FACULTY OF LAW
Lund University

Sanna Kulevska

Humanizing the Digital Age:

A *Right to Be Forgotten* Online?

An EU – U.S. Comparative Study of Tomorrow's Privacy in Light of the General Data Protection Regulation and *Google Spain v. AEPD*

Abstract

Focusing on the right to be forgotten – as provided for by Article 17 of the General Data Protection Regulation as well as in the recent ruling in *Google Spain v. AEPD* – this thesis investigates the issue of responsibility for websites and search engines to erase personal data. It presents the transatlantic clash regarding privacy laws and freedom of expression laws, and investigates the enforcement challenges of such a right in both the EU and the U.S.A. This thesis proposes that a right to be forgotten must be narrowed and reconceptualized to better fit our global differences, and suggests non-legislative solutions to better find a balance between online privacy and freedom of expression. One consistent theme in this thesis is an analysis of the shift from human forgetting to flawless digital remembering, while stressing the need to protect our digital persona in the attempt to humanize the digital age.

JURM02 Graduate Thesis
Graduate Thesis, Master of Laws Programme
30 Higher Education Credits

Supervisor: Professor Hans Henrik Lidgard
Semester: VT 2014

Table of Contents

Summary

Rapid technological developments and globalisation have profoundly changed the way people entrust their personal data to social media websites and search engines. As a result, the European Commission has proposed a General Data Protection Regulation (GDPR), to enhance online privacy rights for the citizens of the European Union. As the GDPR will most likely enter into force in 2016, one of the major extensions from the existing Directive 95/46/EC is the so-called *right to be forgotten*. This implies a right for data subjects to request data controllers to delete all personal data related to them on the Internet, or to remove search results linking to their personal data. The right to be forgotten raised intense discussions in the media on May 13, 2014, when the Court of Justice of the European Union in *Google Spain v. AEPD* interpreted Directive 95/46/EC as granting EU citizens such a right against search engines. As many EU citizens engage in the daily use of these services provided by U.S. online companies, this paper scrutinizes, in a fashion comparing the EU and the U.S.A, how the differentiating attitudes towards privacy and freedom of expression will challenge the implementation of a right to be forgotten in the EU. This thesis also investigates whether such a right could exist in the U.S.A., given that the freedom of expression historically has prevailed in privacy cases. The right to be forgotten will most likely lead to an enhanced transatlantic clash with regard to personal data protection, and this thesis questions whether the U.S.–EU Safe Harbor Agreement is still viable in the wake of *Google Spain v. AEPD* and the upcoming GDPR.

This potentially broad conflict is in fact an existing issue within the EU. It is considered in Article 17(3) of the GDPR, where freedom of expression is stated, in a somewhat unspecific manner, as an exception from erasure. EU Commissioner Viviane Reding stated that "there is no right that is absolute. A right always goes as far as it can until it comes in conflict with another right." The purpose of this thesis is to find out how far a right to be forgotten can be extended before it interferes with freedom of expression. This thesis concludes that the proposed right to be forgotten needs to be narrowed, and that the only feasible extension of such a right appears to be to solely permit deletion of content posted by the data subjects themselves. An application any broader in nature might violate the right of freedom of expression, and risk putting an equal sign between privacy and online censorship. This thesis therefore scrutinizes the great responsibility requirement for websites and search engines, provided for in Article 17(2) of the GDPR and in *Google Spain v. AEPD*, to hide or delete lawful and legitimate content. One complicating factor is the enforcement process for the proposed right. The process does not appear to be satisfactorily worked out by the European Commission, since erasure of this magnitude will be *technically* hard to pursue. To humanize the digital age, where a flawless digital memory is the new default and the proposed right to be forgotten appears to be practically hard to enforce, this thesis proposes non-legislative solutions. These alternative solutions, such as best practice agreements, contextualization, and cognitive adjustment, will work to not only protect our digital persona, but will better balance the competing rights of privacy and freedom of expression.

Sammanfattning

Eftersom snabb teknisk utveckling och globalisering har förändrat sättet på vilket vi anförtror oss personuppgifter till webbplatser för sociala medier samt sökmotorer, har den Europeiska kommissionen föreslagit en ny dataskyddsförordning som kommer att förbättra skyddet för den personliga integriteteten på internet för medborgarna i EU. Då den med stor sannolikhet träder i kraft år 2016 kommer ett av de stora tilläggen från det nuvarande dataskyddsdirektivet 95/46/EC att vara den så kallade *rätten att bli bortglömd*. Det innebär en rätt för individer att kräva av sociala medier och andra innehavare av personlig data att radera personlig information. Den 13 maj 2014 kom en tolkning av detta direktiv genom EU-domstolens dom i målet *Google Spain v. APED,* som gav medborgarna i EU en sådan rätt gentemot sökmotorer. Eftersom många EU-medborgare dagligen använder kommunikationsplattformar som tillhandahålls av amerikanska företag, granskar denna uppsats hur de differentierande attityderna till personlig integritet och yttrandefrihet i EU och USA kommer att försvåra genomförandet av en rätt att bli bortglömd i EU. Denna uppsats undersöker också om en sådan rätt kan existera i USA, där den personliga integriteten historiskt sätt fått lämna företräde åt en mycket stark yttrandefrihet. Rätten att bli bortglömd kommer sannolikt att innebära en förstärkt transatlantisk konflikt gällande dataskyddsnivån för EU-medborgarna vars data kontrolleras av amerikanska företag, och frågan är nu hur livskraftiga avtalsvillkoren numera är i ”Safe Harbor”-avtalet mellan USA och EU.

Konflikten mellan rätten till privatliv och yttrandefrihet har beaktats i den nya dataskyddsförordningen, där yttrandefriheten i artikel 17(3) anges som ett undantag från rätten att bli bortglömd. EU-kommissionär Viviane Reding yttrade att “det finns ingen rättighet som är absolut. En rättighet gäller alltid i den möjliga mån tills den kommer i konflikt med en annan rättighet.” Syftet med denna uppsats är att undersöka hur *utvidgad* en individs rätt att bli bortglömd kan göras innan den kolliderar med en annan individs yttrandefrihet. Olika nivåer av radering undersöks och den enda möjliga vidgningen av rätten att bli bortglömd tycks vara att tillåta radering av innehåll som publicerats av individen själv. En bredare tillämpning av rätten att bli bortglömd skulle kränka yttrandefriheten och risker att sätta ett likhetstecken mellan integritet och censur på internet. En intressant fråga som granskas i denna uppsats är därför det stora ansvaret för hemsidor enligt artikel 17(2) i dataskyddsförordningen att radera lagligt och legitimt innehåll från internet, samtidigt som de har en skyldighet att tillgodose ett öppet forum med utrymme för yttrandefrihet. En komplicerande faktor är att den verkställande processen för en rätt till radering inte tycks vara tillfredsställande utarbetad av den europeiska kommissionen, då en rätt till radering av denna magnitud kommer vara tekniskt svår att fullfölja. För att möjliggöra en humanisering av den digitala tidsåldern, där ett felfritt digitalt minne är den nya standarden och en rätt till radering i så vid bemärkelse praktisk svår att genomdriva, föreslås i denna uppsats icke-juridiska sätt att skydda vårt digitala rykte som bättre balanserar personlig integritet och yttrandefrihet på internet. Exempel på sådana alternativa lösningar är frivilligt utarbetade standarder för internetmarknadens ledande företag, kontextualisering och kognitiv anpassning.

Preface

In this paper I consider the physiology of the brain in the context of a right to be forgotten, since our human brains are constructed to forget. The human brain only remembers things that are of great importance to us.[1] Important to me for the writing of this paper are all the inspiring conversations that I have had with people who share my passion for Internet law in general and who have a curiosity for the right to be forgotten and data protection in particular. I would like to express my gratitude to my supervisor at the Faculty of Law at Lund University, Professor Hans Henrik Lidgard, for helping me with the structure of my argument in this paper. I would also like to thank Michael Rustad, the Thomas F. Lambert Jr. Professor of Law at Suffolk University Law School in Boston, who mentored me and encouraged me to study global Internet law developments while I was a visiting student. I further developed my comparative perspective of U.S. versus European law in his course in Internet Law and Global Technology at Suffolk University Law School. Furthermore, I would like to address my deepest gratitude to the Berkman Center for Internet and Society at Harvard Law School, where I worked as a Research Intern in the Chilling Effects Clearinghouse. During my time at the Berkman Center, I had many very important discussions about the degrees of deletion with my supervisor Adam Holland, as well as other lawyers, professors, engineers and media specialists at this renowned center for global Internet law and policy.

In addition, I would like to thank all the people that I have interviewed or had specific conversations with for this paper: Lewis Hyde, the author of the world renowned book *Common as Air*, Christopher Gibson, Professor and Associate Dean at Suffolk University Law School in Boston, Ulf Maunsbach, Professor at the Faculty of Law at Lund University, the EU official (who desires to be anonymous), who has been involved in the development of the proposal to the GDPR, and David Larochelle, Lead Engineer for the Media Cloud at the Berkman Center for Internet and Society at Harvard Law School. It has been very rewarding and important to get a window into the world of the human, legal, political and technological aspects of deletion with these world-recognized experts. Many thanks also to Brendan Bresnahan, Erl Burns, Johannes Jungschaffer, Louis Grube, Sophie Kulevska, and Tahlil McGough, legal professionals, as well as Carolina Ignell, language expert, for proofreading different chapters of this thesis before publication. Finally, I am extremely thankful for the support and love of my wonderful family during my five years of law studies. I will forever be grateful for their steadfast and consistent encouragement of my studies.

Eslöv in May, 2014,
Sanna Kulevska

[1] VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 16 (2009).

Abbreviations

AEPD	Agencia Española de Protección de Datos (Spanish Data Protection Authority)
AmCham EU	American Chamber of Commerce to the European Union
CDA	Communications Decency Act
CJEU	Court of Justice of the European Union
DMCA	Digital Millennium Copyright Act
ECHR	European Convention of Human Rights
EDPS	European Data Protection Supervisor
EFF	Electronic Frontier Foundation
ENISA	European Union Agency for Network and Information Security
EU	European Union
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
IDC	International Data Corporation
ISP	Internet Service Provider
LIBE	Civil Liberties, Justice and Home Affairs Committee of the European Parliament
MIT	Massachusetts Institute of Technology
NSA	National Security Agency
OECD	Organization on Economic Co-Operation and Development
PRISM	Planning Tool for Recourse Integration Synchronization Management
TFEU	Treaty of the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
U.S.A.	United States of America
U.S.C.	United States Code

Definitions

Data controller refers to any "natural or legal person, public agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data".[2]

Data subject is defined as "any identified person or person who could be identified using reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person".[3]

In this thesis, the term "digital persona" is given a meaning comparable to "online reputation" or "digital identity". I use it to describe the implications of how a data subject portrays him or herself, or is portrayed by other data subjects, on the Internet. In this thesis, this term mainly refers to posts on social network sites, blogs or articles.

Personal data is defined as "any information by which a data subject could be identified".[4] Examples include names, date of birth, photographs, video footage, email addresses, telephone numbers, and communications content.[5]

Internet Service Provider (ISP) is defined as "an entity offering transmission, routing, or providing connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received" or "a provider of online services or network access, or the operator of facilities thereof".[6] Included are, for example, search engines, bulletin board operators, and auction web sites.[7] Social network sites like Facebook might also become an ISP in the future.[8]

---

[2] 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 the Free Movement of Such Data.
[3] European Commission, Proposal for a Regulation of the European Parliament and of the Council, on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) COM(2012) 11 final, 2012/0011 (COD), January 25, 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF [hereinafter *General Data Protection Regulation*].
[4] *Id.*
[5] Press Release, European Data Protection Supervisor, Urgent Reform of EU Data Protection Framework is Essential for a Connected Continent, EDPS/2014/02 (Jan. 16, 2014), http://europa.eu/rapid/press-release_EDPS-14-2_en.htm [hereinafter *Press Release, European Data Protection Supervisor*].
[6] 17 U.S. Code § 512 (k)(1)(A)-(B) limitation on liability relating to material online.
[7] The Chilling Effects Clearinghouse, Berkman Center for Internet and Society, http://www.chillingeffects.org/dmca512/faq.cgi (last visited May 10, 2014).
[8] Gary Kim, *Facebook Will Be an Internet Service Provider,* TECHZONE360, March 4, 2014, http://www.techzone360.com/topics/techzone/articles/2014/03/04/372188-facebook-will-be-an-internet-service-provider.htm.

1 Introduction

1.1 Background

Stacy Snyder was a 25-year-old student in her final year of college whose career aspiration was to become a teacher. She had completed her education and practical training with many honors, but was nevertheless dismissed from her university because of a post on a social media website that university officials thought to be improper for a teacher of young persons. Stacy Snyder had posted pictures of herself wearing a pirate's hat and drinking liquor from a plastic cup. The picture was captioned "drunken pirate".[9] When Stacy Snyder desired to have the picture taken down from the web, the damage was already done. Her picture had been spread across the Internet and archived by search engines.[10] She filed a lawsuit against the university, but her dismissal was upheld.[11]

The Internet has enabled new connections, such as those on social media. But the seamy side of the interconnected world is that this information technology poses new threats to privacy. The European Commission published its Eurobarometer survey that concludes that nearly three out of four respondents see inadvertent and deliberate disclosures of personal data as an "increasing part of modern life".[12] Facebook reported in 2011 that each day four billion "things" were publicly shared on their website and Twitter announced that users tweeted 200 million times per day.[13] For Stacy Snyder, the posting of a seemingly innocuous picture led to her dismissal from a university derailing her goal of becoming a teacher. With the rise of the Internet and social media, this wholesale invasion of privacy is increasingly becoming routinized. For many in Generation Connected, the harm suffered to Stacy Snyder is not an isolated case study.[14]

Unlike the human brain with its imperfections and forgetfulness, the web has a flawless memory and remembers everything we do.[15] Although 72 percent of the European citizens are concerned that their personal data may be abused or

---

[9] MAYER-SCHÖNBERGER, *supra* note 1, at 1.
[10] *Id.*
[11] FREDRIK ALVERÉN, SÅLD PÅ NÄTET – PRISET DU BETALAR FÖR GRATIS (2012) at 193.
[12] Press Release, European Commission, Data Protection: Europeans Share Data Online, but Privacy Concerns Remain – New Survey (June 16, 2011), http://europa.eu/rapid/press-release_IP-11-742_en.htm. [hereinafter *Press Release, European Commission, Data Protection*].
[13] Twitter Engineering, *200 Million Tweets Per Day,* TWITTER BLOG (June 30, 2011), http://blog.twitter.com/2011/06/200-million-tweets-per-day.html.
[14] Press Release, European Commission, Commission Proposes a Comprehensive Reform of EU Data Protection Rules (Jan 25, 2012), http://ec.europa.eu/avservices/video/player.cfm?ref=82655. [hereinafter *Press Release, European Commission, Proposes a Comprehensive Reform*].
[15] MAYER-SCHÖNBERGER, *supra* note 1, at 13.

misused by online companies, such as Facebook and Google,[16] it is difficult to measure the radius of the risk that personally identifiable information has if it goes viral. Social networks offer entertainment for free in return for the right to appropriate personal data of their customers. For years, data subjects have paid with their privacy and with the risk of a permanent record on the Internet.
Until now.

In January 2012, the European Commission proposed the General Data Protection Regulation (GDPR) as a legal response to the rapid pace of technological development and increased globalization, which has profoundly changed the way our personal data is being used and accessed.[17] The newly minted Regulation aims to strengthen online privacy rights for the citizens of the European Union (EU). One of the major expansions from the Data Protection Directive of 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46/EC)[18] is the so-called *right to be forgotten* provided for by Article 17: "If an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system".[19] The rather unspecified right to be forgotten provides for an opportunity to get a "clean slate" and it may be seen as "socially beneficial to encourage individuals to reform their lives [and therefore not] be barred by their past 'mistakes'" when entering into social and economic life.[20] On May 13, 2014, the Court of Justice of the European Union (CJEU) ruled in *Google Spain v. AEPD* that data subjects will now have a right to ask Google and other search engines to delete links connected to them in a Google search on their names – even if the content has not been removed from the original website and although it was lawfully published.[21]

On the contrary, a right to be forgotten could potentially lead to a censoring of the Internet when forcing search engines or websites to erase personal data, which would have impeded effects on freedom of expression. Different attitudes towards the fundamental rights of privacy and freedom of expression have led to a transatlantic clash between the EU and the United States of America (U.S.A.), and it may now be a good time to stop and think about what the different legal systems can lead to in a united cyberworld, and what

---

[16] *Press Release, European Commission, Proposes a Comprehensive Reform, supra* note 14.
[17] European Commission, 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, EUR-Lex (Jan. 25, 2011), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012DC0009:en:NOT.
[18] Directive 95/46/EC, *supra* note 2.
[19] Press Release, European Commission, EU Justice Commissioner, EU Data Protection Reform and Social Media: Encouraging Citizens' Trust and Creating New Opportunities SPEECH 11/827 (Nov. 29, 2011), http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/827&type=HTML [hereinafter *Press Release, European Commission, EU Data Protection Reform*].
[20] ALAN F. WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD KEEPING, AND PRIVACY 267 (1972).
[21] Case C-131/12 *Google Spain v. AEPD* [2014] n.y.r.

potential consequences a right to be forgotten may have in our society – both online and offline.

1.2 Purpose and Question Formulations

The purpose of this thesis is to compare the privacy rights in the EU and the U.S.A., and to investigate, based on the uncertain writing of Article 17 of the GDPR and the ruling in *Google Spain v. AEPD*, the limitations of as well as the responsibility for a right to be forgotten, and how such a right can best be balanced with freedom of expression.

Relevant questions for this purpose are the following:

- What is the importance of remembering and forgetting in the digital age?
- What does the current landscape of privacy law and freedom of expression law look like in the EU and the U.S.A.?
- Can a right to be forgotten exist in the U.S.A.?
- To what *extent* is it currently feasible to extend a right to be forgotten according to Article 17 of the GDPR without violating the freedom of expression online?
- Is the U.S. - EU Safe Harbour Agreement[22] still a viable compromise?
- Who may be held *responsible* for a right to be forgotten under Article 17 of the GDPR and according to the CJEU decision in *Google Spain v. AEPD*?
- Is *legislation* the best way of enacting a right to be forgotten, or are there any non-legal ways that will better balance privacy with freedom of expression while still protecting our digital persona?

1.3 Method and Material

The primary method that I have used while researching the right to be forgotten has not been a traditional legal dogmatic method, but more a *normative discourse* consisting of an examination and analysis of statutory sources, case law, legal doctrine, scholarly articles, and interviews. Due to the incredibly relevant nature of this subject and the fact that the right to be forgotten has not yet been enacted as a law, there is unfortunately no well-developed case law regarding the right to be forgotten. The above mentioned sources will therefore be supplemented by commentary and examples drawn from blogs and the popular press in order to keep the information as up to date as possible.

Since the Internet is global, a right to be forgotten would have an extraterritorial impact beyond the borders of the EU. I have therefore used a

[22] U.S. Department of Commerce, U.S. – EU Safe Harbor Agreement (2000), http://export.gov/safeharbor/ [hereinafter *U.S.-EU Safe Harbor Agreement*].

comparative method in this thesis to enable a comparison between the privacy regulations in the U.S.A. and the EU, with a particular view to whether a right to be forgotten could exist without violating a strong freedom of expression right. The material needed when making this comparison consist of case law, directives, proposals for new legislation, and doctrine from the EU, as well as statutory text, case law, proposals for new legislation by the Obama Administration, hearings from the Federal Trade Commission (FTC), and legal doctrine from the U.S.A. Since there is no federal right to be forgotten in the U.S.A., there is no case law considering such a right. To enlighten the different and comparative attitudes towards the right to be forgotten, I have conducted interviews with law professors from the U.S.A. and the EU (Sweden).

To enable thorough research on the right to be forgotten and its effects on the freedom of expression, a plain legal perspective was not sufficient to answer the questions presented above. Influences from a *legal philosophy* perspective when considering the questions of forgetting and remembering could not be left out. I have used it to contrast the imperfect human memory and the flawless digital memory. With regard to this, the work of Viktor Mayer-Schönberger,[23] Professor of Internet Governance and Regulation at Oxford University, has been a great inspiration for the consistent theme of the paper: the humanization of the digital age. Also, it was necessary to at least raise the larger practical and political questions in implementing this new transborder right for data subjects. To include the political angle, I interviewed an EU-official in Brussels who was involved in the development of the proposal for a right to be forgotten, as provided for in the GDPR.

To get a full understanding of the right to be forgotten, I interviewed a Lead Engineer at the Berkman Center for Internet and Society at Harvard Law School, which enriched this thesis with a discussion of the *technical* aspect of deletion. I want, however, to emphasize the fact that the interviews are no basis for any facts, but merely used to illustrate opinions from experts in their respective areas connected to the right to be forgotten.

1.4 Delimitations

Due to the limited scope of this thesis, several delimitations have been made. First, since the GDPR aims to enhance the privacy rights of the EU citizens, whose data is being processed mainly by U.S. based websites, this paper merely focuses on the legal systems in the EU and the U.S.A.

The proposed GDPR consists of a new regulation and a new directive. The proposed regulation focuses on data protection and the processing of personal data and the free movement of such data. The proposed directive comprises protection for individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the

[23] *See* MAYER-SCHÖNBERGER, *supra* note 1, at 20.

free movement of such data.[24] I have chosen to limit my research to the proposed regulation and specifically Article 17, the right to be forgotten and to erasure.[25] More specifically, the focus in this thesis is on deletion of *accurate* information that has been *lawfully* posted on the Internet, which excludes potential defamation claims, which are based on *false* information. There are many exceptions to obtain a right to be forgotten. Of most interest for the purpose of this thesis is Article 17(3)(a). It underlines the desired balance between a right to be forgotten and freedom of expression online.

The focus in this paper is merely on the personal information that data subjects make public through self-disclosure, meaning an active choice to share posts, tweets, and the like. In some cases these posts are made available through third parties, for example when journalists or other data persons are writing *about* the data subject.[26] I have chosen to define this type of information as "active" user data, as oppose to "passive" user data, which is information collected *about* the data subjects through search quires, collection of cookies and similar, in the attempt to track online behavior and to enable so called *profiling*.[27] A highly relevant issue in the field of *passive* user data is companies' use of metadata in generating databases with millions of data subjects, and whether there are possibilities for data subjects to erase their profile included in a larger database. Since my paper merely focuses on *active* user data I encourage other researchers to further investigate this emerging potential privacy breach.

1.5 Research Position

The right to be forgotten and its balance with freedom of expression is a timely topic because the right to be forgotten was proposed in 2012 and will most likely go into effect in 2016. This is even more true since the ruling in *Google Spain v. AEPD* provided for a right to be forgotten already before the implementation of the new law, solely based on Directive 95/46/EC. Since European users are to a great extent using online services created by U.S. companies, the EU-U.S. comparative perspective on the right to be forgotten is important. This paper investigates how far a right to be forgotten can be extended before it overtakes freedom of expression rights, as well as the transatlantic clash of privacy and free speech resulting from the fact that EU attempts to protect its citizens against material under U.S. control. Prior researchers have suggested that the centrality of the clash between expression and the right of erasure needs further investigation.[28]

The issue of who is responsible for erasure has not been addressed in prior studies, and since *Google Spain v. AEPD* became public on May 13, 2014, this

[24] *General Data Protection Regulation, supra* note 3.
[25] Hereinafter only referred to as "the right to be forgotten"
[26] Information that you, for example, can find through search engines, or social network posts of others.
[27] ALVERÉN, *supra* note 11, at 172.
[28] Napoleon Xanthoulis, *Right to Oblivion in the Information Age: A Human-Rights Based Approach,* 10 US-China L. Rev. 84, 2013, at 98.

thesis will be the first to shed light on how the right to be forgotten will be interpreted.

To better understand a right to be forgotten in the digital age, it is of great importance to investigate remembering and forgetting from a human perspective. The combination of the philosophic viewpoint and the legal, political and technical research adds a distinct character to this thesis.

1.6 Outline

To be able to constructively answer the questions presented above, this thesis is, except for the introduction and the finalizing analysis, divided into three major sections. Each chapter starts with an introduction to the chapter and ends with a short summary containing the most important information presented in the chapter.

The *first* section focuses on data sharing from a philosophic perspective of **remembering and forgetting in the digital age.**

The *second* section, consisting of chapter three and four, investigates whether there is any room for a right to be forgotten in the EU and the U.S.A., by discussing **the transatlantic clash** between privacy law and free expression rights. *Google Spain v. AEPD* will be presented, and the viability of the EU-U.S. Safe Harbor Agreement in the wake of the decision in the case as well as the upcoming GDPR is questioned.

The *third* section aims to find common grounds between the EU and the U.S.A. It focuses on the **enforcement of the right to be forgotten**. It investigates the responsibility issue and whether there are any alternatives to a right to be forgotten that can create a better balance between privacy and freedom of expression in our global online network.

This thesis ends with my own analysis of whether a right to be forgotten is the best way to protect our digital persona in the attempt to humanize the digital age, or if there are other ways to find a balance between online privacy and freedom of expression. To make it easier for the reader to follow my analysis, it follows the same three-part structure as the main research and aims to analyze the questions presented above and answered throughout the whole thesis.

2 Remembering and Forgetting in the Digital Age

2.1 Introduction to the Chapter

This chapter aims to give the reader a human perspective to why we need a right to be forgotten. By giving a philosophical view of the duality of the human memory, it presents the dilemma of adapting to an increasing amount of information in cyberspace and a digital ever-lasting memory, when our human brains are actually programmed to forget.

2.2 Information Overflow

Eric Schmidt, Executive Chairman of Google has stated that we are creating the same amount of information every second day as we did from the beginning of our time up until 2003.[29] In 2005, the stored volume of data in the world was 10 extrabytes per year. One extrabyte is a billion gigabytes, or a million terabytes, or one billion billion gigabytes. This huge volume of information is merely information that we *add* to the global digital memory every year, and there is an estimated annual growth of about 30 percent. The International Data Corporation (IDC),[30] one of the most prominent global market intelligence companies, stated in their 2011 report that the world created information in 2011 was 1.8 zettabyte. This equals 1.8 billion gigabytes, which is nine times more than the amount of data we had on the Internet in 2005. IDC also stated that the cost for creating, collecting, handling and saving all this information has decreased to one sixth of the cost in 2005.[31]

2.3 Forgetting is Easy and Remembering is Hard?

In the past when analog information was our only choice, it was both expensive and hard to store data. It was hard to *remember*. Viktor Mayer-Schönberger argues that digitalization, cheap storage, easy retrieval, and global reach have reversed this thinking and we are now facing the opposite: "Our pasts are becoming etched like a tattoo into our digital skins".[32] Furthermore, it has been said: "We used to have a system in which we forgot things easily and had to invest energy in remembering… Now we're switching to a system in which we remember everything and have to invest energy in order to forget. That's an

[29] M G Siegler, *Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up To 2003,* TECHCRUNCH, (Aug. 4, 2010), http://techcrunch.com/2010/08/04/schmidt-data/.
[30] The Internet Data Corporation, IDC, https://www.idc.com/ (last visited April 13, 2014).
[31] ALVERÉN, *supra* note 11, at 188-189.
[32] MAYER-SCHÖNBERGER, *supra* note 1, at 52.

enormous transformation."[33] Technologies are making the past easily and eternally present.[34] The social networks are creating a society where users can never "unring the bell", since remembering, as opposed to forgetting, is the new default.[35]

Before Web 2.0[36] was introduced in 2000, the Internet was a tool to *access* information, rather than *sharing* information.[37] Today, 75 percent of the teenagers in the U.S.A. use the Internet to create and share information with others.[38] Through global reach, information can be spread more quickly and over a broader area than in the analogue age, when we more commonly relied on individual and oral communication. Even if digitalization has made copying and sharing easier, it has also made it less controllable and impossible to recall or stop others from using it.[39]

To better understand the role of remembering and the importance of forgetting in the digital world, it is vital to investigate the mechanisms behind the *human* memory. For human beings, forgetting is easy and remembering is hard. This way we can grow and change without being linked to our past for eternity: "We can forgive and forget."[40] Forgetting helps us to reconstruct the truth, to generalize and to abstract.[41] The human brain is complex and consists of a hundred billion neurons that process information.[42] We only use a fraction of the brain's possible power, but despite this, our gigantic network of synapses would easily be overwhelmed if we started to process and store every single stimulus we receive.[43] Many people recognize the feeling of trying to recall the name of an old friend. You have failed to remember, and you have forgotten.[44] Neuroscientists and psychologists have been debating for a long time what it means to forget information stored in our long-term memory. Some scholars think that forgetting is not about losing the information itself, merely the link to it. This is comparable to a search online for something that cannot be found because there are no longer any links connected to this information. It is forgotten.

---

[33] Jessica Winter, *The Advantages of Amnesia*, THE BOSTON GLOBE (Sept. 23, 2007), http://www.boston.com/news/globe/ideas/articles/2007/09/23/the_advantages_of_amnesia/?page=full.
[34] A.L. Allen, *Dredging up the Past: Lifelogging, Memory, and Surveillance,* 75 U.Chi. L. Rev. 47 (2008).
[35] Chris Conley, *The Right to Delete*, ACLU of Northern California, at 53.
[36] The term Web 2.0 was coined in 1999 by Darcy DiNucci and is often described as the new web, which allows users to interact and collaborate with each other, as opposed to the old web sites where people were limited to passive viewing of content. Examples of Web 2.0 sites are social networking sites and blogs.
[37] MAYER-SCHÖNBERGER, *supra* note 1, at 85.
[38] Kathryn Zickuhr, *Teen Content Creators*, PEW RESEARCH INTERNET PROJECT (Nov. 18, 2009), http://www.pewinternet.org/2009/11/18/teen-content-creators/.
[39] MAYER-SCHÖNBERGER, *supra* note 1, at 87.
[40] *Id.* at 88.
[41] *Id.* at 117.
[42] *Id.* at 16.
[43] STEVEN W. SMITH, THE SCIENTISTS AND ENGINEER'S GUIDE TO DIGITAL SIGNAL PROCESSING 352 (1997).
[44] MAYER-SCHÖNBERGER, *supra* note 1, at 16.

The Harvard professor Daniel Schacter has criticized the theory on the human brain as a deterministic biological computer, but instead stated that forgetting depends on how frequently we recall a particular incident and of how much of important it was to us. In this way our past changes depending on our own memory of it.[45]

2.4 Remembering – A Questionable Virtue

The defects of the human memory allow us to abstract and generalize our present time, but how would it be if our brains did not have these defects and enabled us to remember everything? A study of a woman with superior memory made at the University of California, shows that even if she remembered exactly every detail of her life since the age of eleven, she was not happier or more successful in her professional career. The only difference is that she spends a lot time immersed in her past instead of enjoying the present.[46]

> I remember good, which is very comforting…but I also remember bad-and every bad choice. And I really don't give myself a break. There are all these forks in the road, moments you have to make a choice, and then it's ten years later, and I'm still beating myself up over them. I don't forgive myself a lot of things. Your memory is the way it is to protect you. I just feel like it just hasn't protected me. […] Most people have called what I have a gift, but I call it a burden.

She underscored that people tend to think of forgetting as an affliction and are disturbed by the loss of so much memory as they age, but that there is a real value of being able to forget a good deal about our lives.[47] Through the use of digital memory, we undermine biological forgetting. This way we make ourselves vulnerable to indecision, which may affect our ability to act in time without thinking about future implications of our actions since we know that what we say or do on the Internet today will remain the same forever.[48] Digital memory rejects the human capacity to learn from mistakes, to grow and to change.[49] Mayer-Schönberger fears that permanent remembering creates a situation where we will be tempted to self-censoring, which, in the end, will prevent us from developing.[50]

We are nowadays used to search engines recording our searches to improve their performance. As do social networks when they collect our status updates or tweets. These personal comments are later on turned into permanent records.[51] The fact that we will be forever remembered on the Internet reconstructs our behavior. If the aspiring teacher, Stacy Snyder, would have

[45] *Id.* at 19.
[46] *Id.* at 21.
[47] *See* Joshua Foer, *Remember This*, THE NATIONAL GEOGRAPHIC MAGAZINE (Nov. 2007), http://ngm.nationalgeographic.com/print/2007/11/memory/foer-text.
[48] MAYER-SCHÖNBERGER, *supra* note 1, at 117.
[49] *Id.* at. 125.
[50] *Id.* at 109.
[51] Conley, *supra* note 35 at 55.

understood the accessibility quality of digital remembering – implying that the information available at one point in life for a specific group of people might in the future be available for other people who has got a fundamentally different purpose[52] – she would most likely have been more restrictive and thought twice before posting a picture of her as a "drunken pirate".[53]

The clue is simple and described by Mayer-Schönberger the following way: "If one abstains from putting personal information online, one does not have to fear the consequences of an enduring digital memory such as loss of control and power over information."[54] An important question here is if we really want to stay away from online interactions with others in fear that this interaction may forever be remembered. The following chapter presents privacy rights in the EU with focus on a right to be forgotten.

2.5 A Short Summary of the Chapter

- In the transformation from analogue to a digital communication, remembering, as opposed to forgetting, has become the new default.
- The inability for the flawless digital memory to forget might lead data subjects to self-censoring and a feeling of lost control over their personal data.
- There is a great need to find a way to challenge the flawless digital memory that will mimic the human brain of forgetting while enhancing the control of the digital persona.

[52] MAYER-SCHÖNBERGER, *supra* note 1, at 109
[53] *Id.*
[54] *Id.* at 53.

3 The Transatlantic Clash: The EU Perspective

3.1 Introduction to the Chapter

In this chapter the most important privacy laws in the EU with focus on data protection are presented. The ruling in *Google Spain v. AEPD* takes a central position since it is based on the writing in Directive 95/46/EC, which will be replaced by the General Data Protection Reform when it most likely enters into force in 2016. Since the collision with freedom of expression is a significant hurdle for implementing a right to be forgotten, the relevant freedom of expression laws are also presented below.

3.2 Privacy Rights in the EU

After the two world wars, European legislators empowered their citizens with information privacy rights. With a history of constant disregard for human rights, the EU made it evident that human dignity will be protected at all costs: "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights".[55] These rights were not applicable merely towards the central government, like in the U.S.A.[56], but towards all public and private sector information processors as well. Originally, information privacy in the EU was more a question of individual consent; something that later on turned into the individual's right to participate in society.[57] The right to data protection in the EU was a result of developments in the field of technology introduced in the 1980s through the *Privacy Principles* created by the Organization for Economic Co-operation and Development (OECD).[58] This was before the World Wide Web, and the OECD Privacy Principles were the first internationally agreed upon set of privacy principles.[59] There is now an updated version of these principles from 2013, which is a part of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[60]

---

[55] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 2007 O.J. (C 306) 13.
[56] *See* chapter four regarding privacy regulations in the U.S.A.
[57] MAYER-SCHÖNBERGER, *supra* note 1, at 137.
[58] OECD Privacy Principles, available at http://www.oecd.org/sti/ieconomy/privacy.htm. OECD is a forum for "countries committed to democracy and the market economy. The organization provides a setting where governments compare policy experiences, seek answers to common problems, identify good practice and coordinate domestic and international policies."
[59] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013), http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.
[60] *Id.*

European privacy rights are designed to protect and respect one's image, name, and reputation.[61] This dignity-based right origins from a concept in German constitutional law, *informationelles selbstbestimmung,* or *informational self-determination*,[62] which is a right for the individual to determine how one will portray oneself to third parties and to the public.[63] The idea that the individual shall have the possibility to control information that relates to him or her is in line with the concept that "knowledge about me is my property".[64] In the very first Charter of Fundamental Rights of the European Union it is provided that "human dignity is inviolable"[65] and the EU Member States have protected dignity-based privacy above freedom of expression.[66] The right to protection of personal data is not an absolute right,[67] and it needs to be considered in relation to its function in society, implying that limitations may be imposed as long as they are provided for by law and meet the general interests of the EU with regard to proportionality as well as the protection of the rights and freedoms of others.[68]

The interrelationship between *privacy rights*, which can be both the right to control information about you and to be "left alone",[69] and *protection for personal data*, has been described in the EU the following way: "Data processing systems are designed to serve man; […] respect their fundamental rights and freedoms, notably the right to privacy, and contribute to […] the well-being of individuals".[70] Protection for personal data in the EU is provided for in several different EU treaties and conventions: Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), as introduced by the Lisbon Treaty, states that "everyone has the right to the protection of personal data concerning them"[71]. Similarly, Article 8 of the European Convention of Human Rights (ECHR)[72] underlines that everybody has a right to respect for

[61] James Q. Whitman, *Two Western Cultures of Privacy: Dignity Versus Liberty,* 113 YALE L.J. 1153, 1161 (2004).
[62] *See, e.g.,* Paul Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AM. J. COMP. L. 675, 686–87 (1989).
[63] *See* Bundesverfassungsgerich [BVerfG] [German Federal Constitutional Court] June 3, 1980, 54 Etscheidungen des Bundesverfassungsgerichs [BVerfGE] 148 (155) (F.R.G.).
[64] Hayden Ramsay, *Privacy Privacies and Basic Needs,* THE HEYTHROP JOURNAL 288-297 (2010).
[65] Charter of Fundamental Rights of the European Union, OJ 2007, C 303/1, art. 1, http://www.europarl.europa.eu/charter/pdf/text en.pdf, [hereinafter *The Charter*].
[66] *See* Donald C. Dowling Jr. & Jeremy M. Mittman, *Data Privacy Regulation Outside the United States: A Clash of Jurisprudential Perspectives*, in PROSKAUER ON PRIVACY (2006).
[67] Court of Justice of the European Union, Judgment of Nov. 9, 2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Hartmut Eifert v Land Hessen (2010).
[68] *The Charter, supra* note 65, Article 52(1).
[69] Samuel Warren; Louis Brandeis, *The Right to Privacy*, 15 Harv. L. Rev. 193 (1890); PETER BLUME, PROTECTION OF INFORMATIONAL PRIVACY, 13 (2002).
[70] Directive 95/46/EC, *supra* note 2, at (2).
[71] Consolidated version of the Treaty on the Functioning of the European Union, OJ 2008, C 115/49, art. 16(2), http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0047:0199:en:PDF [hereinafter *TFEU*].
[72] European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 8, http://conventions.coe.int/treaty/en/Treaties/Html/005.htm [hereinafter *ECHR*].

his private life, which includes personal data, reputation, names and photos.[73] Additionally, Article 12 of the Universal Declaration of Human Rights (UDHR) [74] protects interference with an individual's privacy and attacks upon his honour and reputation. Finally, while Article 7 of the Charter of Fundamental Rights of the EU (the Charter)[75] focuses on general privacy protection for the individual, Article 8 of the Charter enshrines the protection of personal data as a fundamental right[76] and requires the same level of data protection throughout the EU. If there were no such right we would risk having different levels of protection within the EU, which would limit the possibilities of having cross-border flows of personal data between the Member States.[77]

3.3 The EU Data Protection Directive of 1995

The current governing privacy law in the EU is the Data Protection Directive of 1995 (Directive 95/46/EC).[78] In 1995, less than one percent of the EU citizens used the Internet,[79] but due to technological progress and globalisation, almost two decades later a vast majority of the EU citizens use the Internet.[80] The purpose of the enactment of the Directive is to protect fundamental human rights, especially the ones presented in Article 8 ECHR and the general principles of the EU.[81] In Directive 95/46/EC there is no clear right to be forgotten provision stated similar to Article 17 of the proposed GDPR.

---

[73] *Id.*
[74] United Nations, The Universal Declaration of Human Rights, Dec. 10, 1948, art.12, http://www.ichrp.org/en/article_12_udhr [hereinafter *UDHR*].
[75] *The Charter, supra* note 65, art. 7.
[76] *General Data Protection Regulation, supra* note 3.
[77] *Id.*
[78] Similar to this Directive is the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, (EC) No 45/2001 (Dec. 18, 2000). Article 16 herein provides for a right for the data subject to obtain from the controller the erasure of data if the processing is unlawful.
[79] Press Release, European Commission, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses, http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en [hereinafter *Press Release, European Commission, Increase Users' Control*].
[80] *Id.*
[81] *See Google Spain v. AEPD, supra* note 21. Due to its nature of a directive, as opposed to a regulation, the Member States have implemented it differently resulting in variances in enforcements. A regulation is a binding legislative act, which must be applied in its entirety in each Member State, while a directive is a legislative act that is merely binding as to which result is must reach, but where each Member State have a freedom to enact it differently to fit their own legal system. More information available at European Union, *Regulations, Directives and Other Acts, http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm; See* also Article 29 Data Protection Working Party, *Working Party on the Protection of individuals With Regard to the Processing of Personal Data*, Feb 15, 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/rules-art-29_en.pdf (Article 29 Working Party is an independent European advisory board, whose goal is to protect individuals with respect to the processing of personal data. Its tasks are described in art. 29 and 30 of Directive 95/46/EC, and in art. 15 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector).

However, in the recent ruling by CJEU in *Google Spain v. AEPD*[82], presented below, Directive 95/46/EC was interpreted as to give data subjects a right to be forgotten, which implies that a first step towards the enhanced privacy for the EU citizens has already been taken.

3.4 The General Data Protection Reform

The General Data Protection Reform, in which the right to be forgotten is presented, was introduced by the European Commission in January 2012 and is expected to enter into force in 2016.[83] On October 21, 2013, the Civil Liberties, Justice and Home Affairs Committee of the European Parliament (LIBE) voted overwhelmingly in favour of the reform.[84] To become law the proposed reform has to be adopted by the Council of Ministers using the ordinary legislative procedure, which is a co-decision as provided for in Article 294 of the TFEU.[85] The next meeting of Justice Ministers on the Data Protection Reform will take place in June 2014.[86]

The General Data Protection Reform was proposed to present rules adapted for the twenty-first century and the technological progresses that have been made since the existing Directive 95/46/EC entered into force. Based on the fact that "technological progress and globalization have profoundly changed the way our data is collected, accessed and used,"[87] and since Directive 95/46/EC was implemented differently by the EU Member States, a unified law in the EU was needed.[88] The reform consists of one regulation, focusing on privacy protection of users, and one directive, which aims to prevent, detect, investigate or prosecute criminal offences and related judicial activities.[89] The regulation, which is the focus of this paper, has two main objectives: to enhance individuals' control over their personal data, and to provide legal certainty and

[82] *Google Spain v. AEPD, supra* note 21.
[83] Council of Foreign Relations NY, *Privacy Pragmatism: Focus on Data Use, Not Data Collection,* March 1, 2014, http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism.
[84] Press Release, European Commission, *A Data Protection Compact for Europe,* January 28, 2014, Speech/14/62, http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm [hereinafter *Press Release, European Commission, A Data Protection Compact*]; European Commission, *LIBE Committee Vote Backs New EU Data Protection Laws*, Oct. 22, 2013 (MEMO/13/923), http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.
[85] *See* European Commission, *The Co-Decision or Ordinary Legislative Procedure*, (archived June 24, 2007), http://ec.europa.eu/codecision/procedure/index_en.htm.
[86] European Commission, *Data Protection – Progress on EU Reform Now Irreversible After European Parliament Vote,* March 12, 2014, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_dp_plenary_vote_140312_en.pdf.
[87] European Commission, *Commission Proposes a Comprehensive Reform of the Data Protection rules*, Jan. 25, 2012, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.
[88] Christoper Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection law,* Privacy & Security Law Report, 11 PVLR 06, June 2, 2012.
[89] European Commission, *Data Protection Day 2014: Full Speed on EU Data Protection Reform*, Memo, Jan 27, 2014, http://europa.eu/rapid/press-release_MEMO-14-60_en.htm [hereinafter *European Commission, Data Protection Day*].

minimize administrative burdens for businesses.[90] The rules should apply irrespectively of the nationality of the data subject, since the application of different standards to nationals and non-nationals is incomprehensible in an open Internet.[91]

Viviane Reding, EU Commissioner for Justice, Fundamental Rights and Citizenship, stressed in the press release for the General Data Protection Reform that since personal data is "the new currency of the digital market, it needs to be stable and trustworthy. Only if consumers trust that their data is well protected, they will continue to accept new services".[92] Facts show that the technology sector contributes to 20 percent of the productivity growth in Europe, and 40 percent of the investment. This is an implication to why trust in the online environment is vital for continuing to stimulate the economic growth in the EU.[93] Viviane Reding underscored that "we have a whole economy based on collection of data. If people start losing trust, they will stop sharing data".[94] The new regulation aims to make people better informed and less casual with the information they share. It will enable people to be in charge of their personal data and make companies understand that personal data belongs to the data subject, and since the companies are just borrowing it the data can be taken away from them anytime.[95] The reform will work as strong, unified legal framework at the EU level and a one-stop shop for businesses instead of having to adapt to different data protection laws in different countries. This is estimated to save businesses 2.3 billion Euros each year,[96] which will foster economic growth, innovation and job creation.[97] U.S. businesses, on the contrary, claim that this will restrain trade and reduce jobs.[98]

---

[90] Hans Graux, Jef Ausloos, Peggy Valcke, *The Right to be Forgotten in the Internet Era,* Nov. 12, 2012, https://www.law.kuleuven.se/icri/.

[91] *Press Release, European Commission, A Data Protection Compact, supra* note 84.

[92] *Press Release, European Commission, Proposes a Comprehensive Reform, supra* note 14.

[93] European Commission, *How will the data protection reform affect social networks?* June, 2011, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf.

[94] Telephone interview with an EU official (who desired to be anonymous), who was involved in the development of the General Data Protection Regulation, Boston, MA, U.S.A.- Brussels, Belgium, Dec. 11, 2012.

[95] BBC News, *Do you Have a Right to Be Forgotten Online?,* Feb. 10, 2012, http://news.bbc.co.uk/2/hi/programmes/click_online/9695021.stm.

[96] *Press Release, European Commission, Proposes a Comprehensive Reform, supra* note 14.

[97] *European Commission, Data Protection Day, supra* note 89; European Commission, 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 – European Data Protection Framework for the 21st Century,* (COM(2012) 9 final, Jan. 25, 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf.

[98] House of Representatives, *Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?,* Hearing Before the Subcommittee on Commerce, Manufacturing, and Trade of the Committee of Energy and Commerce, March 29, 2012, Serial No. 112-135, http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg81441/pdf/CHRG-112hhrg81441.pdf.

3.5 The Right to Be Forgotten According to the GDPR

The idea of having a right to delete ones past on the Internet is not a new phenomenon. In France there is already a so-called *droit à l'oublie,* or a *right to oblivion*, that is, a legal principle that grants "the right to silence on past events in life that are no longer occurring".[99] This right has mostly been applied in cases where an individual has served a criminal sentence and thereafter wishes to no longer be associated with his or her history of criminal activities. The right to oblivion is usually described as a fundamental right to one's reputation, which historically has been balanced with the public's right to information, if such information may be considered *newsworthy*. The exact scope and rationale behind the right to be forgotten is not totally clear. However, some people mean that the right to be forgotten is a mix between the right to oblivion and the *right to erasure*, which offers deletion or erasure of information that a data subject has disclosed *passively*. Such data is often collected and processed by third parties.[100]

Article 17 of the GDPR presents the proposed right to be forgotten in the EU. It can easiest be described as a right to erasure of information in the possession of other parties. It gives the individual a right to have full control over the data related to him or her, and to delete such data.[101] The right to be forgotten has taken three forms in the literature: the right to have information deleted after a certain time, the right to have a "clean slate", and the right to only be connected to present information.[102] The first concept focuses on the idea that data subjects shall be given a right to require other individuals or organizations to erase information about them, both when the subject itself has uploaded the information and when somebody else has posted it online.[103] The second and third concepts are similar since they provide a possibility for a fresh start, a right to make mistakes and to develop by having a right to erase these mistakes.[104] The right to be forgotten would allow people to "shape their own lives" instead of letting other people do it for them.[105]

According to Article 17 of the GDPR, the data subject shall have a right to obtain from further processing of data relating to him or her, if: the data is no

[99] Norberto Nuno Gomes de Andrade, *Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization, in* COMPUTERS, PRIVACY AND DATA PROTECTION: AN ELEMENT OF CHOICE 66, 90 (Serge Gutwirth et. al. eds., 2011).
[100] Meg Leta Ambrose, Jef Ausloos, *The Right to be Forgotten Across the Pond,* JOURNAL OF INFORMATION POLICY 3 (2013): 1-23.
[101] Kate Brimsted, *The Right to be Forgotten: Can Legislation Put the Data Genie Back in the Bottle?,* PRIVACY & DATA PROTECTION 6-8, 7 (Vol. 11(4) 2011).
[102] Bert-Jaap Koops, *Forgetting Footprints, Shunning Shadows: A Critical Analyze of 'The Right to be Forgotten' in Big Data Practice,* 8 SCRIPTED 229, 236 (2012).
[103] *Id.*
[104] Jean-François Blanchette; Deborah G. Johnsson, *Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness* 4, ACM Policy Conference (1998).
[105] Koops, *supra* note 102.

longer necessary in relation to the purpose for which it was collected or processed, the data subject withdraws his or her consent to further processing of this data, there no longer is any legal ground for processing of such data, the data subject objects to the processing of his or her personal data, or if the processing of the data does not comply with the GDPR for other reasons.[106] One problem is the very broad nature of the right to be forgotten. Privacy experts have questioned whether such a right can be narrowed, or if it simply cannot be more specific than this due to the extremely varied circumstances in the cases regarding the right to be forgotten.[107]

The right to be forgotten will provide a right to request a data controller to *delete* personal data, implying "any information related to the data subject". Through the enactment of the GDPR, the European Commission simply wants the users across the EU to be able to demand search engines, social network sites and other platforms holding personal data to remove undesired data belonging to or relating to the data subjects. According to a Eurobarometer survey made by the European Commission, 84 percent of 18-to-24-year-olds – the so-called "digital natives" – want the right to be forgotten to be legislated.[108] They stress the importance of being able to control the information available about them on the Internet.[109] Since the right to be forgotten is not an absolute right, there are, however, a few exceptions to this obligation, stated in Article 17(3), which gives a data controller a right to obtain personal data for reasons of historical, statistical, public health and scientific research purposes, or to protect free expression online.[110]

3.5.1. Determining the Scope of Application of the Right to Be Forgotten

The idea of a right to be forgotten is far more complex than simply to give data subjects a right to control their history on the Internet. To enable a better understanding of what type of data is or might be included in a right to be forgotten and to identify the scope of such right, it is of great importance to categorize data to make it less abstract and possible to discuss. For this purpose I have chosen to use three common scenarios on the Internet, introduced by Google's Global Privacy Counsel, Peter Fleischer:
(1) If the data subject posts something about him or herself and wants to delete it;
(2) If the data subject posts something that someone else copies, re-posts, re-tweets or "shares", and the data subject would like to delete *both* the original information *and* the copies of it; or

---

[106] *General Data Protection Regulation, supra* note 3, art. 17.
[107] Peter Fleischer, *Foggy thinking about the Right to Oblivion*, March 9, 2011, http://peterfleischer.blogspot.se/2011/03/foggy-thinking-about-right-to-oblivion.html [hereinafter *Fleischer, Oblivion*].
[108] *Press Release, European Commission, Data Protection, supra* note 12.
[109] Xanthoulis, *supra* note 28.
[110] *General Data Protection Regulation, supra* note 3, art. 17.

(3) If *somebody else* writes something *about* the data subject that the data subject would like to delete.[111]

3.5.1.1 The First Degree of Deletion: Erasure of Personal Data Originating From the Data Subject

If a data subject posts something online and later on would like to delete it, shall such right be given to him or her? Most websites already give the data subjects such right.[112] The right to be forgotten that focuses on this first step, has been criticized for being a bit naïve since it just makes it easier to delete something, which you actually already had the right to do; it is just bringing power to a right to delete that already exists.[113] Deletion on such "basic" level has, however, gotten increased popularity through the use of the photo messaging application *Snapchat* where deletion is a default setting.[114] With self-destructing messages as its core concept, the sender of a Snapchat picture can determine the length of time for the recipient to view it, after which the message will be hidden from the recipient's device and deleted from Snapchat's servers.[115] However, no *websites* currently use deletion as the default setting.

3.5.1.1.1 What Type of Information is Included in the Right to Be Forgotten?

Article 17 of the GDPR broadly states that "personal data relating to them" may be deleted, but reveals no further details about what *type* of information this includes. To be able to have a constructive discussion about the right to be forgotten and to be able to investigate what type of information that might be included in such a right, a good start is to use analogies from other legal areas. In *copyright law*, protection is given to *expressive* content. A picture that the data subject posts online might be a work of art, which should *not* be given the right to be copied without the owner's permission or license. A right to be forgotten on the other hand must cover content that is *informational* in nature. An example could be logs of the data subject's search quires on Google.[116] However, a great amount of the information that the average users posts on social media sites are of *both* an expressive *and* informational type, for example a photograph of a person attending a political event. It is an *expressive* and creative work of art at the same time as it *informs* that this person has

---

[111] *Fleischer, Oblivion, supra* note 107; Jeffrey Rosen, *The Right to be Forgotten,* 64 STAN. L. REV. ONLINE 88 (2012).
[112] *See,* e.g., Facebook's Terms, *Statement of Rights and Responsibilities*, https://www.facebook.com/legal/terms.
[113] Julia McClure, *The Right to Be Forgotten in a Digital Age,* National Security Law Brief, Washington College of Law, Nov. 14, 2013, http://www.nationalsecuritylawbrief.com/the-right-to-be-forgotten-in-a-digital-age/.
[114] *See* Snapchat, Terms of Use, last updated Dec. 20, 2013: http://www.snapchat.com/terms/.
[115] *Id.*
[116] Conley, *supra* note 35, at 55.

attended a political event. The question whether it is possible to delete *informational* content and *not* expressive content still remains to be further determined by the EU Commission.[117]

There is a big difference between a user deletion of content from his or her own social media site, and whether the user can delete the information from the whole Internet, which leads to the next degree of deletion.

3.5.1.2 The Second Degree of Deletion: Erasing Copied and Spread Personal Data

The second degree of deletion is when the data subject posts something and someone else copies and re-posts it on their own site. There is obviously always a possibility to ask this individual to remove the picture from his or her site. If he or she refuses or is hard to find there is always a possibility to pursue judicial procedures, which, however, oftentimes are costly and time-consuming. The data subject who wants to have the picture deleted can ask the website hosting the content to take it down. If the picture clearly violates their policy of accepted content, there is a possibility that they will take the picture down. The main idea of a right to be forgotten reflects the notion that people retain a privacy interest in information about themselves, even if the user voluntarily already has exposed that information to the public. It entails control over the information flow about oneself and an artificial restoring of obscure information exposed online. Such provision includes demanding a social network platform or a search engine to remove an embarrassing photo or comment posted by or related to the data subject – even if it has been copied by another data subject.[118] What is actually happening is that the data subject is asking the platform to choose between the privacy right of the data subject to have this picture deleted, and the freedom of expression of the other data subject who now has this picture in his or her photo album.[119]

The American Chamber of Commerce to the European Union (AmCham EU), who speaks for American companies committed to Europe on trade, investment and competitiveness issues,[120] disagrees with the idea of being able to "remove all tracks". Similarly, the Internet founder Vint Cerf has stated that it is not possible to remove content from everybody's computer just because a person would like to have something forgotten. In his attempt to find a common denominator between the analog and the virtual world he gave a vivid example: "[Information published online] may be compared to something you might have published in the analogue world, for example a book that you want everybody to forget about because it is embarrassing. To break in to people's homes and take the book off the bookshelves would have some legal

[117] *Id.*
[118] Robert G. Larson III, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech, Communication Law and Policy*, 18:1, 91-120 (2013).
[119] *Fleischer, Oblivion, supra* note 107.
[120] AmCham EU, more information available at http://www.amchameu.eu/AboutUs/tabid/61/Default.aspx.

repercussions, and it is important to ask ourselves why it should be any different in the online world?"[121]

3.5.1.3 The Third Degree of Deletion: Erasing Other People's Data *About* the Data Subject

The third scenario that Peter Fleischer enlightens is the case where *someone else* posts content *about* the data subject and the data subject desires to have this content deleted. It can be an unflattering picture of the data subject posted online, or an article or blog post that contains legally obtained information, but which might be outdated or embarrassing to the subject portrayed therein. This is where the right to be forgotten gets really complicated.[122]

The AmCham EU believes that the right to be forgotten should not include data posted by third parties since such deletion is already covered by other legal protections such as defamation and libel laws. One, whose reputation was harmed as a result of another person's speech, needs to bring a defamation claim to recover. However, as many plaintiffs may feel unsatisfactory, defamation law requires that the speech is *false* – and truth is a *defense* to such a claim.[123] Peter Fleischer emphasizes that "privacy is far more elastic because privacy claims can be made on speech that is true". He therefore believes that "privacy is the new black in censorship fashion".[124] According to him, the right to be forgotten should not be used to contact a social networking website or a search engine and ask them to remove data about a data subject.[125]

This was clearly the case in *Google Spain v. AEPD,* where the Spanish citizen asked Google to remove the links connected to his name when making a Google search.

3.6 Google Spain v. AEPD

Since there are over one trillion sites on the Internet, search engines like Google enable us to find what we are looking for by creating giant indexes of the web. Search engines are intermediaries using complex algorithms to match a user's search query with the most relevant search result without editing or creating any new material.[126] Lobbyists against a right to be forgotten have argued that it is "technically impossible to implement the right to be forgotten, because of the many back-ups of back-ups that take place. But if you can be

[121] Matt Warman, *Vint Cerf Attacks European Internet Policy,* THE TELEGRAPH, March 29, 2012, http://www.telegraph.co.uk/technology/news/9173449/Vint-Cerf-attacks-European-internet-policy.html.
[122] *Fleischer, Oblivion, supra* note 107.
[123] *See*, RESTATEMET (SECOND) OF TORTS § 558 (1977).
[124] *Fleischer, Oblivion, supra* note 107.
[125] *Id.*
[126] *Id.*

deleted from Google's database, that is, if you carry out a search on yourself and it no longer shows up, it might be in Google's back-up, but if 99 percent of the population do not have access to it you have effectively been deleted".[127]

The CJEU decided in *Google Spain v. AEPD*[128] on May 13, 2014. It concerns a Spanish national resident in Spain, Mr. Costeja González (Mr. Costeja), who, on March 5, 2010 lodged with the Spanish Data Protection Authority, Agencia Española de Protección de Datos (AEPD), a complaint against La Vanguardia Ediciones SL, which publishes a daily newspaper with a large circulation in Spain, and against Google Spain SL and Google Inc. The complaint was based on the fact that upon entering Mr. Costeja's name into the Google Search function two pages of an article in La Vanguardia appeared. The articles were from January 19 and March 9, 1998, respectively, and mentioned Mr. Costeja's name in association with a real-estate auction connected with attachment proceedings for the recovery of a social security debt. Mr. Costeja asked the newspaper to erase the article because it was no longer relevant since the proceedings had been concluded. When the publisher refused to delete the article due to the fact that the published material was effected by order of the Ministry of Labor and Social Affairs,[129] Mr. Costeja asked Google Spain to no longer show links to this article that appeared when he was searching for his name on the search engine. The AEPD later on took care of the case, but was unable to force the newspaper to delete the content since such data in the press was a legally justified publication. The AEPD instead argued that Google should delete information from its search results when it can be shown that an individual's privacy is breached. Spain's highest court, Audencia Nacional, found in favor of the complainant and ruled that Google should be forced to delete the search result. Google thereafter sought the annulment of the decision.[130] The court stayed the proceedings in order to send several questions to the CJEU for a preliminary ruling in the case.

Since the GDPR has not yet entered into force, the ruling in the case was based on the applicable law: Directive 95/46/EC.[131] The questions concerned the *scope of the application* of Directive 95/46/EC, the *definition of "data controller"* in the context of search engines, and whether a *"right to be forgotten" could fall under the Directive*.[132]

---

[127] Kate Connolly, *Right to Erasure Protects People's Freedom to Forget the Past, Says Expert,* THE GUARDIAN, April 4, 2013, http://www.theguardian.com/technology/2013/apr/04/right-erasure-protects-freedom-forget-past; Sanna Kulevska, *The Future of Your Past: A Right to be Forgotten Online?,* Berkman Center for Internet and Society at Harvard Law School, http://www.chillingeffects.org/weather.cgi?WeatherID=769.

[128] *Google Spain v. AEPD, supra* note 21.

[129] *Id.*

[130] *Id.*

[131] Directive 95/46/EC is implemented in Spanish law through the Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. ("B.O.E." núm. 298, de 14 de diciembre de 1999).

[132] *Google Spain v. AEPD, supra* note 21.

On June 25, 2013, Advocate General Niilo Jääskinen gave his opinions about the questions that were sent to CJEU. He argued for no responsibility for Google to remove any links on its search engine based on a privacy claim.[133] In addition, by suppressing legitimate and legal information that has already entered the public domain it would definitely interfere with the freedom of expression and violate the *objectivity* of the Internet.[134] Jääskinen pointed out the importance of the Internet in general, and that we should not undermine the fact that the access to information has revolutionized communication between individuals.[135] Quite frequently the CJEU listens to its Advocate General, but this time the court ruled in stark contradiction to his opinion.

3.6.1 The First Set of Questions to the CJEU

To find out the *scope* of the application of the Directive, the *first* set of questions for the CJEU to answer was whether Google Spain could be considered an "establishment" of Google Inc., and if their activity in Spain could fall under "use of equipment…situated on the territory of that Member State" as provided for in Article 4(1)(a) and 4(1)(c) of Directive 95/46/EC, respectively.

Contrary to Google Spain's arguments, the CJEU held that Google Spain are both considered an establishment and user of equipment in a Member State. The reasons are that Google Spain acts as a commercial representative for Google Inc.'s advertising activities and takes advantage of the activity through advertising based on the search terms on the local website, www.google.es. In addition, Google Search uses computer programs to locate and sweep up the content of web pages methodically and automatically through the use of web crawlers or robots. The CJEU held that it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations laid down in Directive 95/46/EC. That would affect the effective protection of the Directive with regards the protection of privacy with respect to the processing of personal data.[136]

3.6.2 The Second Set of Questions to the CJEU

The *second* set of questions to the CJEU concerned whether Google's activity can be considered "processing of information", and whether Google can be considered "controllers" of the information they index on their search site.

[133] Case C-131/12 Google Spain v. AEPD – Opinion of Advocate General Jääskinen, June 25, 2013,http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=138782&occ=first&dir=&cid=124792 [hereinafter *Opinion Jääskinen*].
[134] John Hendel, *In Europe, a Right to be Forgotten Trumps the Memory of the Internet,* THE ATLANTIC, Feb. 3, 2011, http://www.theatlantic.com/technology/archive/2011/02/in-europe-a-right-to-be-forgotten-trumps-the-memory-of-the-internet/70643/.
[135] *Opinion Jääskinen, supra* note 133.
[136] Case C-342/09, *L´Oréal and Others* [2011] ECR 474, paragraphs 62 and 63.

Article 2(b) of Directive 95/46/EC states that "processing of personal data shall mean any operation […] which is performed upon personal data, whether or not by automatic means, such as collaboration, recording, organization, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".[137]

According to Google Spain and Google Inc., their activity cannot be regarded as "processing of the data" that appear on a third-party website since the search engine processes all the information available on the Internet without being *aware* of the existence of personal data, since personal data "does not manifest itself in any particular way".[138] As regards in particular the Internet, the CJEU has already in the *Lindqvist* case[139] stated that the operation of loading personal data on an Internet page must be considered "processing of data" within the meaning of Article 2(b) of Directive 95/46/EC. The CJEU held that Google's handling of personal data falls within the definition of "processing" and found the argument that Google cannot differentiate between personal data and other types of data irrelevant.[140]

Furthermore, it was investigated whether the Google search engine can be considered a "controller" of personal data within the definition in Article 2(d) of Directive 95/46/EC: "A controller is "the natural or legal person […] which alone or jointly with others determines the purposes and means of the processing of personal data". Google underscored that they do not control data, they only offer links to information freely available on the Internet. Due to the fact that it is the search engine that determines the purposes and means of their activity and of the processing of personal data, the CJEU held that they must be considered the "controller" of such information. This becomes even more clear when considering that the activity of search engines plays a decisive role in the Internet users ability to get access to the information when typing in the name of an individual since the users of the search engine otherwise would not have found the web page on which the personal data is published.

Moreover, it was asked whether Directive 95/46/EC directly can impose on the search engine a requirement that it shall withdraw from its search indexes information published by third parties – even if such information was lawfully published and even if such information has not yet been removed form the third-party website.

The CJEU determined Articles 12(b) and 14(a) of Directive 95/46/EC relevant when answering this question. Article 12(b) states that the data subject shall have a right to "obtain from the controller […] the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete and inaccurate nature of the data". Article 14(a) states the data subject's right to object "[…] at any

[137] *Google Spain v. AEPD, supra* note 21.
[138] *Opinion Jääskinen, supra* note 133.
[139] *See* Case C-101/01, *Lindqvist* [2003] ECR 596, paragraph 25.
[140] *Google Spain v. AEPD, supra* note 21.

time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him […]"

Google Spain and Google, Inc. stated that making them responsible for the removal of personal data would be contrary to the principle of proportionality, and such removal must be addressed to the *publisher* of the website where the personal data exists because it is the website who has the responsibility for making the information public. The publishing website is also, according to Google, the one that most effectively and least restrictively can make the information inaccessible. To require a search engine to remove content from its index would take insufficient account of the fundamental rights of publishers of websites, of other Internet users and of the search engine itself.

The CJEU held that search engines, due to their status of displaying a list of result just by typing in the name of the data subject and thereby making the access to this information so much easier for Internet users, is liable to constitute a more significant interference with the data subject's right to privacy than the original publication of the web page. The CJEU therefore held that Article 12(b) and 14(a) shall be interpreted as to make the search engine obliged to remove from the list of results displayed following a search "made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person".[141] This will be the obligation also where that name or information is not erased beforehand on those web pages.

3.6.3 The Third Set of Questions to the CJEU

The *third* set of questions to the CJEU concerned the *right to be forgotten*, and whether Articles 12(b) and 14(a) of Directive 95/46/EC can be interpreted as to give the data subject a right to require a search engine to remove from the list of results displayed following a search on the data subject's name links to web pages lawfully published by third parties and containing true information related to the data subject. The reason for this erasure might be that the information is prejudicial, or no longer relevant to the data subject, and that he or she wishes to "be forgotten" after a certain time. The CJEU responded affirmatively to this question since Article 6(1)(c) to (e) of Directive 95/46/EC states that personal data must be adequate, accurate, kept up to date and that inaccurate or incomplete data that has been collected and processed shall be erased or rectified. The protection for private data as provided for in Article 8 of the Charter must, according to the CJEU, as a general rule override the interest of the Internet users. This shall, however, be considered based on the nature and sensitivity of that information as well as the certain interest of the public to access the information in question based on the role played by the data subject in the public life.

[141] *Google Spain v. AEPD, supra* note 21.

3.6.4 Summary of the Decision in *Google Spain v. AEPD*

To summarize the ruling by the CJEU, Google will be held responsible, as a processor of personal information, to protect such information. As a controller of the data appearing on its search engine, Google is required to, upon request by a data subject, delete information from its search result that shows links to third-party websites - despite the fact that the personal data has not yet been removed from other websites and even if the original publishing of the information was lawful. These rights override, as a rule, not only the economic interest of the operator of the search engine, but also the interest of the general public in finding that information upon a search relating to the data subject's name. Exceptions will be made if interference with the data subject's fundamental rights is justified by an interest of the general public in having access to the information in question.

3.6.5 Immediate Responses to the CJEU Decision

EU Commissioner Viviane Reding welcomed the CJEU's decision saying that it was a clear victory for the protection of personal data of the Europeans and a "strong tailwind for the Data Protection Reform that the European Commission proposed in January 2012 as it confirms the main pillars of what we have inscribed in the data protection Regulation".[142]

Peter Fleischer, Google's Privacy Counsel, stressed that requiring a search engine to provide Internet users with a the right to be forgotten is not about deleting or forgetting content, but just about *making it harder* to find content.[143] The original information will not be deleted just because it could be removed from Google. A case like *Google Spain v. AEDP* would simply just make it impossible for users to use search engines to *find* content that otherwise continues to exist on the web.[144] Jonathan Zittrain, Professor of law and computer science at Harvard University, agrees and criticizes the CJEU's decision for being both too broad and too narrow. He explains that it is too broad because it allows individuals to "impede access to facts about themselves found in public documents", which is a form of censorship. Search engines are, after this decision, forced to remove personal data that is "inadequate, irrelevant, or no longer relevant", which Jonathan Zittrain believes will lead to search engines erring on the safe side of caution and accepting to most of the take-down requests.[145] On the contrary, he believes that the decision at the same time is too narrow since it does not require the unwanted personal

[142] Viviane Reding' Facebook page, https://www.facebook.com/permalink.php?story_fbid=304206613078842&id=291423897690447.
[143] Peter Fleischer, *The Right to be Forgotten – Seen from Spain*, Sept. 5, 2011, http://peterfleischer.blogspot.se/2011/09/right-to-be-forgotten-seen-from-spain.html [hereinafter *Fleischer, Spain*].
[144] *Id.*
[145] Jonathan Zittrain, *Don't Force Google to 'Forget'*, THE NEW YORK TIMES, May 14 2014, http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0.

information to be totally *deleted* from the Internet. Mr. Costeja's name and other personal information will still exist on other web pages, which does not lead to any actual "forgetting" of such information.

Other critics of the fact that Google now has to provide a right to be forgotten, have argued that if content becomes less searchable on the Internet, it will derogate the role of counterspeech as it disrupts the normal process of communication.[146] They underscore that freedom of expression is vital since it enables citizens to discuss and share information about the society. "A right to be forgotten would deny the would-be speaker the ability to decide what to say and think, and deny the would-be listener the information desired to form his opinions and ideas."[147]

3.7 Freedom of Expression in the EU

A right to be forgotten will indisputably strengthen already existing privacy rights. It is therefore argued that enforcing a right to be forgotten will create an assumption that privacy right has a higher dignity than other human rights, such as freedom of expression.[148] When providing for a right to delete information online the freedom of expression of another individual might be violated. The clash between a right to delete and freedom of expression becomes evident when a data subject mentioned in a comment, picture or an article published online wants to delete such information concerning him or her. Taking the case of Stacy Snyder as an example, the freedom of expression of other people sharing, commenting or re-posting the "drunken pirate" picture online would be violated if she got a possibility to delete it. To restrict their right to speak about such content or their possibilities to find such legally published content on a search engine could risk having a chilling effect on freedom of expression. Viviane Reding stated in the press release to the GDPR: "There is no right that is absolute. A right always goes as far as it can until it comes in conflict with another right."[149] However, similar to Directive 95/46/EC, the GDPR strives to balance these rights by presenting freedom of expression as a limitation of the right to delete.

In order to become a Member of the EU, all Member States must provide their citizens with a right to freedom of expression. Article 11 of the Charter, which corresponds to Article 10 ECHR, reassures that the freedom of expressions shall include a freedom to hold opinions and to receive and impart information and ideas without the interference by a public authority.[150] The freedom of expression contains the freedom of speech and information, and implies all

[146] Larson, *supra* note 118.
[147] *Id.*
[148] Hawktalk, *Data Protection: Forget About a "Right to Forget",* AMBERHAWK, March 28, 2011, http://amberhawk.typepad.com/amberhawk/2011/03/data-protection-forget-about-a-right-to-forget.html.
[149] *Press Release, European Commission, Proposes a Comprehensive Reform, supra* note 14.
[150] *The Charter, supra* note 65, art. 11.1.

kinds of opinions and data that may be made accessible to the public.[151] The freedom of expression is not an absolute right, meaning that it is subject to a number of limitations, mostly for the sake of protecting another human right, or when it is necessary to ensure the maintenance of a democratic society, public safety, or the protection of the reputation or rights of others, to mention a few.[152] With regard to the Internet, freedom of expression may be limited if the speech contains harmful content, such as libel, slander, obscenity, or intellectual property violations.[153]

3.7.1 Do Journalists Have to Fear a Right to Be Forgotten?

Shall journalists fear the right to be forgotten implying that their articles containing legally obtained material about a data subject may be taken down due to a privacy claim? According to the decision in *Google Spain v. AEPD* the content will now be removed from the search engines, but it will not affect the original website where it was originally posted. However, a possible outcome of this decision might be that the deeply investigating journalism will face great difficulties if the search engines will remove personal and sensitive personal data.[154] Article 9 of Directive 95/46/EC provides for an exception from deletion for historical or statistical reasons, which will preserve information online and hopefully do not challenge the investigating work by the journalists.[155]

Since this decision is merely based on Directive 95/46/EC, it is of great importance to emphasize the fact that the GDPR might push the right to be forgotten even further to require deletion even from the original source webpage. The EU official who has been involved in developing the proposal for the GDPR and interviewed for this paper, rejects the violation of the free speech rights as a big issue in the question of a right to be forgotten: "A violation of the freedom of expression is not a strong argument for not having this right".[156] He refers to Article 17(3) of the GDPR, where "the controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary: (a) for exercising the right of freedom of expression in accordance with Article 80". Article 80 states that "Member States shall provide for exemptions or derogations from the provisions on the general principles…[provided for in Article 17]…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

[151] BLUME, *supra* note 69, at 141.
[152] *The Charter, supra* note 65, art. 11.2.
[153] *Id.*
[154] Mattias Goldmann; Jacob Dexe, *Låt inte de digitala fotspåren suddas ut,* May 17, 2014, http://www.svd.se/opinion/brannpunkt/lat-inte-de-digitala-fotsparen-fa-suddas-ut_3568578.svd.
[155] *See* also Eric Pfanner, *Archivists in France Fight a Privacy Initiative,* NEW YORK TIMES, June 16, 2014, http://www.nytimes.com/2013/06/17/technology/archivists-in-france-push-against-privacy-movement.html?pagewanted=2&_r=1&ref=global-home&.
[156] Telephone interview with an EU official, *supra* note 94.

personal data with the rules governing freedom of expression." Although there is an unequivocal exception for a right to be forgotten for journalistic, artistic or literary expression, the scope of such derogation still remains to be determined by the Member States within two years after the GDPR has entered into force.[157] In an online society with an increasing number of bloggers and creative content, the definition of a journalist has blurred since anyone can express himself or herself in a journalistic, or at least in an artistic or literary fashion. Although these freedom of expression exceptions to the right to be forgotten provision may be interpreted broadly, since they are not defined, Recital 121 clarifies the intended scope of application:

> This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights […] Member States should classify activities as 'journalistic' […] if the object of these activities is the disclosure to the public of **information, opinions or ideas** irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.[158]

It is clearly emphasized that it is the Member States' obligation to provide for exceptions for processing of personal data, which is carried out solely for journalistic, artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.[159] However, since the purpose of every public disclosure is to spread information, opinions or ideas, one may think that this very broad definition of journalistic activities would cover *all* public disclosures. "But such a broad exception would eviscerate the earlier privacy protection, and it is inconceivable that the European Commission dedicated 119 pages to the creation of rights which are powerless in the face of a two paragraph exception." Therefore it is important to review the purpose of the regulation, which is to strengthen user *privacy*.[160]

3.8 A Short Summary of the Chapter

- The EU has a dignity-based approach to privacy, which historically has prevailed over freedom of expression.
- The right to be forgotten will provide a right to request a data controller to delete personal data, implying "any information related to the data subject".
- Article 17(3) of the GDPR provides for an exception from deletion for freedom of expression. When the collision between the two rights occurs it not specified in the proposed law. To be able to investigate, illustrate and easier discuss the potential scope of such right before it collides with freedom of expression, I

[157] *General Data Protection Regulation, supra* note 3, art. 80(2) and art. 91(2).
[158] *Id.* recital 121.
[159] *Id.* art 80.
[160] Larson, *supra* note 118, at 106.

divided different types of data into three degrees of deletion. It seems like the collision occurs already after the first degree of deletion, which will be further discussed in the analysing chapter below.

- Search engines are, according to the decision in *Google Spain v. AEPD*, forced to remove links to personal data, even if such data was lawfully published and not yet removed from the source webpage.
- The original information will not be deleted from the Internet just because it could be hidden in a Google search.
- It is up to the Member States to specify in greater detail the exceptions from the processing of personal data and how to balance the right to be forgotten with freedom of expression.

4 The Transatlantic Clash: The U.S. Perspective

4.1 Introduction to the Chapter

Although the collision between privacy and freedom of expression is already a major problem within the EU itself and I could make a satisfactorily scrutinized presentation by focusing simply on the EU, the U.S. perspective cannot be left out. Due to the global nature of the Internet and the fact that the personal data of the European users is being used and processed by American websites and search engines, this chapter aims to present the complexity of the right to be forgotten by making a comparison with the U.S. legal system focusing on privacy law and the laws of freedom of expression. Additionally, this chapter also investigates whether a right to be forgotten could legally exist in the U.S.A. under the current system.

4.2 Privacy Rights in the U.S.A.

While the thought of a right to be forgotten in Europe has grown through the attempt to balance protection of the two constitutionally recognized rights of privacy and freedom of expression, the same thoughts in the U.S.A. have derived as a way to protect citizens' individual privacy from the mass media.[161] It started with Samuel Warren and Louis Brandeis, the first famous advocates of information privacy rights, when they published an article in Harvard Law Review in 1980, entitled "The Right to Privacy", in which they proposed a tort remedy that focused on *invasion of privacy*.[162] It is said that they wrote this article after the local press had undesirably written about the private wedding reception of Warren's daughter in an uncouth manner.[163]

The U.S.A. presently has no federally codified general right to information privacy outside of the federal government.[164] The federal Privacy Act of 1974 merely covers processing of information made by federal agencies.[165] However, some state laws do guarantee information privacy under certain circumstances. For cases which lack those prerequisites, there is a common law right to privacy. Elsewhere privacy rights in the U.S.A. can be found in different sectors, such as in the Health Insurance Portability and Accountability

[161] Franz Werro, *The Right to Inform vs. the Right to be Forgotten: A Transatlantic Clash*, Georgetown University 2009, at 292.
[162] Warren; Brandeis, *supra* note 69.
[163] MAYER-SCHÖNBERGER, *supra* note 1, at 135.
[164] Ira Rubenstein; Ronald D. Lee; Paul M. Schwarts, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches.* 75 CHI. L. REV. 273 (2008).
[165] Privacy Act of 1974, 5 U.S.C. § 552a

Act.[166] This patchwork of privacy legislations often leads to uncertainty and confusion among the citizens regarding what rights they may enjoy, and under what conditions they may act upon such rights.[167]

One month after the European Commission released its proposal to the General Data Protection Reform, the White House released its own proposal, referred to as the *Consumer Privacy Bill of Rights*. Similar to the GDPR, it aims to strengthen privacy protection for online users at the same time that it promotes economic growth and innovation. The main theme is that strong privacy protection for user data will create *trust* in the online environment, which will stimulate online commerce.[168] In this context, trust is explained as the expectations that users have for companies and technical systems regarding privacy, security and reliability. In the proposal, President Barack Obama states: "Americans have always cherished our privacy. From the birth of our republic, we assured ourselves protection against unlawful intrusion into our homes and our personal papers." The Consumer Privacy Bill of Rights, which outlines principles that should be reflected in a privacy law, is the result of a collaborative effort between Internet industry leaders and Congress to implement codes of conduct for enhanced privacy protection.[169] It provides for enhanced transparency for consumers containing a right to get easily accessible and understandable information about a company's privacy and security practices. Thanks to these multistakeholder processes a production of solutions can be made in a more timely fashion, as opposed to the often dreadfully slow regulatory processes and treaty-based organizations. The Obama Administration delegates strong authority to the Federal Trade Commission (FTC) to make sure that online companies abide by their privacy-related public promises.[170] It is important to note that the Consumer Privacy Bill of Rights does not contain any right to be forgotten, which clearly illuminates the current position of the American Federal government in relation to this legal conundrum.[171]

4.3 Freedom of Expression in the U.S.A.

The First Amendment to the American Constitution, which was ratified in 1789 states that "Congress shall make no law […] abridging the freedom of speech, or of the press."[172] It was adopted to curtail the power of Congress to interfere with an individual's freedom to express him or herself. Therefore, the freedom of expression applies only to government conduct and does not regulate the

[166] Often referred to as HIPPA, Pub. L. 104-191, 110 Stat (1996).
[167] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 67 (2004).
[168] Larson, *supra* note 118; White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, Feb. 23, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter *White House, Consumer Data Privacy*].
[169] *Id.*
[170] *Id.*
[171] *Id.*
[172] The Constitution of the United States, Amendment I (1971).

conduct of private parties.[173] Due to the existence of the First Amendment, the freedom of expression and of the press has been fiercely defended in the legal system in the U.S.A. The U.S.A. has a robust history of protecting speech while privacy rights have constantly been subordinated.[174] The preference for free speech has generally held true even when speech threatens privacy interests.[175] The Supreme Court has agreed, stating that "exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and of press."[176] The U.S. Supreme Court has also supported the suggestion that the First Amendment applies to speech and the press on the Internet.[177]

4.3.1 The *Wikipedia* case – Exemplifying the Transatlantic Clash Between Freedom of Expression and Privacy

One case clearly shows the transatlantic clash between freedom of expression and the press and a right to be forgotten, where the former prevails in the U.S.A. and the latter prevails in the EU. The case contains two men, Wolfgang Werlè and Manfred Lauber, who brutally murdered a German actor, Walter Sedlmayr. It resulted in a conviction,[178] which is a public record, and since the actor was famous and of great public interest the case also turned into an article on Wikipedia.[179] Referring to German privacy law, which seeks to protect the name and likeness of private persons from unwanted publicity,[180] the lawyers for the two murderers sent a cease and desist letter to Wikipedia demanding to have their names removed from the website due to the fact that they had already served their sentence in prison and no longer wanted to be associated with their criminal history.[181]

---

[173] *Fox Television Stations, Inc. v. F.C.C.,* 613 F.3d 317, 327 (2nd Cir. 2010).
[174] *See*, e.g., *The Florida Star v. B.J.F,* 491 U.S. 524 (1989).
[175] *See*, e.g., Jack M. Balkin, *Some Realism About Pluralism: Legal Realist Approaches to the First Amendment*, DUKE L.J. 375, 383–85 (1990).
[176] *See*, e.g., *Bartnicki v. Vopper*, 532 U.S. 514, 534 (2000) (holding that "privacy concerns give way when balanced against the interest in publishing matters of public importance").
[177] Matthew R. Millikin, *Note, www.misappropriation.com: Protecting Trade Secrets After Mass Dissemination on the Internet,* 78 WASH. U. L.Q. 931, 948 (2000).
[178] Decision BGH 1StR 83/94 (The appeal is available at http://www.hrr-strafrecht.de/hrr/1/94/1-83-94.php).
[179] Ambrose; Ausloos, *supra* note 100.
[180] Jennifer Granick, *Convicted Murdered To Wikipedia: Shhh!,* ELECTRONIC FRONTIER FOUNDATION, Nov. 10, 2009, https://www.eff.org/deeplinks/2009/11/murderer-wikipedia-shhh. Swiss law already provides a similar right by admitting citizens to preclude anyone from identifying them in relation to their criminal past. The Swiss version of a "right to be forgotten" is called "the rights of the personality", which includes Internet users' right to keep themselves private.
[181] Cease and desist letter on behalf of Mr. Wolfgang Werle to the Wikimedia Foundation Inc., Oct. 27, 2009, accessed Feb. 13, 2014, http://www.wired.com/images_blogs/threatlevel/2009/11/stopp.pdf.

Wikipedia is a part of the Wikimedia Foundation based in the U.S.A., where the First Amendment protects freedom of expression and of the press – which in this case would protect the publication of the article on Wikipedia. Under the First Amendment of the U.S. Constitution there can be no recovery for publicity of facts that are a matter of public record.[182] The requirement to get their names removed from the Wikipedia website did not merely conflict with the rights provided for in the First Amendment, but also with traditional privacy jurisprudence stating that "information made public cannot become private again".[183] The names of the two men were consequently deleted from the German-language version of the article on the Wikipedia site,[184] but when desiring to have their names deleted from the English-language version as well, the First Amendment protection prevailed. Free speech activists, such as the Electronic Frontier Foundation meant that "he, who controls the past controls the future,"[185] and underlined that the Wikipedia case "really is about editing history".[186] Michael Godwin, General Counsel of the Wikimedia Foundation, proclaimed that Wikimedia "doesn't edit content at all, unless we get a court order from a court of competent jurisdiction." The German court prohibited further publication of the victims' names in German media. This case clearly shows that although freedom of expression and the press is strong in Europe, it gives way for the right to privacy and a "clean slate". In the U.S.A. the First Amendment prevails and leaves no room for such "second chance".

4.4 Is There Any Room For the Right to Be Forgotten Under U.S. Law?

There is currently no federally recognized right to be forgotten in the U.S.A. However, some modest first steps towards such a right have recently been taken on a state level. In September 2013, California passed, through Senate Bill No. 568,[187] a narrow and watered-down version of the European right to be forgotten. When it becomes operative in January 2015, it will give children a right to delete posts that they have made to social media websites such as Facebook. However, this narrow right will merely cover deletion of posts that they have made themselves.[188] The Senate Bill No. 568 differs from the right to be forgotten proposed in the GDPR since it does not permit the erasure of all "personal data related to them", meaning copies of the data or content written *about* the data subject.[189]

---

[182] *See*, e.g., *Cox Broadcasting Co. v. Cohn* 420 U.S. 469 (1975).
[183] Jasmine E McNealy, *The Emerging Conflict Between Newsworthiness and The Right to be Forgotten* 39 N. Ky. L. Rev. 119 (2012), at 120.
[184] John Schwartz, *Two German Killers Demanding Anonymity Sue Wikipedia's Parent*, THE NEW YORK TIMES, Nov. 12, 2009, http://www.nytimes.com/2009/11/13/us/13wiki.html?_r=0.
[185] *Id.*
[186] *Id.*
[187] U.S. Senate, Senate Bill No. 568, http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.
[188] *Id.*
[189] McClure, *supra* note 113.

Despite the lack of a federal right to be forgotten in the U.S.A., it is of great importance to investigate whether there is any similar right to control personal information provided for in other U.S. laws. In U.S. criminal law, most states provide for a right for former juvenile offenders to be able to file a petition in court to expunge a juvenile court conviction. This sealing of the criminal history of an individual allows offenders to tell prospective employers, landlords, or licencing agencies that they have never been arrested or convicted.[190]

When taking a deeper look into the *property law*, *ownership* is central. It includes the right to exercise control over that property and the right to exclude other people from using or destroy the property. U.S. intellectual property law, including copyright, trademark, and patent law, extends property right to, among other things, *digital* property. The closest analogy to a right to delete data on the Internet is most likely copyright law, in which copyright holders have rights concerning production and distribution of copies of their original work.[191] The Digital Millennium Copyright Act (DMCA) enables, among other things, the copyright owners to have material taken down from the Internet, which infringes intellectual property rights. By filing a DMCA take-down request, the Internet Service Provider (ISP) is required to expeditiously remove, or disable access to, the allegedly infringing material. The data subject who posted the allegedly infringing material will be informed about the removal and may thereafter, when the content has been taken down, get a chance to appeal this decision. The whole process can go to court if the person who claimed intellectual property infringement still insists on having the content removed from the web and the alleged infringer does not accept a take-down. The DMCA "Safe Harbor" provisions stated in Section 512 of the DMCA[192] gives ISPs *immunity* from copyright infringement claims if they implement notice and takedown procedures. This aims to shelter service providers from the infringing activities of their customers and implies that only the infringing customer will be responsible for the content posted therein and liable for monetary damages, while the service provider's network, through which the person is engaged in the alleged activities, will not be liable.[193] However, such right to have content removed from the web has so far only existed for the protection of intellectual property law and not as a legal tool to be used for privacy reasons and purposes related to the right to be forgotten. In the wake of the decision in *Google Spain v. AEPD,* it remains to be seen whether Google chooses to adapt the DMCA takedown feature even for right to be forgotten related take-down requests.

[190] NOLO, Criminal Defense Lawyer, *Expunging of Sealing a Juvenile Court Record*, http://www.criminaldefenselawyer.com/topics/expunging-or-sealing-a-juvenile-court-record.
[191] Conley, *supra* note 35, at 55.
[192] *See* 17 U.S. Code, *supra* note 6.
[193] Chilling Effects Clearinghouse, Berkman Center for Internet and Society, *DMCA Safe Harbor,* available at https://www.chillingeffects.org/dmca512/faq.cgi.

4.5 The U.S.–EU Safe Harbor Agreement – Is it Still a Viable Compromise?

Even if the U.S.A. and the EU share the goal of enhancing privacy protection for all citizens as presented above, they still have different approaches to privacy. The differing concepts of privacy can be described as a battle between liberty and dignity.[194] While the U.S.A. rely on a mix of legislation, regulation, and self-regulation, the EU has a united legislation for all Member States. As a consequence of these differences in privacy approach, the strong privacy rights established in Directive 95/46/EC could have impeded the ability for U.S. companies, such as social network sites, to enable transatlantic transactions. In order to bridge these differences and enable for U.S. companies to transfer personal data from EU citizens to the U.S.A., the U.S. Department of Commerce and the European Commission developed a "Safe Harbor" Agreement.[195] The agreement implies that the companies, which would like to target European costumers or users, need to satisfy the requirement of an "adequate" level of data protection as stated in Directive 95/46/EC. The agreement, which creates a common ground in an unregulated cyberspace,[196] is signed on a voluntary basis and currently includes over 3 000 self-certified companies.[197]

When taking a deeper look at the privacy principles required in the Safe Harbor Agreement, it is clearly stated that individuals must be able to delete personal information where it is inaccurate. What looks like a right to be forgotten in a light version sets a precedent for enforcing stricter privacy standards in the U.S.A., but due to the voluntary spirit of the Safe Harbor Agreement, it is not binding for American states to embrace these standards.[198] Some of the companies who have adhered to certain data protection principles provided in the Safe Harbor Agreement are Facebook[199] as well as Google[200] and Twitter,[201] which may seem promising with regard to the future of transatlantic collaboration.

However, the trust in the "adequate" level of protection requirement for the EU citizens' personal data has been questioned after the recent disclosures that the secret program PRISM was used by the American National Security Agency (NSA) to get direct access to Internet giants' servers. Nowadays, most U.S.

---

[194] Hendel, *supra* note 133.
[195] *U.S.-EU Safe Harbor Agreement, supra* note 22.
[196] ALVERÉN, *supra* note 11, at 168.
[197] *U.S.-EU Safe Harbor Agreement, supra* note 22.
[198] Kamaal Zaidi, *Harmonizing U.S.-EU Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data*, 12 Mich. St. U. J. Int'l L. 169 (2003) at 176.
[199] Facebook on the U.S. - EU Safe Harbor List, http://safeharbor.export.gov/companyinfo.aspx?id=18810.
[200] Google on the U.S. - EU Safe Harbor List, http://safeharbor.export.gov/companyinfo.aspx?id=19795.
[201] Twitter on the U.S. - EU Safe Harbor List. http://safeharbor.export.gov/companyinfo.aspx?id=18888.

companies, for tax reasons, conduct their businesses through subsidiaries in the EU, which causes the companies to fully fall under the EU data protection laws despite the fact that the data is processed by a U.S. parent company. Now, these tax avoiding strategies have, after the PRISM revelation, lead to a challenging situation for the American companies where they have to abide by both EU privacy law and U.S. surveillance laws. When a European subsidiary send user data to the parent company situated in the U.S.A., this transfer of personal data is considered an "export".[202] The CJEU has interpreted Article 6 of Directive 95/46/EC[203] in the light of Article 8 ECHR,[204] and held that the forwarding and use of personal data for another purpose is interfering with the right to privacy enshrined in Article 8 ECHR. Such processing of data would only be legitimate if it is "necessary in a democratic society".[205]

The EU Commissioner Vivian Reding has therefore underscored that the Safe Harbor Agreement may not actually be safe at all, since it can be used as a loophole for data transfers across the Atlantic due to the fact that the U.S. privacy standards are not comparable to the high level contained within the EU. Therefore the EU Commission recently warned that the Safe Harbour Agreement has to be strengthened or it will be suspended.[206] One way of strengthening the transatlantic processing of personal data to enhance privacy laws even further might be through a new law that would require American companies to seek clearance from EU officials before complying with U.S. warrants that seek personal data.[207] President Barack Obama agrees, and in the Consumer Privacy Bill of Rights presented above, the Obama Administration plans to develop additional ways to strengthen the U.S.–EU privacy regarding data flow crossing the Atlantic. By using mechanisms such as jointly developed codes of conduct, which would support mutual recognition of legal regimes, it will create free flow of information and solve privacy challenges.[208]

---

[202] Europe v. Facebook, *Legal Actions against European Subsidiaries of Facebook, Apple, Microsoft, Skype and Yahoo filed*, June 26, 2013, http://europe-v-facebook.org/EN/en.html.

[203] Article 6 of Directive 95/46/EC sets requirements for processing of data, e.g. that the data must be processed lawfully and be adequate and relevant with regards to the purpose for which it was originally collected. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[204] Article 8 ECHR provides that everyone has a right to respect for his private and family life, his home and correspondence with no interference by a public authority. Full version available at http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[205] *See*, e.g. the decisions by the CJEU in the joined cases C-465/00, C-138/01 and C-139/01; Maximilian Schrems, *Complaint against Facebook Ireland Ltd – 23 "PRISM"*, June 25, 2013, http://www.europe-v-facebook.org/prism/facebook.pdf.

[206] *Press Release, European Commission, A Data Protection Compact, supra* note 84.

[207] James Kanter, *Rules Shielding Online Data From N.S.A. and Other Prying Eyes Advance in Europe,* THE NEW YORK TIMES, October 21, 2013, http://www.nytimes.com/2013/10/22/business/international/eu-panel-backs-plan-to-shield-online-data.html?_r=0.

[208] *White House, Consumer Data Privacy, supra* note 168.

4.6 A Short Summary of the Chapter

- The U.S.A has a patchwork of privacy legislations and relies on a mix of legislation, regulation, and self-regulation.
- While the U.S.A. has a robust history of protecting freedom of expression, privacy rights have constantly been subordinated.
- There is no federal right to be forgotten in the U.S.A., but the state of California recently passed a bill giving children a right to the first degree of deletion of personal data posted by themselves on a website. Take-down procedures already exist in the U.S.A., but only for intellectual property infringements and not for privacy claims of legitimately posted personal data.
- The Safe Harbor Agreement enables for data to be exported from the EU, which has a high level of data protection, to the U.S.A., which lacks strong protection.
- While the recent PRISM scandal is seen as a threat to the "adequate" level of data protection, the Consumer Privacy Bill of Rights proposed by the White House, might, on the other hand, enhance the privacy laws in the U.S.A. and reinforce and advance collaboration with the EU. The Consumer Privacy Bill of Rights is the result of a great collaborative work between Internet industry leaders and Congress to implement codes of conduct for enhanced privacy protection.

5 The Enforcement of the Right to Be Forgotten

5.1 Introduction to the Chapter

In the previous chapters, the different approaches to privacy law in the U.S.A. and the EU have been separately and comparatively presented while problematizing the collision between a right to be forgotten and freedom of expression online. The next part of this thesis puts the different approaches together and narrows down to focus on the right to be forgotten itself by investigating who can be held *responsible* for online deletion according to the GDPR. Now that we know from the decision in *Google Spain v. AEPD* that removal from a search engine does not equal removal from the whole Internet, this chapter investigates the issues of requiring a source website to delete. Facebook's deletion policy is used to exemplify this. In addition, the technical concerns entailed to a right to be forgotten are presented. Since a right to be forgotten might be hard to enforce, both legally and technically, without violating freedom of expression, this chapter aims to present alternative ways to enforcing such right through legislation. Additionally, this part of the thesis serves to present alternatives to a right to be forgotten that can better balance privacy and freedom of expression online while still protecting the digital persona.

5.2 Responsibility for the Right to Be Forgotten

After *Google Spain v. AEPD,* we now know that a data subject will be able to require the removal of links to websites that appears when searching for his or her name in a Google search. If Google does not remove the link, the Data Protection Supervisory Authority in each Member State can intervene and possibly go to court to force Google to take the links down. However, the right to be forgotten for a search engine does not imply deletion of the personal data from the whole Internet, since the content might still exist on the source website. Google's Head of Free Expression, Bill Echikson, has argued that "[…] only the original publisher can take the decision to remove such content" and "once removed from the source webpage, content will disappear from a search engine's index."[209] Do data subjects have a right to have their personal data deleted even from the original source, for example a newspaper website or a social media site?

[209] Helen Gaskell, *Google Must Respect 'Right to Be Forgotten' Rules EU Court,* ARABIAN INDUSTRY, May 14, 2014, http://arabianindustry.com/technology/news/2014/may/14/google-must-respect-right-to-be-forgotten-rules-eu-court-4699734/#.U33S9liSzKM.

5.2.1 Facebook's Privacy Policy and the Right to Delete

As an example of a source webpage, I have chosen to investigate Facebook and its deletion possibility. A right to be forgotten will undoubtedly affect U.S. social network sites since they have European users. To better understand the future clash, which will result as the privacy regulations are and will continue to be enhanced for EU citizens, it is interesting to take a look at the terms that European users have agreed upon. These agreements will most likely have to be amended when a right to be forgotten in 2016 will include even social network sites.

In 2012 Facebook reached one billion users.[210] According to the Eurobarometer survey done by the European Commission in 2011, only 54 percent of the Internet users know their privacy rights when signing up on social network sites.[211] Many users do not always understand and realize to what extent their created content is stored and whether they have any rights to retain over their personal information. The average privacy policy contains 2 514 words and takes ten minutes to read,[212] which with the length of the user agreements and their tendency of being written in a complicated fashion, causes many users to not in fact understand these unilaterally written agreements that are impossible to circumvent.[213] Most social network websites do not install default privacy settings. Therefore the users, who would like to opt-out manually, have to dedicate a lot of time and effort to protect their privacy.[214] A national telephone survey conducted by the University of Virginia and the University of California-Berkeley proved this statement to be correct: 54 percent of American adults falsely believed that if a website has a privacy policy, the site must comply with a request to delete information about a user by that user.[215]

As a main rule on Facebook, the users own all of the content and information they post on the social network.[216] However, for content that is covered by intellectual property rights, such as photos and videos, the company has a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any. This license ends upon deletion of the specific content, or of the whole Facebook account. An important exception to this is if the "content has been shared with others, and they have not deleted it", implying that the lease does

[210] Facebook Statistics, Statistic Brain, http://www.statisticbrain.com/facebook-statistics/.
[211] European Commission, Special Eurobarometer 359 - Attitudes on Data Protection and Electronic Identity in the European Union, June 2011, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.
[212] *See, e.g.,* Alexis Madrigal, *Reading the Privacy Policies You Encountering a Year Would Take 76 Work Days,* THE ATLANTIC**,** March 1, 2012, http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.
[213] Ed Markey, EU-U.S. Conference on Privacy, Speech, March 19, 2012, https://www.youtube.com/watch?v=mdD07BVBZbo.
[214] Madrigal, *supra* note 212.
[215] Conley, *supra* note 35, at 54.
[216] Facebook's Terms, *supra* note 112, at 2.1.

not end.[217]

Today Facebook gives the data subjects the opportunity to delete posts, pictures and similar information that they have shared. Facebook removes the data from the site, but for some of the information to be fully deleted, the company requires the data subjects to permanently delete their accounts, otherwise all personal data will be stored on Facebook's servers in case the data subject desires to re-active the account. This process may take about a month. [218]

Although Facebook promises the data subjects a right to delete personal data published online, there is oftentimes a doubt whether the data is actually deleted from their servers. A well-known case regarding Facebook's possession of user data concerns the Austrian law student Maximilian Schrems' request to Facebook in 2011 to provide him with all his personal data held by the company. He received 1,222 pages of posts, comments and pictures, of which many contained information that he had deleted, but which apparently still was saved.[219] Maximilian Schrems started the organization and website Europe v. Facebook after this revelation about the lack of deletion insurances,[220] and has filed several legal complaints regarding Facebook's privacy policy.[221]

75 percent of the Facebook users are outside the U.S.A. including a large amount of Europeans. [222] An important question to examine is whether Facebook's privacy policy follows European user based standards for data protection and whether it can be compatible with enhanced privacy rules as the right to be forgotten enters into force. As stated above, Facebook is a part of the U.S.–EU Safe Harbor Agreement.[223] Before the users can begin using the services of Facebook, they are required to sign a contract and agree to the terms. Users who live within the borders of the U.S.A. and Canada have a contract with the parent company Facebook Inc., based in California, U.S.A., while users outside the U.S. borders have a contract with the subsidiary company, Facebook Ireland Ltd, based in Dublin, Ireland.[224] According to the terms, it is clearly stated that Facebook strives to respect local laws, but that users outside the U.S.A, "have consent to having [their] personal data transferred and processed in the United States".[225] The CEO and founder of Facebook, Mark Zuckerberg, said that if he had the opportunity to "create Facebook again, user information would by default be public, not private

[217] *Id.*
[218] Europe v. Facebook, *Complaint against Facebook Ireland Ltd – 07 Messages,* Aug.18, 2011, http://europe-v-facebook.org/Complaint_07_Messages.pdf.
[219] Mona Tömböl; Philippe Schennach, *EU vs. Facebook: Fighting for the Right to be Forgotten*, THE VIENNA REVEW, Feb 5, 2013, http://www.viennareview.net/news/special-report/eu-vs-facebook-fighting-for-the-right-to-be-forgotten.
[220] Europe v. Facebook, available at http://europe-v-facebook.org/EN/en.html.
[221] Europe v. Facebook, *Legal Procedure against "Facebook Ireland Ltd",* http://europe-v-facebook.org/EN/Complaints/complaints.html.
[222] Facebook Statistics, *supra* note 110.
[223] Facebook on the U.S. - EU Safe Harbor List, *supra* note 199.
[224] Facebook Inc, Facebook's Terms, *supra* note 112, at 18.1.
[225] *Id.* at 17.1.

[…]"[226] The rise of social networking online means that people no longer have an expectation of privacy,[227] and that the users should "get over it…nobody cares about privacy any longer."[228] The idea of a more public Internet shines through in Facebook's Terms, where it is stated: "When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture)".[229]

5.2.2 Responsibility According to the GDPR

Facebook is not directly affected by the ruling in *Google Spain v AEPD*, but will most likely have to revise their Terms and privacy policy as the GDPR enters into force. There are currently no penalties for the companies who do not comply with the law, but the GDPR will make big companies more vulnerable to enforcement actions.[230] Non-compliance with the rules will be punishable by the national data protection authorities, which will be able to apply penalties up to $ 1.3 million or two percent of the company's annual turnover.[231] A couple of fines like that would really shake their business model. When the right to be forgotten becomes law a controller who has made the personal data public will, according to Article 17(2) of the GDPR, be obliged to "inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data".[232] The controller will have to take steps, including technical measures, to erase the data for which it is responsible. If the controller has *authorized* a third party publication of the data, the controller is considered *responsible* for the publication of such data and thereby also the deletion of it. The fact that a right to be forgotten does not exist on a federal level in U.S.A. does not mean that U.S. companies can be irresponsible when handling personal data that belongs to European users online.[233] Viviane Reding noticeably expressed: "If data is going to flow outside the EU it is going to have be subject to the same high levels of data protection as data within EU member states. And that is very reassuring for users of services like Facebook and Google".[234] As mentioned above, European Facebook users are in a contract relationship with Facebook Ireland Ltd and not directly associated with the mother company, Facebook Inc. This means

---

[226] Marshall Kirkpatrick, *Facebook's Zuckerberg Says the Age of Privacy is Over,* READ-WRITEWEB, Jan. 9, 2010, http://www.readwriteweb.com/archives/facebookszuckerbergsaystheage-of-privacy-is~ov.php.
[227] Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder,* THE GUARDIAN, Jan. 10, 2010, http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy. (Highlighting Zuckerberg's opinions on individuals' level of privacy expectations in the online social media world).
[228] ALVERÉN, *supra* note 11, at 151.
[229] Facebook's Terms, *supra* note 112, at 2.4; *See* also Emily Adams Shoor, *Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation*, 39 Brooklyn J. of Int'L, 514 (2014).
[230] BBC News, *supra* note 95.
[231] *Id.*
[232] *General Data Protection Regulation, supra* note 3.
[233] BBC News, *supra* note 95.
[234] *Id.*

that Facebook needs to follow European data protection rules for their European users. However, since the European user data is being sent to the U.S.A., the data protection needs to satisfy an "adequate" level, according to the U.S.–EU Safe Harbor Agreement. There are still many U.S. companies who have not yet signed the Agreement and it is therefore interesting to investigate whether U.S. law sets up any requirements for U.S. based websites to delete personal data.

5.2.3 Communications Decency Act Section 230 – No Obligation to Delete Personal Data in the U.S.A.

Under common law principles in the U.S.A., a person who published a defamatory statement has the same liability for the statement as if he or she was the creator of it. A publisher of a book or a newspaper will therefore be liable for all such content since he or she has the knowledge, opportunity, and ability to exercise editorial control over such content. With the rise of the Internet and the existence of a great amount of data on each website, the possibility for publishers to control all the content on the sites they host is very small. It would lead to an impossible editorial role and potential censorship if the same rules applied in the online world as in the offline world. The American Government has therefore tried to support freedom of expression in the digital environment by enacting the Communication Decency Act (CDA) of 1996.[235]

According to the so-called "Good Samaritan provision" under Section 230 of the CDA, "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[236] An *interactive computer service* means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server.[237] Simply put, Section 230 of the CDA provides immunity for website hosts from tort claims arising out of their publication of user-generated content, defamatory or not, posted by third parties on their website.[238]

This immunity from tort liability is granted to interactive services of all types, such as search engines, websites, blogs, forums, and listservs. It means that the website host shall not be treated as a publisher in, for example, a physical newspaper with responsibility for the content therein.[239] Through the ruling in

[235] 47 U.S. Code § 230 – Protection for private blocking and screening of offensive material, http://www.law.cornell.edu/uscode/text/47/230.
[236] *Id.* at (c)(1).
[237] *Id.* at (f)(2).
[238] BRIAN CRAIG, CYBERLAW – THE LAW OF THE INTERNET AND INFORMATION TECHNOLOGY 153 (2013).
[239] Digital Media Law Project, Berkman Center for Internet and Society at Harvard Law School, *Immunity for Online Publishers Under the Communications Decency Act*, http://www.dmlp.org/legal-guide/immunity-online-publishers-under-communications-decency-act.

Klayman v. Zuckerberg[240], Facebook is now qualified as an "interactive computer service" under the CDA, since it is acting as the publisher of user-created Facebook pages.[241]

Section 230 of the CDA prevents the website owner from being held liable for deleting material that it considers harmful, unless the plaintiff can show that the website owner was personally involved in the creating of the illegal content.[242] Courts applying Section 230 of the CDA often use a three-pronged test to find out whether: (1) the online entity uses or provides interactive computer services; (2) the entity is an information content provider with respect to the objectionable content; and (3) the plaintiff seeks to treat it as the *publisher or speaker* of information originating with a third party.[243] Section 230 can be seen as a clear free speech law, which is necessary for the existence of a free and open cyberspace. It allows Yelp to host reviews, Craigslist to host classified ads, and Facebook and Twitter to host users' posts.[244] Without Section 230, websites which include user-generated content would most likely operate less efficiently, be more expensive, and, they might be motivated to censor the content on the websites they host. The Electronic Frontier Foundation (EFF), eager to protect freedom of expression online, stresses that, "website operators and Internet service providers host and carry enormous amounts of speech and are in no position to evaluate the legality of what their users do".[245]

There would not be many websites that entail free expression if the host would be liable for every post therein. What does this immunity for hosts mean with regards to the right to be forgotten? Section 230 of the CDA has mostly been used to protect hosts from defamatory content posted on their website. When asked to remove such content, the host may *not* be forced to do it, unless the host has *promised* to remove and fails to do so.[246] This means that the CDA will not be compatible with a right to be forgotten. The CDA is tailored for the

---

[240] *Klayman v. Zuckerberg*, 2012 WL 6725588, D.D.C. Dec. 28, 2012.
[241] *Id.*
[242] CRAIG, *supra* note 238, at 153.
[243] 47 U.S. Code § 230 – Protection for private blocking and screening of offensive material (Communications Decency Act); American Law Reports, *Validity, Construction, and Application of Immunity Provisions of Communications Decency Act, 47 U.S.C.§ 230*, 52 A.L.R. Fed. 2d 37.
[244] Susanna Lichter, *Unwanted Exposure: Civil and Criminal Liability for Revenge Porn Hosts and Posters,* Harvard Journal of Law and Technology, May 28, 2013, http://jolt.law.harvard.edu/digest/privacy/unwanted-exposure-civil-and-criminal-liability-for-revenge-porn-hosts-and-posters.
[245] Electronic Frontier Foundation, *CDA 230 The most important law protecting Internet speech*, https://www.eff.org/issues/cda230/infographic.
[246] *See* e.g. *Barnes v. Yahoo!,* Inc., 570 F.3d 1096 (9th Cir. 2009), where Cecilia Barnes' ex-boyfriend had created fake profiles of her on a Yahoo! Site containing nude pictures and solicitations for sexual intercourse. After contacting Yahoo! requiring them to remove the content, an employee at Yahoo! promised to delete the profile. The content was never removed, which lead to a lawsuit, in which the court used the legal principle of "promissory estoppel". This means that a host, which has promised to remove content – despite the fact that they fall under the Section 230 immunity – might be held responsible for the consequences on another person's reasonable reliance on that promise. In this case, Barnes had such reasonable reliance on the promise from Yahoo!.

U.S.A., with a strong free expression right. However, the immunity provided for in Section 230 of the CDA is not absolute and may be restricted. For example, if a website owner invites to postings of illegal materials or is the author of any defamatory material posted therein, the CDA may not apply.[247] There is no such immunity for website hosts with regards to tortious material in the EU.

Section 230 provides for the possibility of a *user* of interactive computer services, for example a Facebook user, to post and by republication spread defamatory statements, which may be harmful for another person's reputation - and the service provider does not have to take any actions to delete the postings.[248] The court has upheld immunity even after a service provider has unreasonably delayed in in removing defamatory messages posted by a user on the website and failed to take measures to prevent similar incidents from occurring.[249] Providing a broad immunity can foster irresponsibility.[250] "Unfortunately, courts are interpreting Section 230 so broadly as to provide too much immunity, eliminating the incentive to foster a balance between speech and privacy. The way courts are using Section 230 exalts free speech to the detriment of privacy and reputation."[251]

5.2.4 Is the Right to Be Forgotten *Technically* Possible?

The GDPR sets high requirements that data controllers must take even *technical* measures to delete undesired personal data online. However, the decision in *Google Spain v. AEPD* does not give any indicators on how this will be done or whether deletion at all is *technically* possible.

During the interview with David Larochelle, the Lead Engineer for Media Cloud at the Berkman Center for Internet and Society at Harvard Law School, Mr. Larochelle underlined that tracking a public tweet or Facebook post is easy. If it is on the Internet, Google or other search engines will find it. He said that "if they don't find it, then arguably the post effectively doesn't exist. Making websites [*delete*] the information is more complicated".[252] However, one complicating factor in searching for content is the fact that users often take screen shots and copies of content, which can later be reposted on the Internet. Additionally, searching for image content is much harder than searching for text.[253] Internet co-founder Vint Cerf[254] agrees with this and stresses that it is "very, very hard to get the Internet to forget things you don't want to remember

[247] *Whitne Information Network, Inc. v. Xcentric Venture, LLC,* 199 Fed. Appx. 738 (11th Cir. 2006).
[248] *Barrett v. Rosenthal*, 40 Cal. 4th 33 (2006).
[249] *Zeran v. AOL,* 129 F.3d 327 (4th Cir. 1997); Barnes v. Yahoo, inc., 570 F. 3d 1096 (2005).
[250] *Id.*
[251] *Id.*
[252] Interview/e-mail correspondence with David Larochelle, Lead Engineer Berkman Center for Internet and Society at Harvard University Law School, Eslöv, Sweden – Boston, USA, April 9, 2014.
[253] *Id.*
[254] Vint Cerf now works for Google as its Chief Internet Evangelist.

because it's easy to download and copy and re-upload files again".[255] The fact that the same data may be used in many ways and stored on servers that are not controlled by the data controller will lead to a situation where deletion of data may be technically unfeasible.[256]

When discussing remembering and forgetting on the Internet, David Larochelle pointed out that "the conventional wisdom is that the Internet paradoxically makes it very difficult to both delete and preserve information."[257] This thesis focuses on the difficulties for the Internet to *forget* personal information since it is programmed to remember. However, there is an existing problem of link rot,[258] which implies that information actually involuntarily disappears from the web.[259] There was recently a discussion at Massachusetts Institute of Technology (MIT) on how to *irrevocably* publish information. The proposed suggestion to encode the data in a bitcoin transaction block would most likely be the solution that best could resist legal and technical attacks. However, the downside is that it would be far beyond the reach of the average Internet user.[260]

5.3 Non-legislative Solutions to Enforce a Right to Be Forgotten

Since the technically enforceability of a right to be forgotten seems to be a major problem, a legislated right to be forgotten might be a hard burden to place on companies. As seen both in the GDPR and in the *Google Spain v. AEPD* decision, there is a great need, on both sides of the Atlantic, to find a balance between the two fundamental rights of free expression and privacy. In the U.S., Christopher Gibson, Professor of Law and Associate Dean at Suffolk University Law School in Boston, is clear in his statement that a right to be forgotten in the U.S.A. cannot exist right now since it would violate the historically strong First Amendment rights: "A right to be forgotten in U.S.A. would require a new federal statute".[261] On the European side, Ulf Maunsbach, a Swedish Professor of Law at the Faculty of Law at Lund University, predicts that the right balance in the conflict between the right to be forgotten and our free speech rights will be hard to achieve. Even if it is possible to maintain a right to be forgotten, it will be hard to enforce it. He discusses the responsibility issue when implementing such a right and believes that the

[255] Warman, *supra* note 121.
[256] AmCham EU, *supra* note 120.
[257] Interview with David Larochelle, *supra* note 254.
[258] *See*, e.g. Felix Salmon, *The Spread of Link Rot,* REUTERS, June 28, 2013, http://blogs.reuters.com/felix-salmon/2013/06/28/the-spread-of-link-rot/.
[259] *See*, e.g. Internet Archive, which is an Internet archive building a digital library of Internet sites and other cultural artifacts in digital form, www.archive.org.
[260] Interview with David Larochelle, *supra* note 254; Jeff Stibel, *Die, Links, Die! How Link 'Suicide' Can Save the Web,* WIRED, July 31, 2013, http://www.wired.com/2013/07/die-links-die-stop-worrying-about-link-rot/all/1.
[261] Interview with Christopher Gibson, Associate Dean and Professor of Law, Suffolk University Law School, Boston, U.S.A. (Nov. 26, 2012).

service providers are the best entitles to carry the burden, even if it might be hard to do in reality: "Even if Google is a large company, it is not reasonable to force them to 'vacuum clean' the whole net in their search for information that somebody for privacy reasons may have a right to delete".[262] The ruling in *Google Spain v. AEPD* has been criticized for creating a loophole for online censorship. The right to be forgotten provided for in the GDPR might add even more justification for this criticism, which creates a demand to find alternative ways to reach the balance between freedom of expression and a right to be forgotten. I have therefore investigated other ways to reach similar results, where *legislation* does not stand out as the most attractive solution.

5.3.1 Enabling the Right to be Forgotten Through Social Norms on the Internet

Since binding legal requirements are politically very difficult to implement and enforce, market pressure through social norms might be a good option in the attempt to establish a right to delete.[263] A social norm is a rule of conduct, often improper to transgress. There is no actual punishment since norms are not fixed in binding law.[264] If Internet users can agree on the fact that individuals deserve a right to their own digital persona, which would also include content about them held by third parties, a *legal* change is not needed to establish a right to delete. Instead, changing consumer expectations would put pressure on companies holding personal data to adapt their actions to the new social norms. It would, of course, be hard to force companies, whose business models depend on monetizing records about individuals, to comply with this. Even those companies will eventually feel the public pressure and an increasing public demand for control over personal information.[265] Facebook's CEO, Mark Zuckerberg, has stated that Facebook will follow the norm that exists in society for how people want their data to be used. So far Facebook has made user data more public and accessible for other people as opposed to private and personal. Facebook has, on the other hand, made changes in its Terms of Service and recently gave the users a right to delete content that they post on Facebook.[266] Consequently, it is an obvious truth that Facebook users have to require a stronger privacy protection of their private data, or there will be no change.[267] Changes in social norms will slowly turn into voluntary agreements and collaboration. The cooperation between the leading online companies and the U.S. Congress, which resulted in the proposal to the Consumer Privacy Bill of Rights, can as well as the U.S.–EU Safe Harbor Agreements state a good example. When large online companies like Google and Facebook sign these agreements, it clearly shows the important role that these companies have in

[262] Interview/e-mail correspondence with Ulf Maunsbach, Professor of Law, The Faculty of Law at Lund University, Boston, U.S.A. – Lund, Sweden (Nov. 28, 2012).
[263] Conley, *supra* note 35, at 58.
[264] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION 84 (2007).
[265] Conley, *supra* note 35, at 58.
[266] Brian Stelter, *Facebook's Users Ask Who Owns Information.* The New York Times, Feb. 17, 2009, http://www.nytimes.com/2009/02/17/technology/internet/17facebook.html?_r=0.
[267] ALVERÉN, *supra* note 11, at 213-214.

the context of changing attitudes and uniting a fragmented legal regulation in the area of data protection. The changes made by big online companies will most likely also work as role models for smaller companies using personal data.

5.3.2 Expiration Dates for Data

Professor Viktor Mayer-Schönberger proposes *expiration dates* for information. He believes that we are not losing enough data and that we are failing to forget[268] and therefore suggests that we, in order to save personal data, should be required to put a desired deletion date on it. Without this metadata tagged to the original information it would not be possible to save it. Mayer-Schönberger argues that expiration dates on data encourages the thinking of whether expiration of data needs to become the new default in our minds in order to take us back to human-controlled forgetting, as opposed to the present flawless remembering in the digital age.[269]

> Expiration dates are not about imposed forgetting. The main idea of using expiration dates on data would primarily be to force users to reflect over the potential lifespam of their data. They are about awareness and human action, and about asking humans to reflect – if only for a few moments – how long the information they want to store may remain valuable and useful.[270]

The goal with expiration dates is to limit the amount of irrelevant data in cyberspace.[271] At the same time one may think that expiration dates will shake the business models of Google and Facebook and other companies whose survival is depending on the *retaining* of personal data. It is a correct statement that data will disappear from cyberspace. However, deletion of less relevant information and improved focus on present and up-to-date information will in fact increase the quality of the digitally stored information and essentially make Google's search matches more accurate. *This* is something that will enhance such a business model at the same time as it creates *trust* among the consumers.[272]

The most important variable when discussing expiration dates are *time* and *power*. The '*time'* challenge of digital remembering that is to be addressed though expiration dates; for how long time do we want to certain information to be remembered? Expiration dates makes us "act in time" without any burden from comprehensive and flawless digital memory as forgetting performs an important function in human decision-making.[273]

Even if Mayer-Schönberger underscores the time challenge as the most important measure with regards to expiration dates, there is subsequently also a

[268] Connolly, *supra* note 127.
[269] MAYER-SCHÖNBERGER, *supra* note 1, at 172.
[270] *Id.*
[271] *Id.* at 189.
[272] *Id.*
[273] *Id.* at 194.

'power' challenge: when the users have power to set their own expiration date on their data, there will consequently most likely be a shift in power and control over ones personal data. A shift in power from the surveyors to the surveyed.[274] The loudest debate regarding expiration dates has been whether it should be up to the individual to set his or her own expiration time on personal information, or if it should be the legislators' role to make such decisions automatized. The core goal of expiration dates for information is to *not* automatize it, to "not push the problem of digital memory off our consciousness by delegating it to technology, but rather the opposite: to make humans aware of the value and importance of forgetting".[275]

5.3.2.1 Are Expiration Dates *Technically* Enforceable?

A right to be forgotten through expiration dates – is it *technically* enforceable? Since expiration dates would be considered just another meta-data linked to other information, expiration dates would be easy to implement. Just like a digital picture may have meta-information added to it - such as the date and time it was taken - expiration dates may be seen as just an additional meta-information: information about information's life expectancy.[276] Despite this, it will of course be hard to remove the copies of the data that has been downloaded and saved on a desktop. The ability to track such information is impossible. However, Mayer-Schönberger promotes four ways in which expiration dates are a modest response to the demise of forgetting: (1) technically, expiration dates utilize ideas, infrastructures and mechanisms that already exist, or would require just small modifications; (2) legally, there is no need to rely on any new rights or institutions sine expiration dates a default of forgetting that has many similarities to our analogue world; (3) expiration dates are modest in the way they regulate human behaviour, which also includes software and law; (4) politically, expiration dates seems to be more acceptable than a regulatory approach at the same time as they are not extremely controversial.[277]

5.4 Alternative Ways to Find a Balance Between Privacy and Freedom of Expression

A right to be forgotten to its full extent most likely would have a chilling effect on freedom of expression. Are there any alternative ways to a right to be forgotten that could better balance privacy with freedom of expression while still enabling protection for the digital persona?

[274] *Id.* at 191-192.
[275] *Id.* at 185.
[276] *Id.* at 173.
[277] *Id.* at 190.

5.4.1 Contextualization

Facts show that 78 percent of U.S. adults look up information about other persons online before they decide to interact with them. This percentage is relevant also for businesses before deciding to do business,[278] which is a reason to why online reputation also has become increasingly important in today's *offline* society. As an alternative to tracking down all existing copies of the original data that a data subject desires to erase in order to be fully forgotten, the practice of *contextualization* could be an option that works in the contrary direction. Instead of *deleting* information, contextualization would allow users to *add* more information.[279] The new information would hereby link to the original post or photo with a possibility for the original owner of the information to add his or her own explanation and thereby put the original data in the desired *context*, which would smother the negative information with a greater amount of positive information and explanations.[280] This method is obviously most relevant for the third degree of deletion: when *someone else* has written something *about* the data subject. Its enforcement in reality depends, however, on the data subject's eagerness to constantly monitor the existing content about him or herself online.[281] Contextualization could most successfully be applied to searches on a search engine. In 2007, Google experimented in this area by introducing a feature to its Google News aggregator, which allowed for individuals who were mentioned in articles, which were indexed by Google News, to add a comment that would appear next to the article.[282] Such comment could be an explanation of the information contained in the article, as well as an apology or an argument to why the readers should disregard the content. However, Google, later on abandoned this feature, which in the wake of the decision in *Google Spain v. AEPD* has been criticised since such function could allow to give data subjects more influence over their information "without giving [them] the power to censor".[283]

---

[278] Nielsen, Harris Interactive, more information available at http://www.harrisinteractive.com/.
[279] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET – AND HOW TO STOP IT 91-94 (2008).
[280] ALVERÉN, *supra* note 11, at 194.
[281] The business model of helping people protecting their online reputation and controlling what exists about them on the Internet is in fact already used by various companies. Among them is Reputation, which helps you follow what is said about you on the net, how many people that are searching for your name, and whether the results that come up are positive or negative. Reputation can also help you to push negative content to the bottom of the search and push up the good content, Reputation.com, more information available at http://www.reputation.com/reputationdefender.
[282] Dan Meredith; Andy Golding, *Perspective About the News From People in the News*, GOOGLE NEWS BLOG, Aug. 7, 2007, http://googlenewsblog.blogspot.se/2007/08/perspectives-about-news-from-people-in.html.
[283] Zittrain, *supra* note 145.

5.4.2 A Human Approach to New Technology Through Cognitive Adjustment

When discussing the future of forgetting in the digital age, it is important to consider which approach to new technology is the most optimal. Researchers, such as Danah Boyd at the Berkman Center for Internet and Society at Harvard Law School, stresses that we have to adapt our culture to modern technology. We need to assume that people can change, and the best way to accept this is to merely look at most *recent* behavior and opinions of the data subjects in, for example, a Google search about that individual.[284] Danah Boyd believes that we will be able to adjust our cognitive processes to better deal with digital remembering. This way we will not be depending on a legalized right to be forgotten since the attitude towards forgiving and human development will change. The solution is *not to fight* the propagation of memory, but to *adapt* to it. Her idea is that no structural invention can combat this: "people, particularly younger people, are going to come up with coping mechanisms. That's going to be the shift, not any intervention by a governmental or technological body."[285] The idea of cognitive adjustment is simple since it does not require any changes in the society through laws or a new technical architecture. The changes will solely take place in our minds. By adapting this way, our way of thinking will change and go back to a more human approach to remembering and forgetting. The big question that remains to be answered is how long time such change will take.

5.5 A Short Summary of the Chapter

- The responsibility for Google and other search engines to remove *links to* personal data was decided in *Google Spain v. AEPD*.
- The responsibility for actual *deletion* from the source website, is according to Article 17(2) of the GDPR, for data controllers to *inform* third parties, which are processing such data, that a data subject requests them to erase any links to or copies of that data. If the controller has *authorized* a third party to process personal data, the controller will be *responsible* for the deletion.
- There is no responsibility for website hosts in the U.S.A. to delete any content posted by a third party on their website, since Section 230 of the CDA gives websites liability immunity to foster freedom of expression.
- According to technical experts, a right to be forgotten might be technically hard to enforce since copies of the data can be saved on other places outside the Internet.
- Due to the technical difficulties and considering the fact that websites also have a duty to enable free expression, a legislated right to be forgotten might be a hard burden to put on companies and risk transforming the website hosts to censoring machines. Non-legislative

[284] MAYER-SCHÖNBERGER, *supra* note 1, at 154.
[285] Winter, *supra* note 33.

ways to enforce a right to be forgotten could be through social norms and voluntary agreements, or through expiration dates for personal data.

- Alternatives to a right to be forgotten, that will be easier to enforce and better balance privacy and freedom of expression online while still protecting the digital persona are, for example, contextualization and cognitive adjustment.

6 Analysis: Humanizing the Digital Age?

6.1 Introduction to the Chapter

With the GDPR and *Google Spain v. AEPD* as a base, the previous chapters have presented the challenges that the right to be forgotten is facing by digging deeper into (a) **remembering and forgetting in the digital age**; (b) the **transatlantic clash** between privacy and freedom of expression in the EU and the U.S.A. as well as; (c) the **enforcement of the right to be forgotten** by investigating the responsibility issue and alternatives to such right. To make it easier for the reader to follow my train of thoughts, the same structure is used in this analyzing chapter.

To find out whether there is a way we can protect our digital persona and humanize the digital age while finding a balance between privacy and freedom of expression in our global online network, it is of great importance to refresh and analyze the questions that were asked in the beginning, and have been elaborated on throughout this thesis:

- What is the importance of remembering and forgetting in the digital age?
- What does the current landscape of privacy law and freedom of expression law look like in the EU and the U.S.A.?
- Can a right to be forgotten exist in the U.S.A.?
- To what *extent* is it currently feasible to extend a right to be forgotten according to Article 17 of the GDPR without violating the freedom of expression online?
- Is the U.S. - EU Safe Harbour Agreement[286] still a viable compromise?
- Who may be held *responsible* for a right to be forgotten under Article 17 of the GDPR and according to the CJEU decision in *Google Spain v. AEPD*?
- Is *legislation* the best way of enacting a right to be forgotten, or are there any non-legal ways that will better balance privacy with freedom of expression while still protecting our digital persona?

6.2 Remembering and Forgetting in the Digital Age

Time heals all wounds, memory fades, forgive and forget. We have all heard it, and we certainly all know the meaning of it. Are these expressions still

[286] U.S. Department of Commerce, U.S. – EU Safe Harbor Agreement (2000), http://export.gov/safeharbor/ [hereinafter *U.S.-EU Safe Harbor Agreement*].

applicable, or are they merely relegated to the past? Due to digitalization, cheap storage, easy retrieval and global reach we are now facing an enormous transformation from the analog system, where indiscretions could be erased or overcome by time, to a web with a flawless memory that fails to forget. Through the use of digital memory, we have undermined the biological process of forgetting. We have travelled from the time of *forgive and forget* to a period where we cannot "unring the bell" – where we have the inability to be forgiven and forgotten. The American Psychiatrist Gerald Jampolosky once said: "Forgiveness means letting go of the past". As we live in a digital age where "our pasts have become etched like a tattoo into our digital skins,"[287] and remembering, as opposed to forgetting, has become the new default, it is now harder than ever before to forgive.

All the data we share online creates a picture of us, a *digital persona*, and the seamy side of the Internet is that our reputation may be tainted or our privacy compromised with a simple click of the mouse. In the introduction of this thesis I mentioned the case of Stacy Snyder. She wanted to become a teacher, but due to the existence of an inappropriate picture on a social network site showing her wearing a pirate's hat and holding a cup, she was rejected from the teaching job she was applying for. This case clearly shows that our online behavior can result in consequences even offline, making a right to be forgotten vital. Giving the citizens such a right will not only protect your online reputations, but it will also make the ever-lasting memory of the web more human. Yet, is it really the optimal solution when viewed from a *global* perspective?

6.3 The Transatlantic Clash

Due to the global nature of the Internet, European user data is constantly crossing the borders through the use of online services from U.S. websites and search engines. This creates a great need to take the fundamentally different approaches to privacy rights in the EU and the U.S.A. into account when investigating the global implications of a right to be forgotten, and whether such a right could work not only in the EU, but in the USA as well. The difference in approaches to privacy rights can be attributed to America's unilateral protection of the freedoms of expression and the press under the First Amendment, as well as the Europeans inclusion of the countervailing right to personality in Article 8 ECHR. It is a question of liberty versus dignity.

The different attitudes to privacy across the Atlantic are clearly presented in the *Wikipedia* case. If you recall, the names of two former criminals were removed from the German Wikipedia page, but not from the English-speaking site since publication of someone's criminal history is protected by the First Amendment in the U.S.A. and a removal from the Wikipedia site, according to U.S. free speech advocates, would imply "editing of history".[288] *Newsworthiness,*

[287] MAYER-SCHÖNBERGER, *supra* note 1, at 127.
[288] Granick, *supra* note 180.

meaning a right for the public's right to be informed, was a clear argument for retaining the information.

6.3.1 Google Spain v. AEPD and the Responsibility For Search Engines According to Directive 95/46/EC

Newsworthy information was also a topic of discussion in *Google Spain v. AEPD*, where the court stated that information of great public interest will not be deleted from a Google search. Due to the lack of explanation in the court decision of how to interpret the exception for public interest as stated in Article 7(e) of Directive 95/46/EC, I anticipate problems when trying to fit the *newsworthiness* requirement for publication of personal information with *the right to be forgotten,* as no one will ever know what will be newsworthy in the future. According to the decision, Google will be required to delete: "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed".[289] What will happen when an ordinary person, who has erased all the links connected to him or her, later on becomes of public interest? Or, if the *opposite* occurs; how can a search engine determine when a previously public figure no longer is subject to any newsworthy information of public interest? By allowing individuals to ask search engines to remove personal data, data subjects will get a right to delete links to embarrassing vacation pictures that could interfere with their future employment, like in the Stacy Snyder case. On the other hand, such a right will also create to a possibility for political candidates to delete links to pictures from violent protest auctions. It might also give the individual who is applying for a CEO position for a public company the ability to delete links to xenophobic comments that he or she made in a newspaper, a blog or a social media website. Are we really willing to give up our freedom to access information for a right to remove our own links on Google? I believe that in a collaborative Internet there is a need to give information to be able to receive information. Are search engines the right entities to determine whether these candidates for jobs or political positions are of *public interest* yet and thereby fall under the exception in Article 7(e) of Directive 95/46/EC? Is it reasonable to place that burden on a technical online company? The CJEU, in *Google Spain v. AEPD,* did not draw any line for what is considered out-dated or irrelevant. Due to the unspecified decision regarding what may or may not be a violation of data protection according to Directive 95/46/EC, it pushes the responsibility to the search engines to, on a case-by-case basis, make arbitrary assessments of which information that can or cannot be deleted. The *European* approach to newsworthiness used in the French *right to oblivion* and in the Wikipedia case, appears to be a good compromise between privacy and expression. It primarily gives the press its freedom of expression right and at the same time satisfies society's right to access the information, and once criminals have served their sentence, it gives *them* a right to a "clean slate".

[289] *Google Spain v. AEPD, supra* note 21.

The correct decision maker should, in my opinion, be the court itself. Deciding such issues on a case-by-case basis will require large teams of staff in every technology company, teams critics fear will be extremely costly.[290] Google already provides the right for copyright owners to have DMCA infringing material taken down.[291] In May 2014, Google received 25 million take-down requests.[292] When adding privacy complains to this great amount, the responsibility question for deletion might be a great hurdle for many companies. This is not something that can be helped simply by adding a new algorithm, this process is totally dependent on human decision-making. In making a wrong decision, they might face the interference by the national data-protection supervisory authority, or in a worst-case scenario - a lawsuit. I believe, in line with Professor Jonathan Zittrain's argument, that the search engines will err on the safe side of caution and accepting to most of the takedown requests in order to avoid extremely costly lawsuits. A potential lawsuit will, from the complainant's perspective and for the sake of "forgetting", most likely lead to the opposite effect. As the information will be publicized more widely due to the fact that a court decision is a public record, the so-called "Streisand effect"[293] may be the consequence. This was ironically and obviously the truth for Mr. Costeja in the case. Perhaps this is something that would make people think twice before making privacy based take-down requests to Google.

The decision by the CJEU to determine search engines as "processors of information" was correct, since that is obviously their function when they are "collecting, recording, organizing […] and making information available" for other people as defined in Article 2(b) of Directive 95/46/EC. However, there is a distinction between "processing" the information and "controlling" the information as provided for in Article 2(d) of the Directive. In line with Advocate General Jääskinen's opinion, I argue that Google has no *knowledge* of whether the information they process is personal data or other types of data since Google is merely automatically getting the information through web crawlers - and should therefore not be deemed controllers of personal data. Yet, the court did not put any weight on the lack of knowledge regarding the type of information search engines are processing and determined Google to be a "controller" of personal data. *Google Spain v. AEPD* thereby sets a clear precedence in the EU. It might work right now as Google is the most frequently used search engine in the EU. With curiosity I speculate what a downfall for Google in market shares will imply for the users in the future. Will users have to ask each search engine, which has indexed their personal data, to remove the link between their name and the original source webpage? Since nobody knows what the future of the rapidly changing online environment will look like, I can merely predict that a future with more

[290] James Ball, *'Right to Be Forgotten' Ruling Creates a Quagmire for Google et al,* May 13, 2014, THE GUARDIAN, http://www.theguardian.com/commentisfree/2014/may/13/right-to-be-forgotten-ruling-quagmire-google.
[291] Google, Removing Content from Google, https://support.google.com/legal/troubleshooter/1114905?hl=en.
[292] Goldman; Dexe, *supra* note 154.
[293] RationalWiki, *Streisand Effect*, http://rationalwiki.org/wiki/Streisand_effect.

competing search engines will lead to a greater work load for the data subjects to protect their digital persona. Perhaps this potential extra workload is something that will make people less eager to delete, and the problem of a great amount of take-down requests will resolve itself.

In fact, by requesting a search engine to delete the *link* to personal data we are not solving the problem of actual "forgetting". *Google Spain v. AEPD* is not a about deleting or forgetting content, but making it harder to find, as underlined by Peter Fleischer, Google's Privacy Counsel.[294] Since a search engine only is eligible to erase the link between the name of the data subject and the source webpage, the actual information that a data subject wants to forget still exists on the Internet. This can be comparable to a big library where you know that the book you are looking for is somewhere, but where the index telling you were to find it is gone. Google's Head of Free Expression, Bill Echikson, stated that a better way to delete information is by going to the original *publisher* of the information and once it is removed from the source webpage, the content will disappear from a search engine's index. I agree, and I think this is how we best can reach a right to be forgotten.

For a deletion right from a source website to occur the EU citizens will have to wait until 2016, when the data subjects will get a right to delete any personal data related to them, as provided for in Article 17(1) of the GDPR. This is also, however, where the real collision with freedom of expression becomes evident, since it will require not just Google to "hide" data, but for websites to actually *delete* information that someone has posted. Viviane Reding has diplomatically stated that there is no right that is absolute and that a right always goes as far as it can until it conflicts with another right. In this thesis I have tried to determine when this collision actually occurs and how to find the right balance between the two fundamental rights.

6.3.2 How Far the Right to Be Forgotten Can Be *Extended* Before it Violates Freedom of Expression

Article 17(3) of the GDPR provides for an exception from deletion *for exercising the right of freedom of expression*. Since it lacks an *actual* explanation on how far a right to be forgotten for EU citizens can be extended before violating freedom of expression, I tried to reach a resolution by dividing deletion into three accelerating degrees: (1) If the data subject post something online; (2) if someone else *copies* the personal data of the data subject; and, (3) if *somebody else* publicly writes something *about* the data subject that he or she would like to delete.[295]

When signing up for a user account on Facebook, the users are promised a right to delete personal data that they have posted on the social network site. This is a degree of deletion that is already fulfilled by Facebook and most

[294] *Fleischer, Spain, supra* note 143.

websites, since there is a "delete-button". AmCham EU stated that a right to be forgotten cannot, however, be extended further than to include deletion of personal data that the data subject has posted on the web. He or she should have a right to delete it, but *not* an ability to delete "all tracks of the original data," meaning erasing the future travels of this data, or another data subject's opinion *about* him or her. Such broad right to be forgotten interpretation and application would deprive the would-be speaker and would-be thinker the substance that enables their speech. Both the second and the third degrees of deletion will thereby have a chilling effect on freedom of expression and of information, and risk challenging the status quo in cyberspace. Just think about of all the "black holes" of missing information that we will find (or not find) in cyberspace.

When I argue for *not* extending the right to be forgotten to the second or third degree of deletion, I would like to stress that such an extended protection for one's digital persona should *not* go through the use of privacy laws. In letting a privacy claim be the channel to enable deletion, we risk creating an equals sign between privacy and censorship. This sign would imply that "privacy is the new black in censorship fashion"[296] as we are here discussing *voluntarily published* content that is *true, legally obtained* and *has entered the public domain.* Unless the content is illegal, such situations should be attacked through criminal laws, defamation laws, and copyright laws or similar.

Article 80 of the GDPR states that the Member States in the EU shall provide for exceptions or derogations from the right to be forgotten with regards to 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. Based on that broad exception, journalists should not fear a right to be forgotten. However, in a cyberspace where the bloggers have somewhat blurred the definition of journalism, this article needs further explanation - or I predict that most speech will be accepted and the right to be forgotten might end up being an edentulous political utopia. When I interviewed an EU official who has been involved in the development of the proposal to the GDPR, he stressed that "freedom of expression is not a good argument for not having a right to be forgotten." Yes, he might be correct, but with *too much* room for speech, it will be deprival of the right to privacy. Since it, according to Article 80(2) of the GDPR is up to each Member State to, within two years after the GDPR has entered into force, more specifically determine the details regarding what to include in the exception of freedom of expression, I fear that the possible exception from deletion may vary depending on where your keyboard is. The result might be that some comments may be subject to deletion in one country, but not in another, a conflict that seems to be contradictory to the general goal of harmonization. This makes a complicated issue already within the EU. When adding the U.S. and the global dimension to this, anybody can easily understand that the right to be forgotten and its collision with freedom of expression is an extremely complex problem.

[296] *Fleischer, Oblivion, supra* note 107.

To reach a reasonable level of how far a right to be forgotten should be extended before violating freedom of expression, I encourage the European Commission to take a closer look at the right to be forgotten recently enacted in California, and consider narrowing the proposed law in the EU. Although being criticized for not giving enough mandate to require deletion of personal data since it merely gives the data subject a right to delete his or her own posted content, I believe that it most likely is as extended as the European right to be forgotten *practically* can be made to avoid a collision with freedom of expression. My argument that there is a need to narrow the potential scope of application of a right to be forgotten as well as the responsibility requirement of such a right as provided for in the GDPR has recently been backed by other researchers.[297] Although no right to be forgotten case in the future will be the same as another, and even if it might be hard to make the GDPR more specific, I believe that it is vital to try, or the proposed law will merely be an empty and impractical political promise. Additionally, in order for the General Data Protection Regulation to be practically applicable, the EU Commission needs to specify whether to include both *expressional* and *informational* data in a right to be forgotten provision. Since a lot of the online content contains both, drawing a line here might potentially turn Facebook into a censor-in-chief – a responsibility I do not believe should reasonably be given to a social media website.

6.3.3 "Catch 22"

The enforcement of the EU right to be forgotten is not dependant on the existence of a similar right in the United States. Yet, I was curious to investigate whether such a right could even exist in the U.S.A, given the global nature of the Internet and the fact that EU users employ the services of U.S. online companies.

Section 230 of the CDA is a direct result of the First Amendment to the U.S. Constitution. This section protects freedom of expression by giving immunity for providers of an interactive computer service to delete any content posted by third parties. Although forcing companies to become gatekeepers of everything that happens on their networks will risk destroying the essence of the Internet and its value for free communication, I believe that courts in the U.S.A. are unfortunately interpreting CDA Section 230 too broadly and giving too much immunity. This ultimately eliminates the incentives to find a balance between free speech and privacy. I believe that a right to be forgotten that goes beyond the first degree of deletion cannot exist on a federal level in the U.S.A. as long as the CDA is not amended to better fit different approaches to privacy laws in cyberspace. The U.S. approach risks leading to a "blame yourself approach" to forgetting implying "if you want to be forgotten, simply do not get remembered in the first place,"[298] since it is hard to prevent the spread of

[297] *See* e.g. Adams Shoor, *supra* note 229.
[298] Kulevska, *supra* note 127.

public information as long as such information was legally acquired.[299] Although there might not be room for a plain EU style right to be forgotten to exist in the U.S.A. without "requiring a new federal statute,"[300] it does not reduce the responsibility for U.S. companies dealing with European users. The question that remains to be answered is how can we cope with these differences in a global cyberspace?

Although EU citizens have signed an agreement with Facebook Ireland Ltd, which forces Facebook to comply with EU privacy standards, users have also consented to having their personal data transferred and processed in the U.S.A. This is why the Safe Harbour "adequacy" requirement regarding data protection comes into play. Somewhat shaken in the recent PRISM surveillance scandal, one may now question how strict the "adequacy" requirement for processing of personal data actually is, and whether it can be used as a loophole for U.S. companies to target EU users. With the recent decision in *Google Spain v. AEPD,* as well as Article 17 of the GDPR, the Safe Harbor Agreement will most likely need to be strengthened. Viviane Reding has clearly threatened that it must be "strengthened or it will be suspended".[301] Since the Internet is *global* and data is being transferred everywhere, a *suspension* of the Agreement would lead to either no more Facebook use for the EU citizens, or to a restriction of the spread of data outside the borders of the EU - which would be contrary to what an open Internet is all about. I wonder, however, if it could go the other way – that an open Internet might be threatened *just because* the EU citizens will be given a right to delete - as such a right will violate the freedom of expression. We might have reached some kind of "Catch 22," where either way might lead to a fragmented, instead of a global and united, cyberspace. How can we enforce a right to be forgotten that will not violate the freedom of expression, but protect our digital persona?

6.4 The Enforcement of the Right to Be Forgotten

6.4.1 Responsibility for Deletion According to the GDPR

When the GDPR enters into force, Article 17(2) will require a data controller, which has made the personal data public, to take "all reasonable steps including technical measures […] to inform third parties which are processing such data, that a data subject requests them to erase any links to, copy or replication of that personal data." A possible scenario, that the European Commission has not considered yet, is if there can be a mechanism for take-down and put-back when a claim is *fraudulent*. For example, what would happen if someone orders content that is to be forgotten when that information in fact does not implicate the personally identifiable information of the individual making the request? How will the GDPR solve such an issue?

[299] *See, e.g. Florida Star v. B.J.F., supra* note 174.
[300] Interview with Christopher Gibson, *supra* note 264.
[301] *Press Release, European Commission, A Data Protection Compact, supra* note 84.

Facebook will most likely be forced to change its privacy policies if the right to be forgotten will be enacted in its present form, since it currently states that they will take no responsibility for content, which "has been shared with others".[302] According to Article 17(2), Facebook's responsibility to third party deletion is to take "reasonable steps" to *inform* the current content holder. Only if Facebook has *authorized* the third party use of such data, they are *responsible* for the actual deletion of the personal data. Lead Engineer David Larochelle at Harvard's Berkman Center as well as ENISA[303] experts have expressed concerns regarding the technical hurdles of the enforcement of a right to be forgotten since a major complicating factor is all the re-publications of data. As soon as someone has copied the data, taken a screen shot of it or saved it on a desktop, it will be extremely hard to find, which makes even the "reasonable steps" requirement as provided for in Article 17(2) a massive task. Therefore, I believe that the European Commission needs to provide the online community with further specifications of the "technical measures" that data controllers are required to take. The right to be forgotten, according to the proposed GDPR, seems to be asking the data controllers to squeeze the toothpaste back into the tube. This, in my opinion, is far beyond the blurry requirements of "reasonable steps."

6.4.2 Finding the Balance: Alternatives to the Right to Be Forgotten

The lack of an overall supervision of the Internet makes it an open communication tool that can be used by anyone. When trying to regulate the use of data on the Internet, there are many variables to consider. One of them, which is of great importance to this thesis, is the fact that technology develops at a rapid pace and regulations that will try to keep up with these ever-changing technological inventions without risking a legal lag, need to be as interchangeable as the Internet itself. Reg Whitaker wrote in his book "The End of Privacy": "Cyberspace exists nowhere and everywhere, it is forever a *tabula rasa* in the sense that it is constantly being constructed and reconstructed, written and rewritten, by the simultaneous interaction of all those networking in the medium".[304] Perhaps the right approach and balance with free speech interests could be reached if the right to be forgotten is not considered as a right per se, but merely as an interest or a policy goal. *Legislation* seems too stiff and has been criticised for having the style of an

[302] Facebook's Terms, *supra* note 112.
[303] ENISA stands for the European Union Agency for Network and Information Security. More information available at https://www.enisa.europa.eu/ ; Data Guidance, *EU: Right to be Forgotten Now the Right to Erasure*, Oct. 22, 2013, http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2119.
[304] REG WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY 19 (1999).

ultimatum given from the EU to the U.S.A.[305] For the Internet to work globally, we need *global* collaboration.

We have now come to a stage in the digital age where giving a fully extended right to be forgotten will violate freedom of expression, but where *not* giving the data subjects a right to be forgotten might lead to self-censoring and a non-use of their given free speech right because they would feel that the speech is *not* free. Therefore, the *alternative* ways to protect privacy that do not come with a full out attack on free speech, and which are *technically* enforceable, are vital. Is it possible to humanize the digital age and protect the digital persona deprived of a *legislated* right to be forgotten?

As an alternative to a Regulation, I believe that it is of great importance to let the industry leading stakeholders to be a part of the process of creating an international privacy framework as exemplified in the U.S. Consumer Privacy Bill of Rights. This way, international best practice agreements, which are easier to change than unilateral Regulations, will enable the current standard to always be up to date with the latest technological developments. Best practise agreements would most likely be a more efficient method to enable a change, rather than merely relying on changing social norms on the Internet. Because norms of social media usage are so deeply entrenched, and because Facebook continues to modify its privacy policies in favour of more public disclosure, protecting privacy through changing norms would be an uphill battle.

Expiration dates for data, as proposed by Mayer-Schönberger, could be a good way to enhance the data subjects' control over their personal data. It would be rather simple to implement since it is just added meta data to personal data. However, since the function of expiration dates would allow data subjects to erase all copies of that data, it would most likely correspond to the second degree of deletion and thereby interfere with freedom of expression. Consistent with Advocate General Jääskinen's opinion, it is of great importance to emphasize the fact that the access to information has revolutionized communication between individuals.[306]

Expiration dates could, however, be a good *technical tool* to make people start thinking about remembering and forgetting in the digital age. But practically, it can only be used on the data subject's *own* data. Because the *user* would determine the expiration date, this solution fails to provide a remedy for content posted by third parties, equivalent to the third degree of deletion in my categorization.[307] What will happen with data that has an expiration date added to it determining that it will expire in let us say three years? Perhaps Google's staff has, after the decision in *Google Spain v. AEPD,* already determined this

[305] Joel R. Reidenberg, *E-commerce and Trans-Atlantic Privacy,* 38 HOURS. L. REV. 717, 735 (2001).
[306] United Nations, Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Frank La Rue (Document A/HRC/17/27), May 16, 2011, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
[307] Adams Shoor, *supra* note 229.

information to be newsworthy and of great interest to the public since these xenophobic comments are made by the next political leader. Due to the use of expiration dates, this information will now be removed from the whole Internet. From a democratic cyberspace perspective, this self-censoring possibility is dangerous. Therefore there is a need to examine the *alternatives* to *the right to be forgotten*, alternatives that would not have a chilling effect on freedom of expression, while still protecting the reputation of the data subjects.

I believe that by giving *more* freedom of expression we can create enhanced privacy and protection of the digital persona. The ultimate concept that will balance privacy and freedom of expression is most likely to *add* more data through the use of *contextualization.* Think about it: What is the main reason to why you want the right to be forgotten? It is most likely the desire to not have your life presented to the world mechanistically through just a search for your name, a search that will enable the finding of information that you have not been able to review. It is a protection of your online reputation and a right to be the one *in control* of the information available about you online. At the same time you most likely do not want to give up your right to get information about other people. Therefore the Google News' feature enabling to add a comment or explanation about something written about you online would be a great way to *contextualize* and shape your own future of the past. No content beyond the first degree of deletion will be deleted, but this is a compromise people must be willing make to adapt our way of thinking around the new technology, and to find an acceptable balance between privacy and expression. Danah Boyd at the Berkman Center for Internet and Society at Harvard Law School proclaims that such approach to modern technology will go through *cognitive adjustment*. As we assume that people can change, and we know that most people have a lot of personal data revealed online, a good way to deal with this amount of information is to merely focus on the *latest*, and remember that human developing and forgiving lies in our own evaluation of the information. The U.S. Supreme Court has stated that "exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and of press."[308] We should not fight the propagation of memory, but instead adapt to it and this way come closer to the human way of forgetting. The human brain cannot just forget, it can also *adapt* to new realities and forget or ignore content - even if the content itself continues to exist in cyberspace. In light of cognitive adjustments, I strongly believe that the *right to be* ***forgiven*** may be the new approach to deletion that will best be balanced with online free expression. By adapting this way, the case of Stacy Snyder will consequently rarely exist in the future. We do not have to have a perfect digital persona to be forgiven. Another time another employer will be a part of Generation Connected and perhaps not add any importance to a picture like the one of Stacy Snyder, since he or she might have posted many similar pictures on the Internet. In line with Mayer-Schönberger, I agree that less an ability to delete personal information could lead to self-censoring. However, I also believe that what it all comes down to

[308] See, e.g., *Bartnicki v. Vopper*, *supra* note 176.

in the end is not whether we will be given a right to be forgotten or not, but the recipient's ability to forgive and forget, as we all, despite the flawless digital memory, are humans that make mistakes and develop.

Time heals all wounds, memory fades, forgive and forget. We have all heard it, and we certainly all know the meaning of it. Whether these expressions are still applicable, or merely relegated to the past is up to our *own* adaption of the new technology to determine. Like the American Psychiatrist Gerald Jampolosky once said: "Forgiveness means letting go of the past". In order to *humanizing the digital age* we have to, with or without a right to be forgotten*, remember to forget.*

Bibliography

Legislation

Bundesverfassungsgerich [BVerfG] German Federal Constitutional Court (June 3, 1980), 54 Etscheidungen des Bundesverfassungsgerichs [BVerfGE] 148 (155) (F.R.G.).

Charter of Fundamental Rights of the European Union, OJ 2007, C 303/1, http://www.europarl.europa.eu/charter/pdf/text en.pdf (last visited April, 25, 2014).

Consolidated version of the Treaty on the Functioning of the European Union, OJ 2008, C 115/49, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0047:0199:en:PDF (last visited April 25, 2014).

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 the Free Movement of Such Data, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (last visited April 25, 2014).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (last visited April, 25, 2014).

European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, http://conventions.coe.int/treaty/en/Treaties/Html/005.htm (last visited April, 25, 2014).

Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat (1996), http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf (last visited May 21, 2014).

Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. ("B.O.E." núm. 298, de 14 de diciembre de 1999). (Directive 95/46/EC is through this law implemented in Spanish law).

Privacy Act of 1974, 5 U.S.C. § 552a

Proposal for a Regulation of the European Parliament and of the Council of the Protection of Individuals With Regard to the Processing of Personal Data and

on the Free Movement of Such Data (General Data Protection Regulation), 2012/0011 (COD), Jan. 25, 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited April, 25, 2014).

Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data by the Community Institutions and Bodies and of the Free Movement of Such Data (EC) 45/2001 (Dec. 18, 2000), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF (last visited April 25, 2014).

Restatement (Second) of Torts § 558 (1977).

Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 2007 O.J. (C 306/01), http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:C:2007:306:TOC (last visited April 25, 2014).

United Nations, The Universal Declaration of Human Rights, (Dec. 10, 1948), http://www.ichrp.org/en/article_12_udhr (last visited April 25, 2014).

U.S. Senate, Senate Bill No. 568, http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568 (last visited May 22, 2014).

The Constitution of the United States, Amendment I (1971).

17 U.S. Code § 512 (k)(1)(A)-(B) - Limitation on Liability Relating to Material Online.

47 U.S. Code § 230 – Protection for Private Blocking and Screening of Offensive Material (Communications Decency Act).

Literature

Alverén, Fredrik, *Såld på nätet – Priset du betalar för gratis*, Ordfront, Stockholm, 2012.

Blume, Peter, *Protection of Informational Privacy*, Djøf Publishing, Copenhagen, 2002.

Craig, Brian, *Cyberlaw – the Law of the Internet and Information Technology*, Pearson, 2013.

Mayer-Schönberger, Viktor, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, Princeton, 2009.

Smith, Steven W., *The Scientists and Engineer's Guide to Digital Signal Processing*, California Technical Processing, 1997.

Solove, Daniel J, *The Digital Person: Technology and Privacy in the Information Age*, NYU Press, 2004.

Solove, Daniel J, *The Future of Reputation,* Yale University Press, 2007.

Westin, Alan F; Baker Michael A, *Databanks in a Free Society: Computers, Record Keeping, and Privacy*, Quadrangle/New York Times Book Company, New York, 1972.

Whitaker, Reg, *The End of Privacy: How Total Surveillance Is Becoming a Reality,* The New Press, New York, 1999.

Zittrain, Jonathan, *The Future of the Internet – and How to Stop it*, Yale University Press, 2008.

Legal Articles

Adams Shoor, Emily, *Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation*, 39 Brooklyn J. of Int'L, 1 (2014) 487-519.

Allen, A.L., *Dredging up the Past: Lifelogging, Memory, and Surveillance*, 75 U. Chi. L. Rev. 47 (2008).

Ambrose, Meg Leta; Ausloos, Jef, *The Right to be Forgotten Across the Pond*, Journal of Information Policy 3 (2013): 1-23.

American Law Reports, *Validity, Construction, and Application of Immunity Provisions of Communications Decency Act, 47 U.S.C.§ 230*, 52 A.L.R. Fed. 2d 37.

Balkin, Jack M, *Some Realism About Pluralism: Legal Realist Approaches to the First Amendment*, Duke L.J. 375, 383–85 (1990).

Blanchette, Jean-François; Johnsson, Deborah G, *Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness* 4, ACM Policy Conference (1998).

Brimsted, Kate, *The Right to be Forgotten: Can Legislation Put the Data Genie Back in the Bottle?,* Privacy & Data Protection 6-8, 7 (Vol. 11(4) 2011).

Conley, Chris, *The Right to Delete*, ACLU of Northern California.

Dowling Jr, Donald C; Mittman, Jeremy M, *Data Privacy Regulation Outside the United States: A Clash of Jurisprudential Perspectives*, in Proskauer on Privacy (2006).

Koops, Bert-Jaap, *Forgetting Footprints, Shunning Shadows: A Critical Analyze of 'The Right to be Forgotten' in Big Data Practice,* 8 Scripted 229, 236 (2012).

Kuner, Christopher, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection law,* Privacy & Security Law Report, 11 PVLR 06, June 2 (2012).

Larson, Robert G, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech, Communication Law and Policy*, Communication Law & Policy, Uni. Min., 18:1, 91-120 (2013).

McNealy, Jasmine E, *The Emerging Conflict Between Newsworthiness and The Right to be Forgotten,* 39 N. Ky. L. Rev. 119 (2012).

Millikin, Matthew R, *Note, www.misappropriation.com: Protecting Trade Secrets After Mass Dissemination on the Internet,* 78 Wash. U. L. Q. 931, 948 (2000).

Nuno Gomes de Andrade, Norberto, *Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization,* Computers, Privacy and Data Protection: An Element of Choice 66, 90, Serge Gutwirth et. al. eds., (2011).

Ramsay, Hayden, *Privacy Privacies and Basic Needs,* The Heythrop Journal 288-297 (2010).

Reidenberg, Joel R, *E-commerce and Trans-Atlantic Privacy,* 38 Hours. L. Rev. 717, 735 (2001).

Rosen, Jeffrey, *The Right to be Forgotten,* 64 Stan. L. Rev. Online 88 (2012).

Rubenstein, Ira; Lee, Ronald D; Schwarts, Paul M, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches,* 75 Chi. L. Rev. (2008).

Schwartz, Paul, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 Am. J. Comp. L. 675, 686–87 (1989).

Warren, Samuel; Brandeis, Louis, *The Right to Privacy*, 15 Harv. L. Rev. 193 (1890).

Werro, Franz, *The Right to Inform vs. the Right to be Forgotten: A Transatlantic Clash*, Georgetown University (2009).

Whitman, James Q, *Two Western Cultures of Privacy: Dignity Versus Liberty,* 113 Yale L. J. 1153, 1161 (2004).

Xanthoulis, Napoleon, *Right to Oblivion in the Information Age*: A Human-Rights Based Approach, 10 US-China L. Rev. 84 (2013).

Zaidi, Kamaal, *Harmonizing U.S.-EU Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data*, 12 Mich. St. U. J. Int'l L. 169 (2003).

Other Sources

Interviews

Interview with Christopher Gibson, Associate Dean and Professor of Law, Suffolk University Law School, in Boston, MA, U.S.A. (Nov. 26, 2012).

Interview/email correspondence with David Larochelle, Lead Engineer for Media Cloud, Berkman Center for Internet and Society at Harvard University Law School, Eslöv, Sweden - Cambridge, MA, U.S.A. (April 9, 2014).

Interview/e-mail correspondence with Ulf Maunsbach, Professor of Law, The Faculty of Law at Lund University, Boston, MA, U.S.A. – Lund, Sweden (Nov. 28, 2012).

Telephone interview with an EU official (who desired to be anonymous), who was involved in the development of the General Data Protection Regulation. Boston, MA, U.S.A. - Brussels, Belgium (Dec. 11, 2012).

Sources Available on the Internet: Articles, Blogs, Communications, Hearings, Memos, Press Releases, Principles, Reports, Speeches, Videos, and Websites

AmCham EU, more information available at http://www.amchameu.eu/AboutUs/tabid/61/Default.aspx (last visited May 22, 2014).

Article 29 Data Protection Working Party, *Working Party on the Protection of individuals With Regard to the Processing of Personal Data*, Feb. 15, 2010,

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/rules-art-29_en.pdf (last visited April, 25, 2014).

Ball, James, *'Right to Be Forgotten' Ruling Creates a Quagmire for Google et al,* May 13, 2014, The Guardian, http://www.theguardian.com/commentisfree/2014/may/13/right-to-be-forgotten-ruling-quagmire-google (last visited May 22, 2014).

BBC News, *Do you Have a Right to Be Forgotten Online?,* Feb. 10, 2012, http://news.bbc.co.uk/2/hi/programmes/click_online/9695021.stm (last visited Dec. 1, 2012).

Cease and desist letter on behalf of Mr. Wolfgang Werle to the Wikimedia Foundation, Inc., Oct. 27, 2009, http://www.wired.com/images_blogs/threatlevel/2009/11/stopp.pdf (last visited May 22, 2014).

Chilling Effects Clearinghouse, Berkman Center for Internet and Society, *DMCA Safe Harbor,* https://www.chillingeffects.org/dmca512/faq.cgi (last visited April 20, 2014).

Connolly, Kate, *Right to Erasure Protects People's Freedom to Forget the Past, Says Expert,* The Guardian, April 4, 2013, http://www.theguardian.com/technology/2013/apr/04/right-erasure-protects-freedom-forget-past (last visited May 24, 2014).

Council of Foreign Relations NY, *Privacy Pragmatism: Focus on Data Use, Not Data Collection*, March 1, 2014, http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism (last visited April, 25, 2014).

Data Guidance, *EU: Right to be Forgotten Now the Right to Erasure*, Oct. 22, 2013, http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2119 (last visited April 23, 2014).

Electronic Frontier Foundation, *CDA 230 The most important law protecting Internet speech*, https://www.eff.org/issues/cda230/infographic (last visited Feb. 2, 2014).

European Commission, *Commission Proposes a Comprehensive Reform of the Data Protection Rules*, Jan. 25, 2012, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm (last visited April, 25, 2014).

European Commission, 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 – European Data Protection Framework for the 21st Century,* (COM(2012) 9

final, Jan. 25, 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf (last visited April, 25, 2014).

European Commission, *Data Protection Day 2014: Full Speed on EU Data Protection Reform*, Memorandum, Jan. 27, 2014, http://europa.eu/rapid/press-release_MEMO-14-60_en.htm (last visited April, 25, 2014).

European Commission, *Data Protection – Progress on EU Reform Now Irreversible After European Parliament Vote,* March 12, 2014, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_dp_plenary_vote_140312_en.pdf (last visited April 25, 2014).

European Commission, *How Will the Data Protection Reform Affect Social Networks?,* June, 2011, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf (last visited April, 25, 2014).

European Commission, *LIBE Committee Vote Backs New EU Data Protection Laws*, MEMO/13/923, Oct. 22, 2013, http://europa.eu/rapid/press-release_MEMO-13-923_en.htm (last visited April 25, 2014).

European Commission, *The Co-Decision or Ordinary Legislative Procedure*, archived June 24, 2007, http://ec.europa.eu/codecision/procedure/index_en.htm (last visited April 25, 2014).

Europe v. Facebook, available at http://europe-v-facebook.org/EN/en.html (last visited May 24, 2014).

Europe v. Facebook, *Complaint against Facebook Ireland Ltd – 07 Messages,* Aug. 18, 2011, http://europe-v-facebook.org/Complaint_07_Messages.pdf (last visited March 3, 2014).

Europe v. Facebook, *Legal Actions Against European Subsidiaries of Facebook, Apple, Microsoft, Skype and Yahoo Filed*, June 26, 2013, http://europe-v-facebook.org/EN/en.html (last visited March 3, 2014).

Europe v. Facebook, *Legal Procedure against "Facebook Ireland Ltd",* http://europe-v-facebook.org/EN/Complaints/complaints.html (last visited March 3, 2014).

European Union, *Regulations, Directives and Other Acts, http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm* (last visited April 2, 2014).

Facebook on the U.S.-EU Safe Harbor List, http://safeharbor.export.gov/companyinfo.aspx?id=18810 (last visited May 2, 2014).

Facebook's Statement of Rights and Responsibilities, https://www.facebook.com/legal/terms (last visited April 25, 2014).

Facebook Statistics, Statistic Brain, http://www.statisticbrain.com/facebook-statistics/ (last visited May 10, 2014).

Fleischer, Peter, *Foggy thinking about the Right to Oblivion*, March 9, 2011, http://peterfleischer.blogspot.se/2011/03/foggy-thinking-about-right-to-oblivion.html (last visited May 15, 2014).

Fleischer, Peter, *The Right to be Forgotten – Seen from Spain*, Sept. 5, 2011, http://peterfleischer.blogspot.se/2011/09/right-to-be-forgotten-seen-from-spain.html (last visited May 15, 2014).

Foer, Joshua, *Remember This*, The National Geographic Magazine, Nov. 2007, http://ngm.nationalgeographic.com/print/2007/11/memory/foer-text (last visited April 25, 2014).

Gaskell, Helen, *Google Must Respect 'Right to Be Forgotten' Rules EU Court,* Arabian Industry, May 14, 2014, http://arabianindustry.com/technology/news/2014/may/14/google-must-respect-right-to-be-forgotten-rules-eu-court-4699734/#.U33S9liSzKM (last visited May 23, 2014).

Goldmann, Mattias; Jacob Dexe, *Låt inte de digitala fotspåren suddas ut,* May 17, 2014, http://www.svd.se/opinion/brannpunkt/lat-inte-de-digitala-fotsparen-fa-suddas-ut_3568578.svd (last visited May 20, 2014).

Google on the U.S.-EU Safe Harbor List, http://safeharbor.export.gov/companyinfo.aspx?id=19795 (last visited May 2, 2014).

Google, Removing Content from Google, https://support.google.com/legal/troubleshooter/1114905?hl=en (last visited May 14, 2014).

Granick, Jennifer, *Convicted Murdered To Wikipedia: Shhh!,* Electronic Frontier Foundation, Nov. 10, 2009, https://www.eff.org/deeplinks/2009/11/murderer-wikipedia-shhh (last visited May 22, 2014).

Graux, Hans; Ausloos, Jef; Valcke, Peggy, *The Right to be Forgotten in the Internet Era,* Nov. 12, 2012, https://www.law.kuleuven.se/icri/ (last visited Nov. 29, 2013).

Hawktalk, *Data Protection: Forget About a "Right to Forget",* Amberhawk, March 28, 2011, http://amberhawk.typepad.com/amberhawk/2011/03/data-protection-forget-about-a-right-to-forget.html (last visited May 20, 2014).

Hendel, John, *In Europe, a Right to be Forgotten Trumps the Memory of the Internet,* The Atlantic, Feb. 3, 2011, http://www.theatlantic.com/technology/archive/2011/02/in-europe-a-right-to-be-forgotten-trumps-the-memory-of-the-internet/70643/ (last visited March 3, 2014).

House of Representatives, *Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?,* Hearing Before the Subcommittee on Commerce, Manufacturing, and Trade of the Committee of Energy and Commerce, March 29, 2012, Serial No. 112-135, http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg81441/pdf/CHRG-112hhrg81441.pdf (last visited May 2, 2014).

Internet Archive, more information available at www.archive.org (last visited May 24, 2014).

Johnson, Bobbie, *Privacy No Longer a Social Norm, Says Facebook Founder,* The Guardian, Jan. 10, 2010, http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy (last visited May 24, 2014).

Kanter, James, *Rules Shielding Online Data From N.S.A. and Other Prying Eyes Advance in Europe,* The New York Times, Oct. 21, 2013, http://www.nytimes.com/2013/10/22/business/international/eu-panel-backs-plan-to-shield-online-data.html?_r=0 (last visited May 22, 2013).

Kirkpatrick, Marshall, *Facebook's Zuckerberg Says the Age of Privacy is Over,* ReadWriteWeb, Jan. 9, 2010, http://www.readwriteweb.com/archives/facebookszuck erbergsaystheage-of-privacy-is~ov.php (last visited March 3, 2014).

Kulevska, Sanna, *The Future of Your Past: A Right to be Forgotten Online?,* Berkman Center for Internet and Society at Harvard Law School, http://www.chillingeffects.org/weather.cgi?WeatherID=769 (last visited May 23, 2014).

Lichter, Susanna, *Unwanted Exposure: Civil and Criminal Liability for Revenge Porn Hosts and Posters,* Harvard Journal of Law and Technology, May 28, 2013, http://jolt.law.harvard.edu/digest/privacy/unwanted-exposure-civil-and-criminal-liability-for-revenge-porn-hosts-and-posters (last visited May 2, 2014).

Madrigal, Alexis, *Reading the Privacy Policies You Encountering a Year Would Take 76 Work Days,* The Atlantic**,** March 1, 2012, http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ (last visited May 22, 2014).

Markey, Ed, EU-U.S. Conference on Privacy, Speech, March 19, 2012, https://www.youtube.com/watch?v=mdD07BVBZbo (last visited May 22, 2014).

McClure, Julia, *The Right to Be Forgotten in a Digital Age,* National Security Law Brief, Washington College of Law, Nov. 14, 2013, http://www.nationalsecuritylawbrief.com/the-right-to-be-forgotten-in-a-digital-age/ (last visited April 25, 2014).

Meredith, Dan; Golding, Andy, *Perspective About the News From People in the News*, Google News Blog, Aug. 7, 2007, http://googlenewsblog.blogspot.se/2007/08/perspectives-about-news-from-people-in.html (last visited March 2, 2014).

Nielsen, Harris Interactive, more information available at http://www.harrisinteractive.com/ (last visited May 24, 2014).

NOLO, Criminal Defense Lawyer, *Expunging of Sealing a Juvenile Court Record*, http://www.criminaldefenselawyer.com/topics/expunging-or-sealing-a-juvenile-court-record (last visited May 24, 2014).

OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 2013, http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (last visited April 25, 2014).

OECD, *Privacy Principles*, 2013, http://www.oecd.org/sti/ieconomy/privacy.htm (last visited March 20, 2014).

Pfanner, Eric, *Archivists in France Fight a Privacy Initiative,* New York Times, June 16, 2013, http://www.nytimes.com/2013/06/17/technology/archivists-in-france-push-against-privacy-movement.html?pagewanted=2&_r=1&ref=global-home& (last visited May 20, 2014).

Press Release, European Commission, *A Data Protection Compact for Europe,* Speech/14/62, January 28, 2014, available at http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm (last visited April, 25, 2014).

Press Release, European Commission, *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses*, http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en (last visited April, 25, 2014).

Press Release, European Commission, *Commission Proposes a Comprehensive Reform of EU Data Protection Rules*, Jan 25, 2012, http://ec.europa.eu/avservices/video/player.cfm?ref=82655 (last visited April, 25, 2014).

Press Release, European Commission, *Data Protection: Europeans Share Data Online, But Privacy Concerns Remain – New Survey*, June 16, 2011, http://europa.eu/rapid/press-release_IP-11-742_en.htm (last visited April, 25, 2014).

Press Release, European Commission, *EU Data Protection Reform and Social Media: Encouraging Citizens' Trust and Creating New Opportunities,* SPEECH 11/827, Nov. 29, 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/827&type=HTML (last visited April 25, 2014).

Press Release, European Data Protection Supervisor, *Urgent Reform of EU Data Protection Framework is Essential for a Connected Continent*, EDPS/2014/02, Jan. 16, 2014, http://europa.eu/rapid/press-release_EDPS-14-2_en.htm (last visited April 25, 2014).

RationalWiki, *Streisand Effect*, http://rationalwiki.org/wiki/Streisand_effect (last visited May 14, 2014).

Reputation, more information available at http://www.reputation.com/reputationdefender (last visited May 24, 2014).

Salmon, Felix, *The Spread of Link Rot,* Reuters, June 28, 2013, http://blogs.reuters.com/felix-salmon/2013/06/28/the-spread-of-link-rot/ (last visited May 2, 2014).

Schrems, Maximilian, *Complaint against Facebook Ireland Ltd – 23 "PRISM"*, June 25, 2013, http://www.europe-v-facebook.org/prism/facebook.pdf (last visited May 22, 2014).

Schwartz, John, *Two German Killers Demanding Anonymity Sue Wikipedia's Parent*, The New York Times, Nov. 12, 2009, http://www.nytimes.com/2009/11/13/us/13wiki.html?_r=0 (last visited May 20, 2014).

Siegler, M G, *Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up To 2003*, Techcrunch, Aug. 4, 2010, http://techcrunch.com/2010/08/04/schmidt-data/ (last visited April, 25, 2014).
Snapchat, Terms of Use, last updated Dec. 20, 2013: http://www.snapchat.com/terms/ (last visited April 25, 2014).

Stelter, Brian, *Facebook's Users Ask Who Owns Information,* The New York Times, Feb. 17, 2009, http://www.nytimes.com/2009/02/17/technology/internet/17facebook.html?_r=0 (last visited May 24, 2014).

Stibel, Jeff, *Die, Links, Die! How Link 'Suicide' Can Save the Web,* Wired, WIRED, July 31, 2013, http://www.wired.com/2013/07/die-links-die-stop-worrying-about-link-rot/all/1 (last visited May 22, 2014).

The Chilling Effects Clearinghouse, Berkman Center for Internet and Society, http://www.chillingeffects.org/dmca512/faq.cgi (last visited May 10, 2014).

The Chilling Effects Clearinghouse, Frequently Asked Questions (and Answers) About DMCA Safe Harbor, Berkman Center for Internet and Society, http://www.chillingeffects.org/dmca512/faq.cgi (last visited May 10, 2014).

The Internet Data Corporation, IDC, https://www.idc.com/ (last visited April 13, 2014).

Twitter Engineering, *200 Million Tweets Per Day*, Twitter Blog, June 30, 2011, http://blog.twitter.com/2011/06/200-million-tweets-per-day.html (last visited April 25, 2014).

Twitter on the U.S.-EU Safe Harbor List, http://safeharbor.export.gov/companyinfo.aspx?id=18888 (last visited May 2, 2014).

Tömböl, Mona; Schennach, Philippe, *EU vs. Facebook: Fighting for the Right to be Forgotten*, The Vienna Review, Feb 5. 2013, http://www.viennareview.net/news/special-report/eu-vs-facebook-fighting-for-the-right-to-be-forgotten (last visited May 24, 2014).

United Nations, Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Frank La Rue (Document A/HRC/17/27), May 16, 2011, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (last visited May 2, 2014).

U.S.-EU Safe Harbor Agreement, 2000, http://export.gov/safeharbor/index.asp (last visited May 16, 2014).

Viviane Reding' Facebook page, https://www.facebook.com/permalink.php?story_fbid=304206613078842&id=291423897690447 (last visited May 20, 2014).

Warman, Matt, *Vint Cerf Attacks European Internet Policy,* The Telegraph, March 29, 2012, http://www.telegraph.co.uk/technology/news/9173449/Vint-Cerf-attacks-European-internet-policy.html (last visited May 3, 2014).

Winter, Jessica, *The Advantages of Amnesia*, The Boston Globe, Sept. 23, 2007, http://www.boston.com/news/globe/ideas/articles/2007/09/23/the_advantages_of_amnesia/?page=full (last visited April 25, 2014).

Zickuhr, Kathryn, *Teen Content Creators*, Pew Research Internet Project, Nov. 18, 2009, http://www.pewinternet.org/2009/11/18/teen-content-creators/ (last visited April 25, 2014).

Zittrain, Jonathan, *Don't Force Google to 'Forget'*, The new York Times, May 14 2014, http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0 (last visited May 20, 2014).

Table Of Cases

U.S. Courts

Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009).

Barrett v. Rosenthal, 40 Cal. 4th 33 (2006).

Bartnicki v. Vopper, 532 U.S. 514, 534 (2000).

Cox Broadcasting Co. v. Cohn 420 U.S. 469 (1975).

Fox Television Stations, Inc. v. F.C.C., 613 F.3d 317, 327 (2nd Cir. 2010).

Klayman v. Zuckerberg, 2012 WL 6725588, D.D.C. (2012).

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

Whitne Information Network, Inc. v. Xcentric Venture, LLC, 199 Fed. Appx. 738 (11th Cir. 2006).

Zeran v. AOL, 129 F.3d 327 (4th Cir. 1997).

EU Courts

BGH 1 StR 83/94 – Judgement of 21 July 1994 (LG München I) – "The Wikipedia Case" in German Court. (The appeal is available at http://www.hrrstrafrecht.de/hrr/1/94/1-83-94.php).

Case C-131/12, *Google Spain v. AEPD* [2014] n.y.r.

Case C-101/01, *Lindqvist* [2003] ECR 596.

Case C-342/09, *L´Oréal and Others* [2011] ECR 474.

Court of Justice of the European Union, Judgment of Nov. 9, 2010, Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Hartmut Eifert v. Land Hessen* [2010] ECR I-9831.

Joined cases C-465/00, C-138/01 and C-139/01: *Rechnungshof v. Österreichischer Rundfunk and Others* and *Christa Neukomm* and *Joseph Lauermann v. Österreichischer Rundfunk* [2003] I-4989.