgotten-on-the-internet/ (consulted on 25 March 2013).

Hunton & LLP, Williams, Article 29 Working Party Opines on Proposed EU Data Protection Law Reform Package, 30 March 2012, available at http://www.huntonprivacyblog.com/2012/03/articles/article-29-working-party-opines-on-proposed-eu-data-protection-law-reform-package/ (consulted on 29 April 2013).

ISP Liability, Spain asks the ECJ whether Google must delete links to personal data, 2 March 2012, available at http://ispliability.wordpress.com/2012/03/02/spanish-court-asks-the-ecj-whether-google-must-delete-links-to-personal-data/ (consulted on 8April 2013).

Info. Security, Problems with the EU's proposed 'right to be forgotten,' 20 November 2012, available at http://www.infosecurity-magazine.com/view/29412/problems-with-the-eus-proposed-right-to-beforgotten (consulted on 10 April 2013).

Kroes, Neelie, "Cloud computing and data protection", 25 November 2010, available at http://europa.eu/rapid/press-release_SPEECH-10-686_en.htm?locale=en (consulted on 18 April 2013).

Kincaid, Jason, "facebook users uploaded a record 750 million photos over new year's" TechCrunch, 3 Jan 2011, available at http://techcrunch.com/2011/01/03/facebook-users-uploaded-a-record-750-million-photos-over-new-years/ (consulted on 16 April 2013).

Miller, Ron, We May Not Have a 'Right to Be Forgotten' Online, 14 March 2011, available at http://www.internetevolution.com/author.asp?section_id=1047&doc_id=204757 (consulted on 20 March 2013).

Mayes, Tessa, We Have No Right To Be Forgotten Online, 19 March 2011, available at http://www.guardian.co.uk/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet (consulted on 31 March 2013).

Pop, Valentina, EU To Press For "Right To Be Forgotten" Online, 4 November 2010, available at http://euobserver.com/social/31200 (consulted on 5 April 2013).

Rosen, Jeffrey, 'The Web Means the End of Forgetting, New York Times Magazine, 21 July 2010, http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html (consulted on 27 March 2013).

Reding, Viviane, "EU Data Protection Reform and Social Media: Encouraging Citizens' Trust and Creating New Opportunities," speech at the New Frontiers for Social Media Marketing conference, Paris, France, 29 November 2011, available at, http://europa.eu/rapid/press-release_SPEECH-11-827_en.htm (consulted on 25 March 2013).

Reding, Viviane, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age Innovation Conference Digital, Life, Design, 24 January 2012, available at http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm (consulted on 31 March 2013).

Reding, Viviane, 'Independent Data Protection Authorities: Indispensable Watchdogs of the Digital Age Meeting of the Article 29 Working Party', avaiable at http://europa.eu/rapid/press-release_SPEECH-11-863_en.htm?locale=en (consulted on 1 May 2013).

Sedler, Robert A., 'The First Amendment Right of Silence', Wayne State Univ. Law School Research Paper Series No. 07-39, 20 November 2007, available at http://papers.ssrn.com/sol3/papers.cfm?abstract-id=1031505 (consulted on 18 April 2013).

Smętek, Joanna & Warso, Zuzanna, 'The right to be forgotten-step in the right direction?' Helsinki Foundation for Human Rights, 22 Octorber 2012, available at http://www.europapraw.org/en/policy-papers/policy-paper-prawo-do-bycia-zapomnianym-wzmocnienie-autonomii-informacyjnej-czy-wprowadzenie-cenzury-w-internecie (consulted on 29 May 2013).

Soghoian, Christopher, The History of the Do Not Track Header, 22 February 2012, available at http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html (consulted on 4 May 2013).

Sullivan, Danny, Italian Court Finds Google Execs Guilty of Violating Privacy Code, 24 February 2010, http://searchengineland.com/italian-court-finds-google-execs-guilty-of-violating-privacy-code-36813 (consulted on 20 April 2013).

The "right to be forgotten," Germany, and the Wikimedia case, 4 February 2011, available at http://www.pogowasright.org/?p=20228 (consulted on 15 May 2013).

The Free Dictionary, Search and Seizure, available at http://legal-dictionary.thefreedictionary.com/Reasonable+expectation+of+privacy (consulted on 1 June 2013).

US Government and Internet Giants Battle EU over Data Provacy Proposal, 17 Octorbor 2012, available at http://www.spiegel.de/international/business/us-government-and-internet-giants-battle-eu-over-data-privacy-proposal-a-861773.html (consulted on 25 April 2013).

Young, Mark, European Data Protection Supervisor Calls For Clearer and More Privacy-Friendly Rules On Internet Intermediary Liability, 21 September 2012, available at http://www.insideprivacy.com/international/european-union/european-data-protection-supervisor-calls-for-clearer-and-more-privacy-friendly-rules-on-internet-in/ (consulted on 13 May 2013).

Zhang, Chuan, Do Not Track, 24 February 2012, available at http://www.ifanr.com/74499 (consulted on 18 May 2013).

Interview:

Interview with Navi Pillay, United Nations High Commissioner for Human Rights, Office of the United Nations High Commissioner for Human Rights, Leuven, 21 May 2013.

Cases:

Butterworth v Smith, 494 U.S. 624, 634 (1990)

Case C-468/11 Commission v Spain OJ C 340

Cohen v. Cowles Media, 501 U.S. 663, 672 (1991)

Olmstead v United States, 277 US 438, 478 (1928)

Smith v Daily Mail Publishing Co., 443 U.S. 97 (1979)

Stacy Snyder v Millersville University, J. Barry Girvin, DR. Jane S. Bray and DR. Vilas A. Prabhu Case 2:07-cv-01660-PD

The Florida Star v B. J. F., 491 US 524 (1989)

Von Hannover v Germany (App no 59320/00) ECHR 24 September 2004