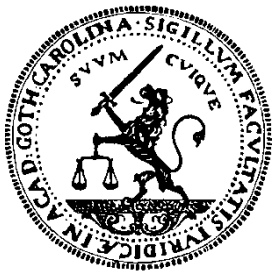
View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Lund University Publications - Student Papers



FACULTY OF LAW
Lund University

Linda Leffler Olsson

The Safe Harbor 2.0

An EU - U.S. Study of the Fundamental Right to Privacy with regard to Transatlantic Transfers of Personal Data

LAGM01 Graduate Thesis
Graduate Thesis, Master of Laws program
30 higher education credits

Supervisor: Henrik Norinder

Semester of graduation: Fall semester 2015

Contents

SUMMARY 1

SAMMANFATTNING 2

PREFACE 3

ABBREVIATIONS 4

1 INTRODUCTION 6
1.1 Background 6
1.2 Purpose and Presentation of Questions 9
1.3 Definitions 9
1.4 Method and Material 9
1.5 Delimitations 11
1.6 Research Position 12
1.7 Outline 13

2 BIG DATA IN THE DIGITAL WORLD 14
2.1 Everything Leaves a Digital Trace 14
2.2 Data Use as a Business Model 14
2.3 Data Use Policies 15
2.3.1 Google 16
2.3.2 Facebook 17
2.4 Summary 18

3 THE EU PRIVACY PROTECTION 20
3.1 The Fundamental Right to Privacy and Personal Data 20
3.2 The OECD Principles 21
3.3 The Data Protection Directive 22
3.4 Google Spain v. AEPD 23
3.5 The General Data Protection Regulation 25
3.5.1 The Right to Erasure 27
3.5.2 Exceptions to the Right to Erasure 29

4 THE U.S.' VIGILANCE TO THE RIGHT TO BE FORGOTTEN 31
4.1 Sectorial Privacy v. Comprehensive Privacy 31
4.2 Freedom of Speech 33
4.3 Privacy Based Cybertorts Supplementing Data Protection Laws 33

4.4 Section 230 of the CDA 34
4.5 No Tradition of the Right to be Forgotten 35
4.5.1 Juvenile Offenses 35
4.5.2 Personal Data of Minors 36
4.6 Privacy Act of 1974 36
4.7 The Patriot Act 36
4.8 The Cybersecurity Information Sharing Act of 2015 37

5 SOLUTIONS FOR CLASHING PRIVACY REGIMES 39
5.1 Transatlantic Transfers of Personal Data 39
5.2 Lawful Instruments for Data Transfers 40
5.3 History of the Safe Harbor 41
5.4 The Content of the Safe Harbor 42
5.4.1 The Safe Harbor Principles 42
5.4.2 Enforcement by Self-Regulation 43
5.4.3 Enforcement by Governmental Bodies 44
5.5 Efforts to Make the Safe Harbor Safer 45
5.6 The End of the Safe Harbor 46
5.7 The *Schrems* Impacts 49

6 ANALYSIS 52
6.1 Impacts of the *Schrems* Ruling 52
6.2 The Transatlantic Discrepancy: Can the U.S Ensure an "Essentially Equivalent" Level of Protection? 53
6.2.1 The U.S. Sectorial Privacy Legislation 54
6.2.2 The Fight Against Terrorism 55
6.2.3 No Respect for the EU Fundamental Rights and Freedoms 56
6.3 The Safe Harbor 2.0 57
6.3.1 Actionable Privacy Rights 57
6.3.2 Self-Regulation and Workable Enforcement 58
6.4 Conclusion 60

BIBLIOGRAPHY 61

TABLE OF CASES 68

Summary

The emergence of Big Data presents the EU legislator with new challenges of how to protect EU citizens' fundamental right to privacy as the Internet allows for massive amounts of personal data to easily cross borders. To meet the new challenges created by the borderless Internet, new privacy legislation is on its way in order to provide EU citizens with an adequate and sufficient protection for their fundamental right to privacy. The EU privacy protection provides its citizens with a broad protection for their fundamental right to privacy and personal data. This is considered as a general principle in EU law. In contrast, the U.S. does not have any comprehensive unanimous data protection laws. Rather it has chosen a sectorial approach, which renders data protection decentralized, fragmented, industry-specific, and largely uncoordinated among varying levels of government. This discrepancy between the EU and the U.S. presents challenges for a uniform international privacy standard that can facilitate for transatlantic transfers of personal data.

In the *Schrems* ruling, the Court of Justice of the European Union held that an adequacy decision under article 41 requires an investigation of the privacy protection offered by a third country. In addition, the Court concluded that the protection in the third country must offer a privacy protection that is "essentially equivalent" to the EU privacy protection. In the case, the Court invalidated the EU-U.S. Safe Harbor Program and concluded that the U.S. legal order did not amount to a privacy protection that is "essentially equivalent". The *Schrems* ruling has left EU and U.S. companies that transfer EU citizens' personal data to the U.S. with few lawful instruments for such transfers. Moreover, the discrepancy between the two privacy regimes will make it difficult to negotiate a Safe Harbor 2.0, especially because the U.S. does not recognize the right to erasure, which is a key provision in the EU privacy protection.

The emergence of Big Data, the discrepancy between the EU and the U.S. privacy protection, the *Schrems* ruling, and the proposed GDPR have resulted in challenges for both legislators and companies with regard to transatlantic transfers of personal data. I contend in this thesis that the U.S. legal order does not amount to a protection that is "essentially equivalent" to the EU privacy protection. However, the discprepancy cannot result in a suspension of transatlantic transfers of personal data. Therefore, a reasonable compromise would be that EU citizens are provided with actionable privacy rights and a workable enforcement in a Safe Harbor 2.0. Consequently, regardless whether or not the data cross borders, EU citizens' fundamental right to privacy is an offline right that also need to apply online.

Sammanfattning

Framväxten av ”Big Data” har ställt EU:s lagstiftare inför nya utmaningar avseende skyddet för EU-medborgarnas grundläggande rätt till privatliv och personuppgifter. Detta då internet har medfört att enorma mängder av personuppgifter numera utan svårigheter kan överföras över landsgränser. Mot bakgrund av de utmaningar som följer av det gränslösa internet är ny EU-lagstiftning är på väg. Denna syftar till att ge EU-medborgare ett fullgott och adekvat skydd för deras grundläggande rätt till privatliv och personuppgifter. Vidare ger EU-rätten ett brett skydd för EU-medborgares rätt till privatliv och personuppgifter. En rätt som även anses utgöra en allmän princip i EU-rätten. I motsats till EU:s syn på rätten till privatlivet har USA ingen övergripande, enhetlig dataskyddslagstiftning. Istället har USA valt ett sektoriellt förhållningssätt. Detta resulterar i att det amerikanska dataskyddet är decentraliserat, fragmenterat, industri-specifikt och i det stora hela okoordinerat för olika myndighetsnivåer. Diskrepansen mellan EU och USA visar tydligt på de utmaningar som finns i utformandet av en internationell enhetlig standard för skyddet till privatliv.

I Schrems-domen fastslog Europeiska unionens domstol att bedömningen av en adekvat skyddsnivå i enlighet med artikel 41 kräver en undersökning av det integritetsskydd som erbjuds i det tredje landet. Därutöver konstaterade domstolen att skyddet i tredje land måste erbjuda ett integritetsskydd som "i huvudsak motsvarar" EU:s integritetsskydd. I fallet, ogiltigförklarade domstolen EU-U.S. Safe Harbor-programmet och ansåg att den amerikanska rättsordningen inte uppnådde denna nivå. Schrems-domen har medfört att europeiska och amerikanska företag som överför EU-medborgarnas personuppgifter till USA har få lagliga medel för sådana överföringar. Skillnaderna mellan de två rättssystemen gör det svårt att förhandla fram en Safe Harbor 2.0. Detta särskilt då USA inte erkänner rätten att bli glömd, vilken är en viktig bestämmelse i EU:s integritetsskydd.

Framväxten av ”Big Data”, skillnaderna mellan EU:s och USA:s skydd för privatliv och personuppgifter, Schrems-domen och den föreslagna GDPR har resulterat i utmaningar för både lagstiftare och företag när det gäller transatlantiska överföringar av personuppgifter. I uppsatsen hävdas att den amerikanska rättsordningen inte uppnår en skyddsnivå som "i huvudsak motsvarar" EU:s grundläggande skydd för privatliv och personuppgifter. Det är dock inte rimligt att diskrepansen ska leda till ett upphörande av transatlantiska överföringar av personuppgifter. Därför är en rimlig kompromiss att EU-medborgare förses med effektiva och angripbara rättigheter. Därutöver ska en fungerande tillsyn av rättigheterna garanteras i en Safe Harbor 2.0. Därför, oavsett om personuppgifter korsar landsgränser, är EU-medborgarnas grundläggande rätt till privatliv en rättighet offline som även måste gälla online.

Preface

My exchange year at Suffolk University Law School in Boston was a highlight in my education. Not only did I get to develop my academic English, but I was also introduced to IT law. The constantly changing Internet creates new challenges for legislators, which tend to not keep up with techonology and there seems to be a constant legal lag where the Internet is concerned. One particular issue is the borderless character of the Internet and the national character of legislation. This discrepancy between different legal orders results inconsistencies in the legal application affecting both companies and the legal protection offered to Internet users around the world. Because Internet has become such a big part of our everyday life, I hope this thesis can make my readers more aware of some of the legal issues surrounding personal data.

I want to thank my supervisor Henrik Norinder for his support in writing this thesis. His availability and service has been of great help in getting through this final part of law school. I am especially thankful that he put me in contact with Karl-Hugo Engdahl, who is the next person I want to thank. Because the legal lag especially affects companies, an important aspect of this thesis has been the impacts of the *Schrems* ruling for EU and U.S. companies transferring personal data to the U.S. Karl-Hugo's experience as legal counsel at Klarna AB has contributed to a better understanding of the practical issues surrounding this subject, which has benefitted the outcome of this thesis. I am very grateful for the time he has been willing to set aside to discuss this subject. I also want to thank professor Michael Rustad at Suffolk University Law School, who inspired me to learn more about this subject. He has been a great inspiration in this particular subject and has helped me gain a better comparative perspective of the U.S. and the EU devlopments in IT law. Special thanks to Linda Nyström who volunteered to proofread my thesis, even though she has not studied law. That really is true friendship.

Lastly, I want to thank the persons who have made this fall, while writing my thesis, more fun. Anders – because you are always there with your love and support (and print copies of my thesis for me), and Lejla and Ulrica – because you are awesome. Five years of law school are done and now I am going to celebrate this with Bosnian Christmas.

Gislaved, January 2016
Linda Leffler Olsson

Abbreviations

AEPD	Agencia Española de Protección de Datos
the Charter	the Charter of the Fundamental Rights of the European Union
CISA	the Cybersecurity and Information Sharing Act of 2015
CJEU	the Court of Justice of the European Union
the Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
DPA	Data Protection Authority
ECHR	the European Convention for the Protection of Human Rights and Fundamental Freedoms
FTC	Federal Trade Commission
GDPR	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)
Google Spain v. AEPD	Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González
NSA	the National Security Agency
OECD	the Organization for Economic Co-operation and Development
Section 230 of the CDA	Section 230 of the Communications Decency Act
SNS	Social Networking Site

the Principles	the Safe Harbor Privacy Principles and Frequently Asked Questions
the Safe Harbor	U.S.-EU Safe Harbor Program
WP29	Article 29 Data Protection Working Party
U.S.	United States
U.S.C.	United States Code

1 Introduction

1.1 Background

So, why are the angry birds really angry? Vice-President of the European Commission, Vivane Reding, says it is because applications (and Social Networking Sites "SNS") provide their services on a "take-it-or-leave-it" basis. [1] Due to the take-it-or-leave-it rule, the birds are angry because that is when trust evaporates and people feel forced to part with their privacy.[2] An issue with the take-it-or-leave-it method is that users may not understand the extent of their given consent or, users do understand and disagree but do not possess the power to act. Snapchat, Instagram, and Facebook have grown to become popular SNS that all provide their services on a take-it-or-leave-it basis.[3] Although use is optional, the number of users of SNS is increasing, which indicates that use, in fact, may not be optional.

Another reason for them being angry could also be that SNS are obscure and deceitful regarding how they use personal data. For example, in 2014, the Federal Trade Commission ("FTC") alleged that Snapchat was deceiving consumers by a misrepresentation of its data collection practices.[4] The FTC complaint alleged a misrepresentation of Snapchat's practices with regard to the privacy, security, and confidentiality of users' information.[5] Even though Snapchat represented that it would not ask for, track, or access any location-specific information, it had integrated an analytics tracking service by which it collected users' location information.[6] Pursuant to the FTC complaint, the FTC and Snapchat settled the charges in a settlement agreement under which Snapchat is prohibited from misrepresenting the extent to which it maintains the privacy, security, or confidentiality of users'

[1] Viviane Reding, *A Data Protection Compact for Europe*, 28 January 2014,
[2] *Id*.
[3] See Facebook, Statement of Rights and Responsibilities, 25 November 2015, "By using or accessing the Facebook Services, you agree to this Statement", https://www.facebook.com/legal/terms; Instagram, Terms of Use, 19 January 2013, "If you do not agree to be bound by all of these Terms of Use, do not access or use the Service", https://instagram.com/about/legal/terms/; Snapchat, Terms of Service, 28 October 2015, "By using the Services, you agree to the Terms. Of course, if you don't agree with them, then don't use the Services."
[4] Federal Trade Commission, *In the Matter of Snapchat, Inc., a corporation*, docket no. 132 3078, https://www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf [hereinafter: *In the Matter of Snapchat, Inc., a corporation*], at paras 6-8.
[5] *In the Matter of Snapchat, Inc., a corporation*, at paras 20-24.
[6] *In the Matter of Snapchat, Inc., a corporation*, at paras 20-22.

information.[7] However, it is not only companies that use personal data, but personal data has also proven valuable in the fight against terrorism. The U.S. government was strongly criticized after the Snowden revelations, which disclosed that the National Security Agency ("NSA"), *inter alia*, had accessed personal data on a generalized basis under the USA PATRIOT Act[8] – a method, which was criticized for violating individuals' privacy rights.[9] The lack of knowledge among users, with regard to privacy and data collection practices, requires rigid privacy legislation that set the framework for how SNS and government authorities can use personal data. This way, trust can be restored among users allowing for offline rights to also apply online.

It is the European Commission's ("Commission") task to restore trust in the way that companies and governments process personal data.[10] However, the borderless digital world presents challenges for the enforcement of privacy rights as different nations provide their citizens' with different privacy protection. These challenges become especially prominent with regard to transatlantic transfers of EU citizens' personal data, due to the discrepancy between the EU and the U.S. privacy protection. Whereas the EU believes that individuals have a fundamental right to privacy and personal data, which has resulted in a strong protection for EU citizens, the U.S. has a fragmented and sectorial privacy protection leaving its citizens with a weak protection for their privacy.[11] In addition, the proposed General Data Protection Regulation ("GDPR") strengthens EU citizens' fundamental right to privacy as it contains an express provision of the right to erasure[12] ("the right to be forgotten"), which may drive the EU and the U.S. even further apart. To bridge the differences, the EU-U.S. Safe Harbor program ("the Safe Harbor") was negotiated to facilitate for transatlantic transfers of personal data. The objective was to provide a solution that would ensure an adequate level of protection set out in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free

[7] See Federal Trade Commission, *In the Matter of Snapchat, Inc., a corporation – Agreement Containing Consent Order*, file no. 132 3078, https://www.ftc.gov/system/files/documents/cases/140508snapchatorder.pdf.
[8] See Ewen Macaskill, Gabriel Dance, *NSA Files: Decoded – what the revelations mean for you*, The Guardian, 1 November 2013, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1; and Section 4.6.
[9] *Id*.
[10] Viviane Reding, *A Data Protection Compact for Europe*, 28 January 2014.
[11] See Section 3 and Section 4.
[12] The right to erasure of the GDPR is the equivalent to "the right to be forgotten" first recognized in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*. The two phrases will be used synonymously throughout the thesis.

movement of such data ("the Directive").[13] However, the Court of Justice of the European Union ("the CJEU") invalidated the Safe Harbor in the *Schrems* ruling.[14] Here, the Court held that a third country to which personal data is transferred, must ensure an adequate level of protection that is "essentially equivalent" to the EU privacy protection.[15] Given that the Safe Harbor did not contain any findings regarding the existence of U.S. rules that would guarantee the fundamental rights of EU citizens, the existing Safe Harbor could not ensure an effective legal protection for EU citizens' right to privacy and personal data.[16]

Pursuant to the *Schrems* ruling, the Article 29 Data Protection Working Party[17] ("WP29") has granted a grace period until the end of January 2016 that allows for companies to find alternative methods for transfers of personal data.[18] The legal situation is at this point uncertain and EU and U.S. companies that have relied on the Safe Harbor for transfers of personal data are now left with few lawful, attractive instruments for such transfers after the *Schrems* ruling. The EU and the U.S. are currently trying to negotiate a Safe Harbor 2.0 under which transfers to the U.S. can be done lawfully. Given the CJEU's demand for an adequate level of protection that is "essentially equivalent" to the EU protection, one issue is whether the U.S. at all can satisfy the EU's "strict" privacy protection. In addition, it is unclear how the discrepancy between the two privacy regimes will affect a Safe Harbor 2.0 in light of the requirements in the *Schrems* ruling and the right to erasure of the GDPR.

---

[13] See Sections 5.3-5.5.
[14] Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner* (6 October 2015) [hereinafter: Schrems v. DPC].
[15] See Section 5.6.
[16] *Id*.
[17] "The Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data is an independent advisory body on data protection and privacy, set up under Article 29 of the Data Protection Directive 95/46/EC. It is composed of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The Article 29 Working Party is competent to examine any question covering the application of the data protection directives in order to contribute to the uniform application of the directives. It carries out this task by issuing recommendations, opinions and working documents." Article 29 Data Protection Working Party, *Statement of the Article 29 Working Party*, 16 October 2015, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf .
[18] Article 29 Data Protection Working Party, *Statement of the Article 29 Working Party*, 16 October 2015, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf .

1.2 Purpose and Presentation of Questions

The purpose of this thesis is to investigate how the differences between the EU and U.S. privacy protection will affect a Safe Harbor 2.0 in light of the *Schrems* ruling and the right to erasure of the GDPR. The following questions will be answered in order to satisfy this thesis' objective:

- What are the impacts of the *Schrems* ruling for EU and U.S. companies engaging in transatlantic transfers of personal data?
- Can the U.S., at all, ensure an adequate level of protection that is "essentially equivalent" to the EU privacy protection?
- How will the discrepancy between the EU and the U.S. privacy protection affect a future Safe Harbor 2.0?

1.3 Definitions

"**Citizens**" is defined as a data subject in accordance with article 4(1) of the GDPR, i.e. "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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."

"**Personal data**" refers to EU citizens' personal data and has been given the definition provided in article 4(1) of the GDPR, i.e. "any information relating to an identified or identifiable natural person."

"**The EU privacy protection**" refers to the privacy rights individuals afford under both EU law and European law.

"**The U.S. privacy protection**" refers to the privacy rights individuals afford under both U.S. federal and state law.

"**Transfers**" refers to the situation when an EU or a U.S. company transfers EU citizens' personal data to the U.S.

1.4 Method and Material

This thesis is an elaboration of a "Directed Study" I did during my exchange year at Suffolk University Law School, academic year of 2014/2015 for professor Michael Rustad. The Directed Study had the working title "Does

the Right to be Forgotten Signal a Need to Reform the EU-U.S. Safe Harbor?" and contended that the current EU-U.S. Safe Harbor was to be outdated by the GDPR. In this thesis I continue to discuss the clashing transatlantic views on privacy. The discrepancy between the two privacy regimes presents challanges for the transatlantic flow of EU citizens' personal data for commercial purposes, and it is unclear how EU and U.S. companies should transfer such data in light of the proposed GDPR and the fact that the CJEU invalidated the current Safe Harbor.[19] Consequently, a part of the thesis will address some aspects of my Directed Study, i.e. the Safe Harbor. However, the objective of this thesis is to investigate how the differences between the EU and U.S. privacy protection will affect a Safe Harbor 2.0 in light of the *Schrems* ruling and the right to erasure of the GDPR. Moreover, the conclusions in this thesis have been based on the final compromise text of the GDPR from the Presidency of the European Council to the Permanent Representatives Committee made on 15 December 2015.[20]

The research in this thesis is based on a customary legal dogmatic method – a definition for which it has been found difficult to establish a homogenous factual content.[21] Acknowledging this fact, the method and material used can also be described as a scientific reconstruction of legal systems.[22] In this thesis, I will study EU and U.S. primary and secondary legislation, case law, guidelines, preparatory work, doctrine, and general principles. This will constitute an effort to systematize and structure relevant material in order to describe the EU and the U.S. privacy protection, the solutions for the clashing privacy regimes, and analyze the challenges for a Safe Harbor 2.0. Recent developments in this legal area have made the legal situation with regard to transatlantic transfers of personal data uncertain. The topic is current and there are many proposed changes affecting this legal area. Therefore, I have chosen also to use relevant news articles, and blog posts in my research in order to keep the information as up-to-date as possible. In addition, two data use policies will be used in order to illustrate the wide range of areas of use that personal data makes possible. The policies are used to illustrate how the use of personal data can be implemented in a company's privacy policy and demonstrate the extent to which personal data can be used, not only by the company collecting the data but also by third

[19] See Section 5.4.
[20] See Council of the European Union, *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) [first reading] - Analysis of the final compromise text with a view to agreement*, 15 December 2015, 2012/0011 (COD) [hereinafter "GDPR"].
[21] Sandgren, Claes, *Är rättsdogmatiken dogmatisk?*, at 649.
[22] Jareskog, Nils, *Rättsdogmatik som vetenskap*, SvJT 2004 at 4.

parties. This will facilitate for the reader in understanding the rationale for the EU privacy protecion.

To understand the issues surrounding the Safe Harbor 2.0, it is important to provide an overview of the EU and U.S. privacy protection. Therefore, the thesis is also written from a comparative perspective. This provides the reader with an understanding of the obstacles data transfers to the U.S. now face. The EU material include the European Convention for the Protection Human Rights and Fundamental Freedoms ("ECHR"), the right to privacy and personal data of the Charter of Fundamental Rights of the European Union ("the Charter"), the OECD Principles, The Directive, *Google Spain v. AEPD*, and the GDPR. Furthermore, the U.S. material include statutes illustrating the sectorial privacy approach, the White House proposal – *Consumer Privacy in a Networked World*, the First Amendment, the role of torts for privacy-based claims, Section 230 of the CDA, the Privacy Act of 1974, the USA PATRIOT Act, and the proposal for a Cybersecurity Information Sharing Act.

1.5 Delimitations

Since the thesis is directed to readers with an understanding of EU law, fundamental EU law will not be addressed. A reader who wishes to be more familiar with EU law is suggested to read *EU Law: Texts, cases, and materials* (2015) by Paul Craig and Gráinne de Búrca. Moreover, as one aspect of this thesis is to describe the privacy protection U.S. citizens enjoy, a comprehensive examination of the U.S. privacy protection will not be provided. Rather certain statutes have been selected to provide the reader with a basic understanding of the U.S. privacy protection in order to illustrate why the U.S. does not provide an "essentially equivalent" privacy protection.

One aspects of this thesis to discuss the impacts of the *Schrems* ruling for EU and U.S. companies engaging in trannsfers of personal data. In doing so, the thesis will address the lawful means for companies to transfer EU citizens' personal data to third countries. However, the research will focus on the Commission's possibility to make an adequacy decision in accordance with article 41 of the GDPR as this provides companies with an attractive instrument for transfers of massive amounts of Big Data. Other lawful means for transfers to third countries will only be briefly touched upon in order to provide the reader with a basic understanding of how personal data lawfully can be transferred to third countries. This thesis will focus on the invalidated Safe Harbor in analyzing what aspects should be considered when negotiating a Safe Harbor 2.0 that will satisfy EU demands

on privacy protection. However, I will not make any speculations regarding the actual content of a Safe Harbor 2.0.

The proposed GDPR lays down provisions for the protection of EU citizens' fundamental right to privacy. As the GDPR is an extensive privacy legislation, this thesis is limited to focus on Chapter V of the GDPR addressing transfers of personal data to third countries or international organizations in conjunction with the right to erasure. The right to erasure has been chosen to facilitate for the reader in understanding the problems arising from the discrepancy between the two privacy regimes, with regard to transatlantic transfers of personal data. The provision illustrates a certain aspect of privacy law where the EU and U.S. privacy protection clearly differ. This provision is especially important as the U.S. legal order does not recognize the right to erasure. This will facilitate for the reader to follow the arguments put forward in this thesis when discussing whether the U.S., at all, can ensure an adequate level of protection that is "essentially equivalent" and how the discrepancy will affect a Safe Harbor 2.0.

Finally, I will not address the second part of the data protection reform that regards the proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, which is intended to replace the 2008 Data Protection Framework Decision.

1.6 Research Position

The CJEU's ruling in the *Schrems* case has made the Safe Harbor an important topic to discuss as transfers of personal data is crucial to transatlantic trade. The outcome of the ongoing negotiations between the EU and the U.S. is difficult to predict, as this is just as much about politics as it is law. The consequences of this ruling are still being assessed and discussed in various forums, such as communications from the EU as well as articles and blog posts from both practicioners and journalists. Nonetheless, companies are left in obscurity when it comes to lawfool tools for transatlantic transfers of personal data. This is why every research that may shed some light on this important, yet obscure issue, is a welcome contribution.

1.7 Outline

This thesis starts off with a brief introduction to the concept of ”Big Data” and how companies can benefit from such data for commercial purposes. In the same Section 2, the reader will be introduced to how the use of personal data for commercial purposes can be reflected in a company’s data use policy. Section 2 has as its objective to provide the reader with a basic understanding of how companies use personal data in their business models. This knowledge is key in understanding the important role personal data can play in companies’ business models as well as understanding the rationale for the development of privacy protection in the “digital age”. In Section 3, the reader will be introduced to the EU privacy protection and the developments that lead up to the right to be forgotten. An introduction to the U.S. privacy protection will then follow in Section 4, reflecting the developments of the U.S. privacy protection that are the basis for the U.S. vigilance to the right to be forgotten. Together, Section 4 and 5 provide the reader with an overview of the EU and the U.S. privacy protection. This knowledge is key in understanding whether the U.S. at all can ensure a level of protection that is “essentially equivalent” to the EU privacy protection. Section 5 will describe the lawful measures that have been taken to facilitate for transatlantic transactions involving personal data, and will especially focus on the Safe Harbor. The section focuses on governmental enforcement and self-certification of the Safe Harbor in order to provide the reader with an understanding of the issues surrounding the program with regard to the protection of EU citizens’ personal data as a fundamental right. The section provides the reader with knowledge that is key for understanding the analysis addressing the impacts of the *Schrems* ruling for EU and U.S. companies engaging in transatlantic transfers of personal data. The final Section 6 will analyze the legal obstacles that stem from the discrepancy between EU and U.S privacy protection. The section discusses the impacts of the *Schrems* ruling for EU and U.S. companies engaging in transatlantic transfers of personal data, whether the U.S., at all, can ensure an adequate level of protection that is “essentially equivalent”, as well as any considerations that are required when negotiating a Safe Harbor 2.0.

2 Big Data in the Digital World

2.1 Everything Leaves a Digital Trace

Unlike information in history when a piece on information was taken and written down, Big Data is the opposite. Everything done online leaves a digital trace. For example, when using Google – a search is not just an extraction of data, but also a contribution to valuable information that allows for companies such as Google to save your searches. When turning and twisting such data, the data may be analyzed in a way that ultimately creates information. The data collected ranges from what we do to where we live to what we eat and how we sleep. The combinations are endless and everything is saved. This can be used for many beneficial purposes e.g. to predict infection risks for pre-maturely born infants, to predict flu epidemics, to predict health risks from data extracted from our genes, to discover treatments based on genetic profiles etc. However, the consequences of human interaction with techonology are yet to be discovered. Even though such data individually may be useful, a risk is created when every Internet user in one way or another contributes with that person's data creating a big cloud of data about peoples' behavior that can be crawled through by pattern recognition algorithms. This can, *inter alia*, allow companies to target consumers for marketing purposes, which can be either beneficial or detrimental for the consumer.[23]

2.2 Data Use as a Business Model

The economy has rapidly moved from an industrial economy to an informational economy where companies such as Google or Facebook have as their underlying business model the use of personal data, sharing and earning revenue on personal data provided by private persons.[24] To illustrate how companies can use personal data for marketing purposes one example can be made through Target. Target wanted to find out which of their customers were pregnant for marketing purposes.[25] To accomplish this objective, Target tracked the purchases of the customers that had signed up for Target's "Baby Register" and looked for patterns. By analyzing

[23] *I* UR Play, The Human Face of Big Data, 27 October 2014, http://urplay.se/Produkter/190174-Big-data-sa-kartlaggs-hela-ditt-liv [hereinafter: The Human Face of Big Data].
[24] Billy Ehrenberg, *How much is you personal data worth?*, The Guardian, 22 April 2014 08.17 a.m., http://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth.
[25] The Human Face of Big Data.

customer data and purchasing patterns, Target was able to predict which customers were pregnant and could use this information for marketing purposes.[26]

There is a new generation of practices and business models emerging, targeting consumers and using their personal data for commercial purposes. According to the World Economic Forum (WEC), personal data creates new opportunities for economic and societal value creation and is held to emerge "as a new asset class touching all aspects of society."[27] Moreover, personal data has been held to be "the new oil of the internet and the new currency of the digital world".[28]

While the value of personal data is growing, European citizens are worried about how their personal data is used online according to a new Eurobarometer. The trust in digital environments is low and only 15 % of the respondents feel that they have complete control of their online information whereas 31 % worry about having no control at all. Furthermore, seven out of ten respondents are concerned about their information being used for other purposes than the one for which it was collected. Most importantly, European citizens believe that they should have the same level of protection for their personal data, regardless whether the data processor is situated within the EU or in a third country.[29] There is also a risk that users do not understand the extent of their consent due to obscurity in a company's data policy or terms of use.[30] Obscure methods could result in that lawful means of data use are perceived as unlawful due to ignorance among users.[31] Consequently, there is a need to discuss how to best balance the businesses' right to use personal data for commercial purposes and any privacy concerns for the individuals raised by such business models.[32]

2.3 Data Use Policies

The previous Sections 2.1 and 2.2 have described the concept of Big Data and how it can be used in a company's business model. In practice, data use

[26] The Human Face of Big Data.
[27] World Economic Forum, *Personal Data: The Emergence of a New Asset Class*, January 2011, at 5.
[28] Meglena Kuneva, European Consumer Commissioner, *Roundtable on Online Data Collection, Targeting and Profiling,* 31 March 2009 [hereinafter: Meglena Kuneva (2009)].
[29] European Commission, *Data Protection Eurobarometer out today*, 24 June 2015, http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm [hereinafter: European Commission, *Eurobarometer*].
[30] See Section 2.4.
[31] Interview with Karl Engdahl, Legal Counsel at Klarna AB, 27 May 2015.
[32] Meglena Kuneva (2009).

policies are used in order to inform users of the company's collection of their personal data. One risk for companies when handling personal data is that the management of the company has not adopted any data use policies.[33] Even if a personal data protection officer[34] has been appointed within the organization, such officer must have the support from the management in order to secure that any privacy policy is accepted and implemented throughout the whole organization.[35] Data useage is a concern for a whole organization and not for the personal data protection officer alone.[36] Just as any other management business decision, a data use policy must actively be reviewed and revised in accordance with any future business development.[37] In the following, two data use policies will illustrate how the use of personal data can be implemented in a company's business model.

2.3.1 Google

Google collects information in order to improve the services that are provided to Google's users. The collected information is used to calculate and predict anything from a user's mother tongue to which advertisements or other users that may be of interest to a specific user, or suggest YouTube videos a user may like. The information Google collects about its users includes, *inter alia*, the information a user provides when signing up for a Google Account or when creating a Google Profile. It also includes the information that is provided from the use of Google's services. Examples of such information are when a user visits a website using Google's advertising services, or view and interact with Google's advertisements and content. More specifically the information includes device-specific information, log information, location information, information about unique application numbers, local storage information, and cookies and similar technologies.[38]

The collection of information allows Google to combine and analyze the information in order to provide personally relevant product features.[39] The Privacy Policy acknowledges that different people have different privacy concerns and a goal is therefore to be transparent about the collected

[33] Björn Johansson Heigis (Forum för Dataskydd), *Integritet i fokus nr 3/2015*, The Data Protection Board's Magazine (sv. Datainspektionens tidning), at 11 [hereinafter: Björn Johansson Heigis (2015).
[34] See the GDPR, art. 35-37.
[35] Björn Johansson Heigis (2015).
[36] See the GDPR, art. 35-37.
[37] Björn Johansson Heigis (2015).
[38] Google, *Privacy Policy*, last revised 19 August 2015, https://static.googleusercontent.com/media/www.google.com/sv//intl/en-GB/policies/privacy/google_privacy_policy_en-GB.pdf [hereinafter: Google, *Privacy Policy*].
[39] *Id*.

information. Therefore, the users can make certain choices on how Google uses their personal data. However, the Privacy Policy stresses that many of Google's services may not function if cookies are disabled. In some cases Google may also share personally identifiable information with third party companies, organizations, or indiviuals when Google has consent, the third party is a domain administrator, the information is needed for external processing, or for legal reasons. Additionally, non-personal identifiable information can be shared publicly with Google's partners, such as publishers, advertisers, or connected sites, or to demonstrate trends about the general use of Google's services.[40]

2.3.2 Facebook

Facebook's Data Policy states that Facebooks collects information, not only about what its users do and the information that they provide but also information about what *others* do and provide about *a specific user*. Depending on the permissions granted, Facebook also collects information from every device, e.g. computers, phones, or iPads, where its services have been installed or accessed. Even information related to visits on third-party websites and apps that use Facebook's services is collected. For example, information is collected when the website or app offer Facebook's "Like button", "Facebook Log In", or use its measurement and advertising services. Each and every piece of information is used in order to provide Facebook's users with customized experiences and personalized content.[41] In this way Facebook is able to understand its users interaction with the services Facebook provides, and the people and things their users are interested in, on and off its services.[42]

The information that Facebook collects is later used to provide, improve, and develop its services, to communicate with its users, to show and measure advertisements and services, and to promote safety and security.[43] However, the information is not limited to use in Facebook's own services and it can also be shared in a number of ways, e.g. to the people you share and communicate with, to people that see content that others share about you, apps, websites and third-party integrations on or using Facebook's

[40] Google, *Privacy Policy*.
[41] Facebook, *Data Policy*, last revised: 30 January 2015, https://www.facebook.com/full_data_use_policy, Section I [hereinafter: Facebook, *Data Policy*], at Section II.
[42] Facebook, *Data Policy*.
[43] Facebook, *How do we use this information?*, last revised: January 2015, https://www.facebook.com/about/privacy.

services, sharing within Facebook companies, and any new owners.[44] Additionally, the information can be shared with third-party partners and customers for e.g. advertising, measurement and analytics purposes,[45] and to vendors, service providers and other partners.[46] When sharing information to any third-party, Facebook complies with the U.S.-EU Safe Harbor Framework.[47]

2.4 Summary

Based on the foregoing, Big Data has emerged as a new asset class in the digital age and personal data has even been held to be the new oil of the Internet. Today, products are not the only source of revenue for a company but revenue can also be earned by the use of personal data. If you have a Facebook account, you have surely noticed how the advertisements on your Facebook page changes depending on e.g. the searches you do and which websites you visit. Everything done online leaves a trace and everything can be saved, unlike in history when information was normally written down on a piece of paper, allowing for easy erasure of that information. Personal data can be twisted and turned in endless combinations to fit the preferences of a specific company.

As illustrated by the data use policies, the use of personal data in a company's business model can be extensive and it is not only information that the user provides but can also amount to information that *others* provide about specific user. In addition, personal data may not only be kept within one entity but may often also be transferred to other entities with the organization or to third parties. One risk for such transfers is that not all companies have developed a policy for how it will ensure an adequate protection for personal data that covers the entire chain of transfers. On the one hand, customized experiences can be beneficial in a sense that users are presented with things they like and are interested in. On the other hand, it can be detrimental because a user's choices are narrowed and limited to be in line with the user's previous online preferences. For example, imagine you want to travel abroad and search for airline tickets on Google. You click on a website, which contains information about travel destinations in which you are interested. This specific website happens to be a third-party website that has incorporated Facebook's "Like button". Because you like the

[44] Facebook, *How is this information shared?*, last revised: January 2015, https://www.facebook.com/about/privacy [hereinafter: Facebook, *How is this information shared?]*.
[45] In these cases, Facebook only shares non-personally identifiable information.
[46] Facebook, *How is this information shared?*.
[47] Facebook, *How our global services operate?*, last revised: January 2015, https://www.facebook.com/about/privacy.

content, you click the “Like button”. One simple click, allows Facebook to collect your personal data that follow from your visit on the travel site. This piece of information is then used to provide you with “customized experiences and personalized content”. Hence, there is a chance (or a risk) that third-party advertisements related to travels abroad will show up on your Facebook homepage after your visit to that third-party website. This way, Facebook is able to understand how you, as a user, interact with its services, on as well as off its services.

The consequences of human interaction with techonology are yet to be discovered. Pattern recognition algorithms can crawl through big clouds of personal data about peoples’ behavior, ultimately resulting in revenue for companies using personal data as a business model. This is when a need arises to regulate the business’ right to use personal data for commercial purposes for the protection of individuals’ right to privacy. As awareness of data use differs, it is important that individuals are provided with legislation that protects their right to privacy.

3 The EU Privacy Protection

This thesis highlights an important transatlantic problem, i.e. the differences between the EU and the U.S. privacy protection. To understand the rationale for why the EU has given its citizens a right to be forgotten on the Internet, it is important to understand the developments of the EU privacy protection.

3.1 The Fundamental Right to Privacy and Personal Data

When the Lisbon Treaty entered into force on 1 December 2009, it amended the two fundamental treaties constituting the EU resulting in the Treaty on European Union ("TEU") and the Treaty on the Functioning of the European Union ("TFEU"). [48] Most importantly, Article 6 of the TEU sets out how the EU shall integrate fundamental rights into its legal order. The Lisbon Treaty also gives the ECHR the same legal status as the treaties, which enhanced the EU's connection with the fundamental rights of the ECHR. Furthermore, the Treaty states that any fundamental rights guaranteed by the ECHR shall constitute general principles in EU law.[49]

The right to privacy is also recognized in Article 8 of ECHR.[50] In Europe, the notion of privacy is "a broad term not susceptible to exhaustive definition."[51] It encompasses the physical as well as the psychological integrity of a person, and can also "embrace aspects of an individual's physical and social identity." Moreover, Article 8 of the ECHR protects "the right to personal development, and the right to establish and develop relationships with other human beings and the outside world."[52]

In addition to the ECHR, the EU has strengthened the fundamental rights for European citizens through the Charter of Fundamental Rights of the European Union ("the Charter").[53] This was considered a necessity in light of the changes in society, social progress and scientific and technological

[48] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306, 17.12.2007 [hereinafter: TEU], at 1–271.
[49] See TEU, art. 6.
[50] Directive 95/46/EC, at recital 10.
[51] European Court of Human Rights, *Case of Pretty v. The United Kingdom*, no. 2346/02, 29 April 2002, at para 61.
[52] *Id*.
[53] European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02, [hereinafter: the Charter], at C 326/395.

developments.[54] Articles 7 and 8 of the Charter state that everyone has the right to respect for private and family life including the person's communication and the right to protection of personal data.[55] Several EU Member States also provide a fundamental right for its citizens to access public records.[56] This right has also been recognized in the Charter.[57] Furthermore, in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González ("Google Spain v. AEPD")*, the CJEU highlighted that the provisions in the Directive shall be interpreted in the light of the Charter.[58] Through these provisions and the judgment of the CJEU, the EU offers a strong protection for privacy, which is complemented by the ECHR.

3.2 The OECD Principles

The Organization for Economic Co-operation and Development ("OECD") has promoted privacy as a fundamental value since 1980 and considers this as a condition for the crossborder flow of personal data.[59] Through the OECD, governments can work together and receive help in understanding how to best respond to new developments and concerns arising from, *inter alia,* the information economy.[60]

Because of the borderless character of the Internet, there is a common interest in a strengthened international privacy framework.[61] As a result, the OECD has provided guidelines that recommend Member Countries and non-Member Countries to adhere to their recommendation for how to handle challenges to the security in personal data.[62] The 1980's OECD Privacy Guidelines were revised in 2013, which recommend that eight basic principles should apply to personal data when it is processed in a way that poses a risk to privacy.[63] The eight principles are: (1) the Collection

[54] The Charter, at C 326/395.
[55] The right to personal data is hereinafter included in the notion "the right to privacy".
[56] See The Freedom of the Press Act (sv. Tryckfrihetsförordningen), ch. 2, § 1 and; The Data Inspection Board, *Kommissionens förslag till dataskyddsförordning (KOM (2012) 11 slutlig)*, dnr: 250-2012, 12 March 2012, at 2.
[57] The Charter, art. 42.
[58] Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (May 13, 2014) [hereinafter: *Google Spain v. AEPD*], at para 68.
[59] OECD, *OECD Privacy Principles*, http://www.oecd.org/sti/ieconomy/privacy.htm.
[60] OECD, *The OECD Privacy Framework*, 2013, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, at 2.
[61] *Id*. at 11-12.
[62] *Id*. at 12.
[63] OECD, *Guidelines governing the protection of privacy and transborder flows of personal data*", art. 2 in "The OECD Privacy Framework (2013)", http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [hereinafter: OECD Guidelines], at 11 and 13.

Limitation Principle, (2) the Data Quality Principle, (3) the Purpose Specification Principle, (4) the Use Limitation Principle, (5) the Security Safeguards Principle, (6) the Openness Principle, (7) the Individual Participation Principle, and (8) the Accountability Principle.[64] These principles were later embodied in the Data Protection Directive and provide the basis for the principles to which a company must adhere when developing its own self-regulatory principles under the Safe Harbor.[65]

3.3 The Data Protection Directive

Based on the notion of privacy as a fundamental right, the EU adopted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and of the free movement of such data. This went into effect in October 1998.[66] The objective was to remove obstacles with regard to the flow of personal data between Member States.[67] The EU had acknowledged that the processing of personal data was increasing in economic and social activity online.[68] Therefore, it was important that the data-processing systems contributed to an individual's well-being and respected its fundamental freedoms, notably the right to privacy.[69] The Directive requires Member States to comply with a number of principles relating to data quality.[70] These principles require that the processing of data must be (a) fair and lawful; (b) collected for legitimate and specified reasons; (c) adequate, relevant and not excessive in relation to the purposes for which it is collected; (d) accurate, and where necessary, kept up to date; and (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected.[71]

The Directive also addresses the fact that the Internet allowed personal data to easily cross borders, not only between Member States but also to third countries.[72] Because the flow of personal data on the Internet operates

[64] OECD Guidelines, at 14-15.
[65] This will be discussed further in Part IV. See also Michael L. Rustad, *Global Internet Law* (2014), West Academic Publishing [hereinafter: Michael L. Rustad (2014)], at 531.
[66] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050, 24 October 1995 [hereinafter: Directive 95/46/EC].
[67] Directive 95/46/EC, at recital 4 and 8.
[68] Directive 95/46/EC, art. 1 and recital 4.
[69] Directive 95/46/EC, at recital 2.
[70] Directive 95/46/EC, art. 6.
[71] *Id*.
[72] See Directive 95/46/EC, Chapter V – Transfer of Personal Data to Third Countries.

without borders, needless to say, so must the Directive.[73] In order to be able to regulate such processes the Directive was given extra-territorial effect meaning that data processors established in third countries were also subject to the application of the Directive.[74] Accordingly, such data processors had to respect the Directive in practice and ensure that an adequate level of protection was applied when transferring personal data to third countries.[75] In adopting the Directive, the EU wanted to harmonize national legislation that protects fundamental freedoms, i.e. the right to privacy, of EU citizens concerning the processing of their personal data.[76]

The Directive seeks to ensure an effective and complete protection of fundamental rights and freedoms of EU citizens as well as a high level of protection for such rights and freedoms.[77] To ensure compliance with the Directive, each member state had to provide a Data Protection Authority ("DPA") responsible to monitor application and enforce the provisions in the Directive.[78] Such DPA was to be given investigative powers, effective powers of intervention, and the power to initiate legal proceedings.[79]

3.4 Google Spain v. AEPD

This case is a historic ruling where the CJEU imposed an obligation for operators of search engines to remove personal information published by third parties relating to a person even when the publications originally were lawful.[80] This ruling recognized a first right to be forgotten for EU data subjects.[81] Through this ruling the broad notion of privacy as a fundamental right, became even broader as the CJEU extended the Directive's reach to third parties that processed a EU citizen's personal data.[82]

In 2010, Mario Costeja Gonzáles, a Spanish national, lodged a complaint with the *Agencia Española de Protección de Datos* ("AEPD") seeking erasure of personal data relating to him, which had been published and made

[73] See Directive 95/46/EC, at recital 56; and MacKay Cunningham, *Diminishing Sovereignty: How European Privacy Law Became International Norm*, 11 Santa Clara J. Int'l L. 421 (2012-2013) [hereinafter: MacKay Cunningham (2012-2013)], at 440.
[74] Directive 95/46/EC, at recital 20.
[75] *Id.* art. 25 and recitals 22, 57, and 60.
[76] Directive 95/46/EC, at recital 7; The European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS 5; 213 UNTS 221 [hereinafter: ECHR], art. 8; The Charter, art. 8.
[77] Directive 95/46/EC, art 1 and recitals 2 and 10. See also *Schrems v. DPC*, at para 39.
[78] Directive 95/46/EC, art. 28.1.
[79] Directive 95/46/EC, art. 28.3.
[80] C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González [hereinafter: Google Spain v. AEPD]*, May 13, 2014, at para 88.
[81] *Google Spain v. AEPD*, at paras 98-99.
[82] See Directive 95/46/EC, art. 4.

public by the daily newspaper, La Vanguardia and Google Spain or Google Inc.[83] The original La Vanguardia articles regarded true stories about Mr. Costeja González's insolvency.[84] However, as these proceedings had been resolved for over a decade, he contended that the information was now entirely irrelevant.[85] The AEPD held that the personal information relating to the La Vanguardia articles were legally justified, as they were part of a Ministry of Labour and Social Affairs order.[86] However, insofar the information was provided as links in a search result by Google's indexing programs, the AEPD held that this compromised the fundamental right to data protection and ordered Google to remove or conceal the links.[87] Google Spain and Google Inc. brought separate actions against the AEPD decision before the Audiencia Nacional ("the National High Court"), which stayed the proceedings to obtain a preliminary ruling from the CJEU.[88]

The CJEU concluded that a search engine processed personal data within the meaning of the Directive as the activity of a search engine consists of "finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference."[89] Moreover, the operator of the search engine was also regarded as the 'controller' in respect of that processing.[90] The Court held that it is the responsibility of the controller to take every reasonable step necessary to ensure that the personal data is processed in a way compatible with Article 6 of the Directive.[91] Incompatibility may arise when the data is inaccurate, inadequate, irrelevant, or excessive in relation to the purposes for which the data is processed.[92]

Furthermore, in its reasoning, the Court considered, *inter alia*, the Directive's objective and concluded that the provisions had to be interpreted in the light of the fundamental rights set out in the Charter, and the principle of proportionality.[93] By displaying results after merely typing in a person's name, a search engine could significantly affect fundamental rights to privacy and the protection of personal data.[94] Given that a search engine's

[83] *Google Spain v. AEPD*, at paras 14-15.
[84] *Id*. at para 14.
[85] *Id*. at para 15.
[86] *Id*. at para 16.
[87] *Id*. at paras 17, 28.
[88] *Id*. at paras 18, 20.
[89] *Id*. at para 41.
[90] *Id*. at para 41.
[91] *Id*. at para 72.
[92] *Id*. at para 92.
[93] *Id*. at paras 66-68.
[94] *Id*. at para 80.

list of results of information based on a person's name provides easy access and plays a decisive role in the dissemination of that information, this was concluded to "constitute a more significant interference with the data subject's fundamental right to privacy than the publication on [a] web page."[95] The CJEU therefore concluded that a data subject had a right to have content relating to his or her name removed from a list of result provided by a search engine in accordance with his or her fundamental rights set out in the Charter.[96] Nonetheless, the original information could still be accessed using other search terms than the person's name, or by direct access to the original source.[97] Consequently, complete deletion of the link generated by the indexing programs is not required.[98]

In conclusion, *Google Spain v. AEPD*, has given data subjects a right to request, under certain conditions, search engines to de-list links in search results based on his or her name.[99] It is important that data controllers adapt the processing of personal data to the CJEU's ruling, and implement new routines, which will guarantee an effective and complete protection of the data subject's right to be forgotten.[100] However, it should be noted that the right to be forgotten does not override any EU or Member State legislation requiring the retention of any personal data subject to a takedown request.[101]

3.5 The General Data Protection Regulation

To create a Single Digital Market within the EU, the European Commission proposed a comprehensive reform with the objective to strengthen online privacy rights for EU citizens and enhance the digital economy.[102] The GDPR has as its objective to "reinforce data protection rights of individuals, facilitate the free flow of personal data in the digital single market and reduce [the] administrative burden."[103] The reform is also intended to

[95] *Google Spain v. AEPD*, at para 87.
[96] *Google Spain v. AEPD*, at para 99.
[97] See *Google Spain v. AEPD*, at para 99; and European Commission, *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*, January 25 2012, Press Release Database, IP/12/46, http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en [hereinafter: Commission's proposal for comprehensive reform of data protection rules].
[98] *Id*.
[99] Article 29 Data Protection Working Party, *Adoption of guidelines on the implementation of the CJEU's judgment on the "right to be forgotten"*, November 26, 2014, Press Release, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20141126_wp29_press_release_ecj_de-listing.pdf.
[100] *Id*.
[101] See GDPR, art. 17.3(d).
[102] See Commission's proposal for comprehensive reform of data protection rules.
[103] See GDPR, at 2 and para 2.

increase European citizens' trust in digital services.[104] Furthermore, the inconsistency in how Member States implement the Directive has resulted in complexity, legal uncertainty, and administrative costs.[105] To ensure individuals right to privacy, there was a need to introduce a robust set of rules that are effective in the digital age. The GDPR will modernize the privacy principles set out in the Directive and focuses on "reinforcing individuals' rights, strengthening the EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards." The reform will especially ensure the protection of individuals' personal data when meeting the challenges of the borderless Internet. This will result in control and easier access by the individuals to which the personal data belong.[106] On 15 December 2015, the European Parliament and the Council presented their agreement on the final compromise text of the GDPR, which was presented by the Presidency of the European Council to the Permanent Representatives Committee.[107] The proposed GDPR will enter into force two years after adoption, at the earliest by 2018 if the current time frames are upheld[108], and will replace the Directive.[109]

According to the Eurobarometer, EU citizens are concerned about the protection of their personal data and how it is used online.[110] As consciousness about online use of personal data is growing, the EU legislator has recognized the need to have an effective enforcement to ensure that EU citizens' fundamental right to privacy and personal data is upheld.[111] The concerns of EU citizens are addressed by a specific set of rules, which include the right to be forgotten, easier access to one's data and right to data portability, the right to know when one's data has been hacked, data protection by design and default, and stronger enforcement of the rules.[112] In addition, the GDPR also aims to strengthen the powers of national data protection authorities.[113]

---

[104] European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIALCOMMITTEE AND THE COMMITTEE OF THE REGIONS, *A Digital Single Market Strategy for Europé*, 6 May 2015, COM(2015) 192 final, at 12-13.
[105] European Commission, *Questions and Answers – Data protection reform*, 21 December 2015, http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm?locale=en [hereinafter: European Commission, *Questions and Answers – Data protection reform*].
[106] *Id*.
[107] See the GDPR.
[108] The Data Inspection Board, *EU:s dataskyddsreform*, last updated March 2015, http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddsreform/.
[109] *Id*.
[110] European Commission, *Eurobarometer*
[111] See GDPR, Chapter V.
[112] European Commission, *Questions and Answers – Data protection reform*.
[113] See GDPR, Chapter VI and *Independent Supervisory Authorities*; and Commissioner Vera Jourová, *First Vice-President Timmermans and Commissioner Jourová 's press*

However, it is not only individuals the reform will benefit. For companies, the GDPR will result in clarity and consistency in application of the rules.[114] It also restores the trust of consumers, which will be beneficial for companies when operating on the "Digital Single Market". The GDPR will (1) eliminate any inconsistencies between Member States will be replaced by a single law for data protection, (2) introduce a one-stop-shop, making it cheaper and simpler for companies to do business when only having to deal with one single supervisory authority, (3) apply to all companies regardless where they are established when they offer goods or services on the EU market, and (4) enable innovation to thrive.[115]

3.5.1 The Right to Erasure

Article 17 of the GDPR gives an EU citizen a right to request, under certain conditions, a controller of personal data to erase the citizen's personal data and to inform any third party that such request has been made.[116] This provides all EU citizens with a right to be forgotten, a right which was first recognized in *Google Spain v. AEPD* when interpreting the provisions in the Directive.[117] In particular, this right can be exercised when the data is no longer necessary.[118]

The methodology for when and how the data subject may successfully claim a right of erasure is provided in the article:

> "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
> (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
> (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing of the data;
> (c) the data subject objects to the processing of personal data pursuant to Article 19(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing of personal data pursuant to Article 19(2);

---

conference on Safe Harbour following the Court ruling in case C-362/14 (Schrems), 6 October 2015, http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm.
[114] European Commission, *Questions and Answers – Data protection reform*.
[115] *Id*.
[116] See GDPR, art. 17.
[117] See Section 3.6.
[118] European Commission, *Questions and Answers – Data protection reform*.

> (d) they have been unlawfully processed;
> (e) the data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
> (f) the data have been collected in relation to the offering of information society services
> referred to in Article 8(1)."[119]

The article also provides an obligation for the data controller to inform third party websites that a request of erasure has been made. This gives the data controller the role as an intermediary between the data subject and any third party websites that have published personal data subject to the erasure request.[120] However, the obligation only includes "reasonable steps" to inform a third party, taking into account available technology and the cost of implementation.[121] If the conditions set out in Article 17.1 of the GDPR are satisfied, the data controller shall erase the personal data without delay.[122]

The media's reports of the right to be forgotten have lead citizens to believe that there is an absolute right to have their personal data erased. This is however an incorrect assumption given the exceptions to the right to be forgotten.[123] Because of the incorrect assumptions, trust and transparency have become essential facilitators in gaining access to citizens' data.[124] At the same time there are many companies, which choose control over sharing their data practices with citizens. In these cases, the key word is forgiveness rather than permission.[125] Such practices can lead to the belief that companies, which are transparent with their data practices to be perceived, as if they are the companies that collect personal data in an illegal manner.[126] Therefore, transparency is important for data practices in order to not make it a disincentive for companies that actually are transparent with their users. Clear and transparent information about the collection of personal data in e.g. a privacy statement or policy also provides users with an understanding of the company's business. Noteworthy is that the latest version of the GDPR includes a "further processing" provision, addressing Big Data, and that any further processing be compatible with the original

[119] GDPR, art. 17.1.
[120] *Id.* art. 17(2) of the GDPR. See also Michael L. Rustad, Sanna Kulevska, *Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow,* Harvard Journal of Law & Technology, Volume 28, Number 2 (2015) [hereinafter: Rustad, Kulevska (2015)], at 26.
[121] GDPR, art. 17.2a.
[122] See GDPR, art. 17.3.
[123] *Id*.
[124] Timothy Morey, Theodore "Theo" Forbath, and Allison Schoop, *Customer Data: Designing for Transparency and Trust,* May 2015, Harvard Business Review, https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.
[125] *Id*.
[126] Interview with Karl-Hugo Engdahl, Legal Counsel at Klarna AB, 27 May 2015.

purpose for which the data was collected.[127] The provision also lays down factors to consider when assessing the compatibility for such further processing.[128] The GDPR demands that any further processing for other purposes than the original purpose, for which the data was collected, is based on the data subject's consent.[129] At the same time, the GDPR provides that the information given to data subjects concerning processing should be extensive.[130] Thus, the new requirements concerning further processing and information present companies with new challenges in how to meet the requirements in a clear and transparent manner.

3.5.2 Exceptions to the Right to Erasure

As mentioned above, article 17 of the GDPR provides an exception to the obligation of erasure of the data controller. The exceptions applies when the retention of the personal data is necessary and one of the following conditions apply:

> "(a) for exercising the right of freedom of expression and information;
> (b) for compliance with a legal obligation which requires processing of personal data by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
> (c) for reasons of public interest in the area of public health in accordance with Article 9(2)(h) and (hb) as well as Article 9(4);
> (d) for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 83(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of the archiving purposes in the public interest, or the scientific and historical research purposes or the statistical purposes.
> (e) for the establishment, exercise or defence of legal claims."[131]

The exceptions of freedom of expression and historical and scientific research allow for e.g. news websites to operate on the basis of these principles.[132] For example, politicians cannot expect to have data, which was published with regard to his or her official position, removed from the website.[133] Additionally, because an assessment has to be made in each

[127] See GDPR, art. 5.1 (b) and art. 6.3a.
[128] GDPR, art. 6.3a.
[129] *Id.*
[130] GDPR, art. 7.
[131] GDPR, art. 17.3.
[132] European Commission, *Questions and Answers – Data protection reform*.
[133] *Id*.

specific case, this could be problematic as there is a risk that U.S. companies do such assessments based on U.S. privacy policies.[134]

The right to erasure is a key provision in the new privacy reform. It strengthens EU citizens' fundamental right to privacy as there now is an express provision regarding the right to be forgotten. This allows for erasure requests and clarifies this right, which was first articulated in *Google v. AEPD's*. The following section introduces the reader to the U.S.' vigilance to the right to be forgotten.

[134] See Section 4, which discusses the U.S. Vigilance to the Right to Be Forgotten.

4 The U.S.' Vigilance to the Right to Be Forgotten

4.1 Sectorial Privacy v. Comprehensive Privacy

In contrast to the EU, the U.S. does not have any comprehensive unanimous data protection laws, but rather it has chosen a sectorial approach. This approach renders data protection decentralized, fragmented, industry-specific, and largely uncoordinated among varying levels of government.[135] Therefore, when examining the privacy rights afforded under U.S. law, it is necessary to analyze all privacy-related statutes for a complete understanding of the U.S. privacy protection.[136] Various statutes such as the Health Insurance Portability and Accountability Act[137], the Health Information Technology for Economic and Clinical Health Act[138], the Children's Online Privacy Protection Act[139], and the Gramm-Leach-Bliley Act[140] provide a flawed patchwork of privacy legislation for U.S. citizens.[141] This was also acknowledged in the White House's proposal, *Consumer Data Privacy in a Networked World* ("the White House's proposal").[142] An example of the U.S. sectorial approach was well illustrated in MacKay Cunningham's, *Diminishing Sovereignty: How European Privacy Law Became International Norm*:

> "Examples of the U.S. sectorial approach include the Telecommunications Act of 1996, which restricts telecommunications carriers' use of private customer

[135] MacKay Cunningham (2012-2013), at 441 citing Patrick J. Murray, Comment, *The Adequacy Standard under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?*, 21 FORDHAM INTL L.J. 932, 949-51 (1998).
[136] Brian Craig, *Cyberlaw – The Law of the Internet and Information Technology*, Pearson Education (2013), at 183.
[137] *The Health Insurance Portability and Accountability Act of 1996*, Pub. L. 104-191, 110 Stat. (1996).
[138] *The Health Information Technology ("HITECH") Provisions of American Recovery and Reinvestment Act of 2009*, Title XIII, Subtitle D (Pub. L. 111-5, 123 Stat. 115, codified in relevant part at 42 U.S.C. §§ 17937 and 17954.
[139] *The Children's Online Privacy Protection Act of 1998*, 15 U.S.C.A. § 6501 Pub.L. 105-277, 112 Stat. (1998).
[140] The *Gramm-Leach-Bliley Act* (*GLB Act* or *GLBA*), also known as the Financial Modernization Act of 1999 is codified at 15 U.S.C. §6801.
[141] Rustad, Kulevska (2015), at 38.
[142] White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), http:// www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter: White House (2012)], at 6.

> Information; the Gramm-Leach-Bliley Act, which restricts financial institutions' use and dissemination of private financial data; 166 and the Fair and Accurate Credit Transactions Act, which restricts credit reporting and increases protections for related personal information. Whereas the European Directive articulates a single definition of personal information that governs its twenty-seven Member States, the U.S. sectorial approach breeds [*multiple, often disparate, definitions*]. The definition of personal data under the Fair Credit Reporting Act, for example, differs from the Video Privacy Protection Act, which differs from the Gramm-Leach-Bliley Act."[143]

As cross-border data flows have become a vital commercial component, international interoperability is crucial.[144] This is one of the reasons for the White House's proposal that was released in February 2012.[145] The rationale of the proposal was the need to address issues of "basic privacy principles that applied to the commercial world, and a sustained commitment of all stakeholders to address consumer data privacy issues."[146] This is to be accomplished by a Consumer Privacy Bill of Rights built on the Fair Information and Practice Principle. The bill will give consumers comprehensive, actionable, and flexible privacy rights that translate to the dynamic environment of the Internet.[147] Specifically, the Consumer Privacy Bill of Rights will provide for: individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability.[148] The proposal suggests enforcement through both self-regulatory bodies that will strengthen trust and commitment by companies in a code of conduct, and enforcement by the FTC.[149] Even though the Administration introduces a concept of mutual recognition,[150] the right to be forgotten has been held to be an "impermissibly antithetical" and an obstacle for unifying the transatlantic privacy regimes.[151] This discrepancy between the EU and the U.S. presents challenges in creating a uniform international privacy standard that facilitates for transatlantic transfers of personal data.

[143] MacKay Cunningham (2012-2013), at 442.
[144] See White House (2012), at 31.
[145] See White House (2012).
[146] See White House (2012), at 1, 10.
[147] See White House (2012), at 1, 9.
[148] See White House (2012), at 1.
[149] See White House (2012), at 29.
[150] See White House (2012), at 31.
[151] Robert G. Larson III, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech,* 18 Communication Law and Policy 91 (2013) [hereinafter: Robert G. Larson III (2013)], at 93.

4.2 Freedom of Speech

> ” 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.”[152]

This citation of the U.S. Supreme Court provides an understanding of the American position towards privacy. The key rationale for resisting the adoption of a national data protection regulation has been the constitutional right of free speech.[153] The First Amendment of the U.S. Constitution expressly protects free speech of U.S. citizens and was ratified in 1789.[154] The First Amendment states: “Congress shall make no law […] abridging the freedom of speech, or of the press.[155] Even if free speech compromises privacy interests, it is generally the latter that must give way as the First Amendment is construed to protect the free flow of information.[156] Defendants of the U.S. approach to data privacy contend that limitations of the sharing of personal information are a violation of the First Amendment.[157]

4.3 Privacy Based Cybertorts Supplementing Data Protection Laws

Where the patchwork of privacy legislation fails to provide protection, U.S. citizens have the option of tort as a cause of action.[158] The causes of action for invasion of privacy comprise four different torts: (1) intrusion upon seclusion, (2) right of publicity, (3) public disclosure of private facts, and (4) false light.[159] However, U.S. courts have been reluctant to stretch the tort of privacy to the Internet.[160]

All privacy-based torts, except for right of publicity, require that the invasion of a person’s privacy must be highly offensive to a reasonable person, which has been an obstacle for plaintiffs to prevail in privacy-based

[152] *Bartnicki v. Vopper*, 532 U.S. 514, 534, 121 S. Ct. 1753 citing *Time, Inc. v. Hill*, 385 U.S., at 388, 87 S.Ct. 534 (citing *Thornhill v. Alabama*, 310 U.S. 88, 102, 60 S.Ct. 736, 84 L.Ed. 1093 (1940).
[153] MacKay Cunningham (2012-2013), at 443.
[154] U.S.C.A. Const. Amend. I.
[155] The Constitution of the United States, Amendment I (1971).
[156] See *Bartnicki v. Vopper*, 532 U.S. 514, 534; Robert G. Larson III (2013), at 96; Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. Rev. 1149 2004-2005, at 1160.
[157] MacKay Cunningham (2012-2013), at 443.
[158] Michael L. Rustad (2014), at 418.
[159] RESTATEMENT (SECOND) OF TORTS § 652(B) (1977).
[160] Michael L. Rustad (2014), at 418.

causes of actions.[161] In *Booring v. Google, Inc*, the plaintiff's intrusion upon seclusion and right to publicity claims were dismissed because a reasonable person would not find a Google Street View car taking pictures of them to be "highly offensive".[162] The "highly offensive" prong in a torts claim leaves U.S. citizens with a weak protection for their private life and personal data. This also demonstrates the risk that EU citizens' face when their data has been transferred to the U.S. with regard to the possibility to prevail on a legal claim concerning their fundamental right to privacy.

4.4 Section 230 of the CDA

To entirely understand the U.S.' vigilance towards the right to be forgotten it is also important to mention Section 230 of the Communications Decency Act ("Section 230 of the CDA"). Congress enacted Section 230 of the CDA because of the U.S. policy to promote development of the Internet and to preserve a vibrant and free market with regard to the Internet and interactive computer services.[163] The section provides immunity for websites from liability for third party postings.[164] More specifically, websites are not regarded as publishers or speakers of information posted by third parties and can therefore not be held liable for defamatory content.[165] Neither can they be held liable for failing to remove tortious content.[166] In *Zeran v. America Online, Inc*, the Court ruled that Section 230 provides immunity for service providers even when refusing to take down illegal defamatory content posted by third parties after receiving notice.[167] Consequently, Section 230 provides a broad immunity for websites reflecting the U.S. privacy protection. In contrast, the CJEU's ruling in *Google Spain v. AEPD* went so far as to even impose a duty for search engines to remove irrelevant content in relation to a person's name.[168] This provides an example on the difference of the transatlantic privacy protection. Where the U.S. provides immunity for websites for defamatory third party content, the EU imposes liability even for search engines that merely finds information published or placed

[161] Michael L. Rustad (2014), at 419-424.
[162] *Boring v. Google, Inc.*, 362 Fed.Appx. 273, 279, 280, 38 Media L. Rep.1306 (2010).
[163] 47 U.S.C. § 230(b)(1)-(2).
[164] 47 U.S.C. § 230.
[165] 47 U.S.C § 230(c)(1).
[166] See *Zeran v. America Online, Inc.* 129 F.3d 327, (4th Cir. 1997).
[167] *Id*. at 331.
[168] See Section 3.6; and *Google Spain v. AEPD*, at para 16. "By decision of 30 July 2010, the AEPD rejected the complaint in so far as it related to La Vanguardia, taking the view that the publication by it of the information in question was legally justified as it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible."

on the Internet by third parties, indexes it automatically, stores it temporarily and, makes it available to Internet users.[169]

4.5 No Tradition of the Right to be Forgotten

The U.S. reluctance towards the right to be forgotten, and the absence of such right in the *Consumer Privacy Bill of Rights,* may lead to the assumption that the U.S. in all aspects has distanced itself from such a right.[170] Although a U.S. right to be forgotten in EU standards may be considered undeveloped, it is incorrect to assume that a right to be forgotten in the U.S. does not exist altogether.[171] In fact, the right to be forgotten has been recognized on a state level, in relation to some specific cases.[172]

4.5.1 Juvenile Offenses

Even though the notion of the right to be forgotten has yet to reach information on the Internet, there are other contexts in which the right to be forgotten has been acknowledged. One example is the expungement of juvenile offenses, which is treated under different statutes than when a defendant is an adult.[173] For juvenile offenders, most states provide procedures that allow them to have a juvenile court conviction expunged upon filing a petition in court.[174] The records can then be destroyed, expunged, sealed or otherwise made permanently inaccessible.[175] One state has even made expungement mandatory unless the state can show good cause for the retention of the records.[176] Through this possibility, a juvenile offender may choose to not disclose its criminal record to a prospective employer, property owner, or licensing agency.[177]

[169] See *Google Spain v. AEPD*, at paras 41 and 99.
[170] See White House (2012); and Section 4.1.
[171] Rustad, Kulevska (2015), at 40.
[172] See Section 4.6.
[173] Rustad, Kulevska (2015), at 40 citing James L. Buckwalter, *Causes of Action to Expunge Adult Records*, 37 Causes of Action 2d 615 (Originally published in 2008).
[174] Donald T. Kramer, 2 Leg. Rts. Child. Rev. 2D § 23:18 (2d ed.) available in Westlaw Secondary Sources.
[175] *Id*.
[176] *In Interest of John W.*, 300 Pa.Super. 293, 298, 446 A.2d 621.
[177] Rustad, Kulevska (2015), at 41 citing NOLO, Criminal Defense Lawyer, *Expunging of Sealing a Juvenile Court Record*, http://www.criminaldefenselawyer.com/topics/expunging-or-sealing-a-juvenile-court-record.

4.5.2 Personal Data of Minors

Furthermore, in 2013, the state of California passed Senate Bill No. 568, which went into effect on January 1, 2015.[178] The Bill provides a right for minors to request an online operator to remove content posted by the minor on a website.[179] Unlike GDPR's right to be forgotten, minors cannot request an online operator to remove data *related* to them as the right only covers postings made by the minors themselves.[180] Although this right may be considered limited in comparison with the GDPR's right to be forgotten[181], the right for minors to have their personal data removed is hopefully one step closer to approximation between the transatlantic regimes.

4.6 The Privacy Act of 1974

The Privacy Act of 1974 has as its objective to provide a comprehensive regulation of how personal data is processed.[182] The Act establishes a code for federal agencies in which the collection, maintenance, uses, and dissemination of all types of personal information is regulated.[183] This is the most approximate U.S. legislation to a European data protection law.[184] However, the protection is only afforded in relation to federal governmental bodies and even though it exists, the following Sections 4.7 and 4.8 demonstrates that the protection can be undermined.

4.7 The Patriot Act

As will be illustrated by the *Schrems case*, one important aspect of the U.S. approach to privacy is the USA PATRIOT Act ("the Patriot Act"). Pursuant to 9/11, Congress enacted the Patriot Act with the objective to unite and strengthen America by providing appropriate tools required to intercept and

[178] SB-568 Privacy: Internet: minors.(2013-2014) An act to add Chapter 22.1 (commencing with Section 22580) to Division 8 of the Business and Professions Code, relating to the Internet, [Approved by Governor September 23, 2013. Filed with Secretary of State, 23 September 2013.], http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.
[179] Cal. Bus. & Prof. Code § 22581(a)(1).
[180] *Id*.
[181] See Rustad, Kulevska (2015), at 41.
[182] Privacy Act of 1974, 5 U.S.C. § 552a.
[183] *Id*.
[184] Prof. Francesca Bignami, *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens*, Policy Department of the European Parliament, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU(2015)519215_EN.pdf, at 10.

obstruct terrorism".[185] The Act allows U.S. authorities to, *inter alia*, examine business records in national security terrorism cases.[186] Before the Patriot Act, such information could only be obtained by a grand jury subpoena, which was not considered appropriate with regard to national security cases.[187] In addition, the U.S. government can obtain business records by asking the Foreign Intelligence Surveillance Court which can order the production of the same type of documents available through a grand jury subpoena.[188] In light of the Snowden revelations, the Patriot Act is alleged to have resulted in access to records of personal data on a generalized basis.[189] The NSA defended itself stating, "if you have nothing to hide, you have nothing to fear."[190] However, the nothing-to-hide argument pervades discussions on privacy and the critique against U.S. authorities to access business records of personal data remains.

4.8 The Cybersecurity Information Sharing Act of 2015

On 27 October 2015, the Senate passed the controversial Cybersecurity Information Sharing Act of 2015 ("CISA").[191] The Act has as its objective to encourage the sharing of cyber threat information amongst private entities and between private entities and the federal government.[192] Consequently, the bill permits cross-sharing of information between entities and/or the federal government in cases where the information includes "cyber-threat indicators" and "defensive measures" that are consistent with a "cybersecurity purpose".[193] In reality, this means that entities and the federal government can share technical information, which indicates attacks on networks, and how such entities or the government have successfully

[185] Department of Justice, *The USA PATRIOT Act: Preserving Life and Liberty*, http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf.
[186] *Id*.
[187] *Id*.
[188] *Id*.
[189] *Schrems v. DPC*, at paras 93-95.
[190] Ewen Macaskill, Gabriel Dance, *NSA Files: Decoded – what the revelations mean for you*, The Guardian, 1 November 2013, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.
[191] congress.gov, *S.754 – Cybersecurity Information Sharing Act of 2015*, https://www.congress.gov/bill/114th-congress/senate-bill/754/text.
[192] See Sections 103-105 of the CISA.
[193] See the CISA; and Boris Segalis, Kathryn Linsky, *Senate passes cybersecurity bill, bringing immunity for sharing cyberthreat data closer to reality*, 2 November 2015, Norton Rose Fulbright, Data Protection Blog, http://www.dataprotectionreport.com/2015/11/senate-passes-cybersecurity-bill-bringing-immunity-for-sharing-cyberthreat-data-closer-to-reality/ [hereinafter: Segalis, Linsky (2015)].

detected, prevented, or mitigated such attacks.[194] Most importantly, an entity that wishes to participate in the program is offered significant protection. The CISA expressly states that entities sharing information under the program are effectively immune from liability.[195] Hence, there is an express prohibition of any cause of action against an entity that monitor or share information in accordance with the Act.[196] The bill's opponents have argued that this strips individuals of their basic privacy protection, as there is no possibility for individuals to opt out of CISA-sponsored monitoring.[197] The counter-arguments point to the fact that prior to sharing information, entities are required to review and remove any "irrelevant personally-identifiable information that may be contained in cyber threat indicators or defensive measures."[198] Yet again, EU citizens may be faced with the issue of having the U.S. government and U.S. companies deciding the fate of their personal data in accordance with U.S. policies with no regard for the EU fundamental right to privacy.

There clearly is a discrepancy between the EU and the U.S. privacy protection. However, personal data has become a valuable asset of transatlantic trade. This is why the discrepancy cannot result in a suspension of transfers of personal data altogether. The following section examines the solutions for the clashing privacy regimes with regard to transfers of personal data.

[194] Segalis, Linsky (2015)
[195] CISA, Section 106.
[196] *Id*.
[197] Segalis, Linsky (2015).
[198] See Segalis, Linsky (2015); and U.S. Senator for North Carolina, Richard Burr, *Debunking Myths about Cybersecurity Information Sharing Act*, 20 October 2015, http://www.burr.senate.gov/press/releases/debunking-myths-about-cybersecurity-information-sharing-act-.

5 Solutions for Clashing Privacy Regimes

5.1 Transatlantic Transfers of Personal Data

Transfers of personal data to third countries are addressed in Chapter V of the GDPR. Pursuant to this chapter, one instrument for lawful transfers of such data is if the third country in question can ensure an adequate level of protection for personal data.[199] It is the Commission that decides if such protection is ensured.[200] In determining whether this condition has been met, the Commission shall consider the following:

> " a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectorial, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of this legislation, data protection rules[,] professional rules and security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or international organisation, jurisprudential precedents, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
> (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate sanctioning powers for assisting and advising the data subjects in exercising their rights and for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Member States; and
> (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."[201]

[199] GDPR, art. 41.1.
[200] *Id*. art. 41.3.
[201] *Id*. art. 41.2.

Consequently, when the Commission deems that a third country ensures an adequate level of protection for personal data, no further authorization is required for transfers to that country.[202] The provision gives the Commission the power to provide companies with an attractive instrument for transfers of personal data to third countries, which ultimately facilitates for transatlantic trade.

The final compromised version of the GDPR contains two additions to the original wording in the Commission's proposal made in 2012. The two conditions that have been added to the methodology for the assessment of an adequate level of protection of importance to this thesis are (1) respect for human rights and fundamental freedoms, and (2) the access of public authorities to personal data.[203] Moreover, a new article has been added, which provides that any court judgment that require a company to transfer or disclose personal data is only recognized and enforceable if its been authorized by EU law.[204]

5.2 Lawful Instruments for Data Transfers

In cases where the Commissions has not made an adequacy decision, personal data can still be transferred to a third country if the data controller or processor can provide appropriate safeguards in a legally binding instrument.[205] Such safeguards can constitute e.g. binding corporate rules or standard protection clauses.[206] Pursuant to the *Schrems* decision, the WP29 has stated that it considers transfers under Standard Contractual Rules ("SCR") and Binding Corporate Rules lawful until the end of January, making their future existence uncertain.[207] Moreover, the SCR contain the same exception as the invalidated Safe Harbor and provide that mandatory national legislation do not contradict the SCR.[208] Consequently, there is reason to believe that the SCR as they are formulated today are also an unacceptable instrument for transfers. Additionally, other lawful instruments for transfers of personal data are when (1) the data subject has given its consent; (2) the transfer is necessary for the performance or conclusion of a contract; or (3) the transfer is necessary for public interest, or legal

[202] GDPR, art. 41.1.
[203] *Id*. art. 41.2 (a).
[204] *Id*. art. 43a.
[205] *Id*. art. 42.1.
[206] *Id*. art. 42.2 (a)-(c).
[207] *Id*.
[208] European Commission, COMMISSION DECISION of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 2010/87/EU, at clause 5, note 1.

claims.[209] Regarding transfers based on consent, the German DPAs consider that strict requirements apply and that such transfers may not generally take place repeatedly, excessively, or routinely.[210]

5.3 History of the Safe Harbor

As mentioned above, article 41 of the GDPR[211] provides the Commission with the power to provide companies with an attractive instrument for transferring personal data to third countries. When the Directive entered into force, U.S. companies were concerned with how to transfer EU citizens' personal data in a way that would satisfy the "strict" directive.[212] These concerns are still relevant with regard to the adoption of the GDPR. Given the concerns, the U.S. and the EU negotiated the Safe Harbor with the objective to develop a program for how U.S. companies could comply with the Directive.[213] In order to provide transparency for U.S. companies, the Safe Harbor program was negotiated as a way to harmonize the transatlantic views on the protection of personal data.[214] The Safe Harbor also provided streamlined and cost-effective means for U.S. companies to comply with the Directive.[215]

The Safe Harbor acknowledges that both the U.S. and the EU are working to enhance privacy protection for their citizens.[216] However, the protection of privacy is regarded from two different perspectives where the U.S. has a sectorial approach consisting of a mix of legislation, regulation, and self-regulation. To bridge the differences between the EU and the U.S, the U.S. Department of Commerce issued the Safe Harbor Privacy Principles and Frequently Asked Questions.[217] Pursuant to the Directive, the Commission decided that compliance with the Principles was considered to ensure an adequate level of protection when transferring personal data from the EU to

[209] GDPR, art. 44.1 (a)-(e).
[210] Jan Geer Ments, partner at DLA Piper, *German DPAs issue a Position Paper on Safe Harbor* (unofficial transfer of "Der Hessiche Datenschutzbeaufragte, *Positionspapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)*", 25 October 2015, https://www.linkedin.com/pulse/german-dpas-issue-position-paper-safe-harbor-jan-geert-ments, at para 9.
[211] Article 41of the GDPR corresponds with article 25.6 of the Directive.
[212] Daniel R. Leathers, *Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement,* 41 Case W. Res. J. Int'l L. (2009) [hereinafter: Daniel R. Leathers (2009)], at 194.
[213] Daniel R. Leathers (2009), at 193-195.
[214] *Id*.
[215] U.S. Department of Commerce, *Safe Harbor Privacy Principles*, 21 July 2000, http://www.export.gov/safeharbor/eu/eg_main_018475.asp [hereinafter: Safe Harbor Privacy Principles].
[216] Safe Harbor Privacy Principles.
[217] *Id*.

the U.S. ("the Safe Harbor decision").[218] However, on 25 June 2013, Austrian law student Maximilian Schrems challenged this decision resulting in the CJEU declaring the decision invalid.[219]

5.4 The Content of the Safe Harbor

5.4.1 The Safe Harbor Principles

The Principles create an assumption of satisfying the requisite of an adequate level of protection when transferring personal data to third countries set out in article 25 of the Directive.[220] The seven principles in the Safe Harbor Framework include:

1) The Notice Principle: requiring companies to give notice in a clear and conspicuous language to individuals about the purposes for which they collect and use their personal data, and of any disclosures of such data to third parties;
2) The Choice Principle: requiring companies to give individuals a choice to opt out when the personal data may be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected;
3) The Onward Transfer Principle: requiring companies to apply the principles of notice and choice when disclosing the personal data to third parties;
4) The Access Principle: requiring companies to give individuals a right to correct, amend, or delete information a company holds where it is inaccurate and the request for correcting, amending, or deleting is proportionate;
5) The Security Principle: requiring companies to take reasonable precautions to protect the personal data;
6) The Data Integrity Principle: requiring that the personal data must be relevant for the purposes for which it is to be used; and
7) The Enforcement Principle: ensuring compliance with the Principles and provides that a company shall have (a) readily and affordable independent recourse mechanisms, (b) proceedings for verifying that companies implement the Principles, and (c) sufficiently rigorous

[218] 2000/520/EC: COMMISSION DECISION of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, (notified under document number C(2000) 2441), OJ L 215, 25.8.2000, at 7–47.
[219] *Schrems v. DPC*, at paras 28, 106.
[220] Safe Harbor Privacy Principles.

remedies to ensure compliance with the Principles and that such remedies are enforced if a company fails to do so.[221]

5.4.2 Enforcement by Self-Regulation

The Safe Harbor's Enforcement Principle consists of three requirements. Firstly, a company must have an independent recourse mechanism.[222] This is similar to other U.S. privacy laws where the exclusive remedy is to bring a civil law suit if a company violates such laws.[223] The independent recourse mechanism gives companies several options. For instance, they can "self-certify" their use and aggregation of personal data through private e-sector privacy programs, such as BBB EU Safe Harbor Program or TRUSTe.[224] Another option is commitment to cooperate with the EU member states' Data Protection Authority or other private independent recourse mechanisms that "meet the requirements of the Enforcement Principle and the FAQ". They also have to option to comply with "legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution."[225] However, this does not amount to allowing the company itself to be its own "independent recourse mechanism."[226] A company can also qualify for the Safe Harbor by setting up its own self-regulatory privacy program provided it conforms to the Principles.[227] Failure to comply with its own self-regulation must be actionable under Section 5 of the Federal Trade Commission Act.[228] Secondly, a company must also verify that it has implemented its stated privacy principles. This requirement can be met by either submitting annual outside compliance reviews or by self-verification.[229] Thirdly, a company must provide remedies that can reverse any effects of non-compliance with the Principles, and ensure future compliance when processing personal data.[230] Such remedies should include publicity for findings of non-compliance and requirement to delete personal data.[231] However, it is within the discretion

[221] Safe Harbor Privacy Principles.
[222] *Id*.
[223] Daniel R. Leathers (2009), at 203-204.
[224] See export.gov, *Privacy "Seal" Programs* and *Alternative Dispute Resolution*, http://www.export.gov/safeharbor/eg_main_018241.asp.
[225] See Safe Harbor Privacy Principles, Annex II FAQ 6 – Self-Certification; Daniel R. Leathers (2009), at 204; and Christopher Wolf, PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE 14-3 (Christopher Wolf ed., Practicing Law Institute 2007), at 14-26.
[226] Daniel R. Leathers (2009), at 228.
[227] Safe Harbor Privacy Principles.
[228] *Id*.
[229] Safe Harbor Privacy Principles, *FAQ 7 – Verification*, *supra* note 18, Annex II.
[230] Safe Harbor Privacy Principles, *FAQ 11 – Dispute Resolution and Enforcement*, Annex II.
[231] *Id*.

of the dispute resolution body to decide whether sanctions for non-compliance should be used.[232]

Consequently, the company decides whether or not to delete the personal data depending on the sensitivity of the data and whether it has collected, used, or disclosed the data "in blatant contravention of the Principles."[233] If a company fails to comply with the Principles, an independent recourse mechanism must notify such failure to the Department of Commerce and the governmental body with applicable jurisdiction, which is usually the Federal Trade Commission.[234] Furthermore, the Principles suggest that sanctions include "suspension and removal of a seal, [and] compensation for individuals for losses incurred as a result of non-compliance and injunctive orders."[235]

5.4.3 Enforcement by Governmental Bodies

In addition to a company's option to self-regulate compliance with the Principles, the FTC was given authority to ensure that U.S. companies comply with the Safe Harbor framework.[236] The FTC has authority to regulate any "unfair or deceptive acts or practices in or affecting commerce."[237] This means that the FTC can only initiate actions when a company has failed to protect personal data "in accordance with their representations and/or commitments."[238] For instance, as in the Snapchat example where Snapchat misrepresented the use of data in its privacy policy.[239] Accordingly, such failure gives the FTC the power to prosecute any false representation as deceptive trade.[240] Several types of remedies are available to the FTC, such as a cease and desist order, restraining orders or injunctions, and in severe cases the FTC can promulgate an administrative ruling barring an act or practice as per se unfair or deceptive.[241]

One of the criticisms raised against the Safe Harbor was whether the internal and external enforcement mechanism is inadequate.[242] As of 12 November 2014, the FTC had brought ten enforcement actions since it went into force

[232] Safe Harbor Privacy Principles, *FAQ 11 – Dispute Resolution and Enforcement*, Annex II, at note 3.
[233] *Id*.
[234] Safe Harbor Privacy Principles, *FAQ 11 – Dispute Resolution and Enforcement*, Annex II.
[235] *Id*.
[236] *Id*.
[237] Federal Trade Commission Act, 15 U.S.C. §§ 41-58, Section 5.
[238] Safe Harbor Privacy Principles, Annex III.
[239] See Section 1.1.
[240] Daniel R. Leathers (2009), at 208.
[241] 15 U.S.C. § 45(b), § 53(b), and 57a(1)(b).
[242] Daniel R. Leathers (2009), at 195.

in July 2000.[243] However, since 2009, the FTC has brought 24 Safe Harbor cases and only in 2014 the FTC obtained separate settlements with fourteen companies that allegedly falsely claimed that they complied with the Safe Harbor.[244] From the FTC's own statistics follow that from 2009 until 2013, only ten Safe Harbor actions were brought over the course of five years, while in 2014 more than half of the enforcement actions were brought in just one year. The inconsistency in the FTC's enforcement of the Safe Harbor may have given critics a basis for alleging that the Safe Harbor's self-regulatory nature has failed to provide a surveillance mechanism adequate enough to ensure the protection of EU citizens' personal data. Additionally, the FTC's lack of efficient enforcement actions left EU citizens to report a company's violation of the Safe Harbor on their own.[245] For instance, if a U.S. company was subject to a data breach where thousands of identities were stolen, the company does not have an obligation to notify EU citizens under the Safe Harbor.[246] Moreover, the Safe Harbor does not address the right to be forgotten and U.S. companies have yet to recognize such right.[247]

5.5 Efforts to Make the Safe Harbor Safer

Pursuant to the Safe Harbor decision, the Commission issued a Staff Working Document on the implementation of its prior decision.[248] In the report, the Commission expressed its disappointment for the low number of registrants.[249] The number was lower than initially anticipated and raised concerns whether the benefits of the Safe Harbor, both for companies and data subjects, were sufficient.[250] The Commission's report concluded that there was significant non-compliance with the Principles.[251] For instance,

---

[243] The Federal Trade Commission, *Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework*, 12 November 2013, http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf, at 3. In its comments the Federal Trade Commission promises that it will continue to make the Safe Harbor "a top enforcement priority" and that more enforcement actions can be expected.
[244] Federal Trade Commission, *Privacy & Data Security Update (2014)*, http://www.ftc.gov/reports/privacy-data-security-update-2014.
[245] Daniel R. Leathers (2009), at 195.
[246] *Id*. at 195-196.
[247] Viviane Reding, *A Data Protection Compact for Europe*.
[248] COMMISSION STAFF WORKING DOCUMENT, The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC (2004) 1323, Brussels, 20 October 2004 [hereinafter: Commission Staff Working Document (2004)].
[249] *Id*. at 5.
[250] *Id.*
[251] *Id*. at 13-14.

"less than half of organisations post privacy policies that reflect all seven Safe Harbour Principles."[252] Specifically, the report called for a more proactive FTC in monitoring organizations compliance with the Principles.[253] The report urged the FTC to encoure data subjects to protect their rights and to seek FTC intervention, inform Safe Harbor members about the requirements, and to initiate actions in cases where the requirement is not satisfied.[254]

As of March 2013, the Department of Commerce made it mandatory for companies that had made commitments to the Safe Harbor program to make its privacy policy for customer data readily available on its public website.[255] This way, EU citizens could immediately verify whether or not a U.S. company had undertaken to comply with the Safe Harbor by visiting the official Safe Harbor List and website.[256] In its communication from the Commission to the European Council, it was yet again pointed out that there was a need to make the Safe Harbor safer.[257] Although the number of certified companies had increased to 3246 as of 2013[258], the lack of enforcement and transparency was held to have a negative impact on the fundamental rights of EU citizens.[259] Furthermore, it put EU companies at disadvantage when competing with U.S. companies that had joined the program but did not comply with the Principles.[260] To solve any compliance issues arising from the Safe Harbor, the Commission stated that the Department of Commerce must ensure incorporation by providing a methodology of compliance under which U.S. companies would comply with the Principles when handling EU citizens' personal data.[261]

5.6 The End of the Safe Harbor

The concerns truly escalated on 25 June 2015 when Austrian law student Maximilian Schrems lodged a complaint with Ireland's data protection

[252] Commission Staff Working Document (2004), at 9.
[253] Commission Staff Working Document (2004), at 8 and 10.
[254] *Id*.
[255] European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL – Rebuilding Trust in EU-US Data Flows, COM(2013) 846 final, 27 November 2013 [hereinafter: European Commission, Rebuilding Trust in EU-US Data Flows], at 7.
[256] *Id*.
[257] European Commission, Rebuilding Trust in EU-US Data Flows, at 6-7.
[258] European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final, 27 November 27, 2013, at 4.
[259] European Commission, Rebuilding Trust in EU-US Data Flows, at 6.
[260] *Id*.
[261] European Commission, Rebuilding Trust in EU-US Data Flows, at 9.

commissioner alleging that Facebook Ireland's transfer of his personal data to the U.S. could not be guaranteed an adequate level of protection in light of the Snowden revelations.[262] On 25 July 2014, the High Court of Ireland referred the case to the CJEU for a preliminary ruling to, *inter alia*, decide whether the Safe Harbor, *de facto*, provides an adequate protection for transfers of EU citizens' personal data.[263] The Court concluded the Safe Harbor decision to be invalid and gave the following grounds for its decision.[264]

When determining whether an adequate level of protection is offered by a third country, the assessment must be made by reason of the third country's domestic law or its international commitments. Moreover, the adequate protection must be assessed in light of "the protection of the private lives and basic freedoms and rights of individuals."[265] The objective is to ensure that "the high level of […] protection continues where personal data is transferred to a third country."[266] In order to ensure that a third country provides an adequate level of protection, the third country is required to have a level of protection of fundamental rights and freedoms that is "essentially equivalent" to the protection provided in the EU.[267] Hence, it is the legal order of the third country that must ensure an adequate level of protection. The requisite of an "essentially equivalent" level of protection must prove effective in practice in order to satisfy the requisite.[268] In this regard, the Commission's adequacy decision only concerned the adequate level of protection provided in the U.S. under the Safe Harbor, without sufficient findings of whether the U.S. ensured an adequate level of protection by reason of its domestic law or its international commitments.[269] Furthermore, an adequacy decision must be subject to periodical checks to ensure that the decision is still factually and legally justified.[270] In light of the Charter, any review regarding the validity of an adequacy decision should be strict.[271]

Even though self-certification in itself is not contrary to the requirement that a third country must ensure an adequate level of protection, the reliability of

[262] Nikolaj Nielsen, *EU-US data pact skewered in court hearing*, 25 March 2015, euobserver, https://euobserver.com/justice/128131.
[263] See *Schrems v. DPC*; Sam Pfeifle, *ECJ Hears Safe Harbor Arguments*, 24 March 2015, The Privacy Advisor, https://privacyassociation.org/news/a/ecj-hears-safe-harbor-arguments/.
[264] *Schrems v. DPC,* at para 106.
[265] *Id.* at para 71.
[266] *Id.* at para 72.
[267] *Id.* at para 73.
[268] *Id*. at para 74.
[269] *Id.* at para 83.
[270] *Id.* at para 76.
[271] *Id.* at para 78.

the U.S. system was questioned as the U.S. public authorities had no obligation to comply with the Safe Harbor.[272] The Court considered that the U.S. system did not provide any effective detection or supervision mechanism that identified and punished infringements of the Safe Harbor in practice.[273] The Safe Harbor decision did not only allow for companies to self-certify to the Principles, but also stated that in cases where U.S. law imposes a conflicting obligation, U.S. law precedes over the principles pursuant to the Safe Harbor.[274] The Court considered this to result in that U.S. organizations, receiving personal data from the EU, were bound to disregard the Principles without limitation whenever the Principles were in conflict with U.S. law.[275]

The Court also addressed the fact that the Commission's own assessment of the Safe Harbor had pointed out that U.S. authorities could access personal data transferred from Member States and that such data later was processed in a way incompatible with the original purpose "beyond what was strictly necessary and proportionate to the protection of national security."[276] The Court noted that the Safe Harbor decision did not contain any findings regarding the existence of U.S. rules that would limit such interference with the fundamental rights of EU citizens or any effective legal protection of such interference.[277] According to the Court, it is clear that any EU legislation protecting fundamental rights and freedoms must lay down clear and precise rules governing the scope and application of measures and impose minimum safeguards. This in order to provide EU citizens with sufficient guarantees for effective protection of their personal data "against the risk and abuse and against any unlawful access and use for that data."[278] Any derogation or limitation from this can only apply in so far as it is strictly necessary.[279]

Additionally, the Court stated that effective protection cannot be achieved when storage and access by public authorities of personal data is made on a generalized basis.[280] This was considered to compromise the very essence of the fundamental right to privacy. Hence, the Court held that there is no

[272] *Schrems v. DPC,* at paras 81-82.
[273] *Id.* at para 81.
[274] *Id.* at paras 80 and 85. See also Decision 2000/520, art. 1(2) and (3) in conjunction with FAQ 6 of Annex II and Part B of Annex IV.
[275] *Schrems v. DPC,* at para 86.
[276] *Id.* at para 90.
[277] *Id.* at paras 88 and 89.
[278] *Id.* at para 91.
[279] *Id.* at para 92.
[280] *Id.* at paras 93-95. See also art. 47 of the Charter requiring a right to an effective remedy before a tribunal if there is a violation of an individual's rights and freedoms guaranteed by EU law.

respect for the fundamental right to effective judicial protection in these situations.[281] The same is true when there is no possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data.[282]

Furthermore, the Safe Harbor decision layed down specific rules regarding the powers available to the national supervisory authorities in relation to the decision resulting in a restriction of such authorities' investigative powers.[283] The Court held that the Commission exceeded its powers when it restricted the national supervisory authorities powers.[284] In addition, an adequacy decision cannot prevent a supervisory authority from examining a claim of an individual with regard to his or her fundamental rights and freedoms. Especially not when the claim concerned (1) the processing of that individual's personal data transferred from a Member State to the third country; and (2) when such claim contends that the third country does not ensure an adequate level of protection.[285] Based on the foregoing, the Court concluded the Safe Harbor decision invalid in its entirety.[286]

5.7 The *Schrems* Impacts

Pursuant to the *Schrems* decision, the German DPAs issued a position paper on the Safe Harbor.[287] However, the German DPAs have not yet initiated any investigation, which may be due to the fact that the WP29 stated that this landmark ruling requires a "robust, collective, and common position on the implementation of the judgment."[288] Moreover, the WP29 considers massive and indiscriminate surveillance to be contrary to EU legislation on privacy and that it is also a key element of the CJEU's analysis.[289]

---

[281] *Schrems v. DPC*, at paras 93-95.
[282] *Id*. at para 95.
[283] *Id*. at paras 100-103.
[284] *Id*. at para 103-104.
[285] *Id*. at para 66.
[286] *Id*. at paras 104-105.
[287] See Der Hessiche Datenschutzbeaufragte, *Positionspapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)*, last updated: 26 October 2015, https://www.datenschutz.hessen.de/ft-europa.htm#entry4521; and Jan Geer Ments, partner at DLA Piper, *German DPAs issue a Position Paper on Safe Harbor* (unofficial translation of "Der Hessiche Datenschutzbeaufragte, *Positionspapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)*", 25 October 2015, https://www.linkedin.com/pulse/german-dpas-issue-position-paper-safe-harbor-jan-geert-ments.
[288] Article 29 Data Protection Working Party, *Statement of the Article 29 Working Party*, 16 October 2015, http://ec.europa.eu/justice/data-protection/article-29/pressmaterial/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf [hereinafter: *Statement of the Article 29 Working Party* (2015)].
[289] *Statement of the Article 29 Working Party* (2015).

Furthermore, it stated that a safe destination for transfers is not at hand when the authorities of third countries can access information beyond what is necessary in a democratic society. Consequently, political, legal, and technical solutions are required to enable transfers of personal data to the U.S that respect fundamental rights. The WP29 has granted companies and organizations a "grace period" until the end of January 2016 that allows for companies to find alternative methods of transfers. During this time, the WP29 also considers transfers under Standard Contractual Rules and Binding Corporate Rules as lawful. However, the WP29 demands an appropriate solution to be found between EU and the U.S. If a solution cannot be found, EU data protection authorities will be compelled to take all necessary and appropriate actions, which may include coordinated enforcement actions.[290] Additionally, the alternative instruments for lawful transfers, i.e. the BCR and the SCR, are only considered lawful until the end of January 2016. Thereafter, investigations can be expected which will evaluate the adequacy of the BCR and the SCR and it is questionable whether the instruments will be upheld or quashed.[291] Moreover, the GDPR includes provisions of stricter penalties and fines for infringements of the regulation.[292] Each supervisory authority has the power to impose administrative penalties, which aim to strengthen and harmonize the penalties against infringements.[293] Infringements regarding the data subject's rights can be subject to penalties amounting to 20 000 000 EUR, or up to 4 % of the total annual turnover, whichever is higher.[294] For now, companies transferring personal data across the Atlantic are not only left with few lawful instruments for transfers, awaiting the Safe Harbor 2.0, but they are also left with the fear of penalties.

Because of the legal uncertainty, compliance has become important for EU and U.S. companies that handle personal data. One obvious, straightforward method to comply with the *Schrems* decision is to keep the data within the EU. For example, Oracle now offers their cloud customers the possibility to store data in Europe in order to avoid that data is being sent across geographical border or to any other legislative boundary.[295] However, the *Microsoft* case shows that U.S. federal courts may consider search warrants issued in the U.S. sufficient to access personal data that is subject to another

[290] *Statement of the Article 29 Working Party* (2015).
[291] See Section 5.2.
[292] GDPR, at recital 118b.
[293] *Id*. at recital 120 and art. 79.1a.
[294] *Id*. art 79.3a.
[295] Karlin Lillington, *Oracle keeps European data within its EU-based data centres*, 28 October 2015, The Irish Times, http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505.

jurisdiction.[296] The case is currently on appeal before the Unites States Court of Appeals for the Second Circuit.[297] However, even if the decision is upheld, a company may enjoy protection under the GDPR as a court judgment that require a company to transfer or disclose personal data only is recognized and enforceable if its been authorized by EU law.[298] Thus, the choice of storing personal data in the EU to avoid the legal impacts of the *Schrems* case may still be a reliable measure.

Optimally, a company that relies on the Safe Harbor for transfers of personal data should cease its transfers while waiting for the Safe Harbor 2.0. However, for most businesses this is not an option. For transfers of personal data during the grace period, David Frydlinger, partner at Swedish law firm Lindahl advise companies to obtain an inventory of their transfers of personal data to the U.S.[299] This allows companies to analyze under which exception the data has been transferred. Consequently, this provides companies with an overview of their transfers as well as an opportunity to transfer the data under another exception than the Safe Harbor.[300]

During the "grace period" transfers of personal data should be well documented.[301] One option for companies is to create an internal policy document for transfers of personal data.[302] The policy may constitute legal assessments of the invalidation of the Safe Harbor regarding transfers of personal data. Moreover, the policy may provide obligations of documentation for the company's transfers of personal data regarding the exceptions under which each transfer is made. In any case, no new agreements for data transfers should be entered into that relies on the Safe Harbor.[303]

---

[296] *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation*, 15 F.Supp.3d 466 (S.D.N.Y. 2014).
[297] United States Court of Appeals for the Second Circuit, *Microsoft Corporation v. Unites States of America*, Case number 14-2985.
[298] GDPR, at recital 90 and art. 43a.
[299] David Frydlinger, partner at Lindahl, *Frukostseminarium med Advokatfirman Lindahl om Safe Harbor-domen*, 23 October 2015, http://www.lindahl.se/se/om-oss/senaste-nytt/seminarier/2015/frukostseminarium-om-safe-harbor-domen/.
[300] *Id*.
[301] *Id*.
[302] Interview with Karl-Hugo Engdahl, Legal Counsel at Klarna AB, 4 December 2015.
[303] *Id*.

6 Analysis

The previous chapters have described as well as briefly analyzed how the "digital" privacy protection has developed in the EU and the U.S. and has aimed to give the reader an understanding of why there is a discrepancy between the two privacy regimes. The reader has also been introduced to the solutions for the clashing privacy regimes and the lawful instrument for transfers of personal data that are available to EU and U.S. companies. In Section 1.2 the reader was presented with three questions that would satisfy this thesis objective of investigating how the differences between the EU and U.S. privacy protection will affect a Safe Harbor 2.0 in light of the *Schrems* ruling and the right to erasure of the GDPR. These comprised the following questions:

- What are the impacts of the *Schrems* ruling for EU and U.S. companies engaging in transatlantic transfers of personal data?
- Can the U.S., at all, ensure an adequate level of protection that is "essentially equivalent" to the EU privacy protection?
- How will the discrepancy between the EU and the U.S. privacy protection affect a future Safe Harbor 2.0?

In the following, I will answer these questions based on the findings in the research.

6.1 Impacts of the *Schrems* Ruling

This thesis has focused on the possibility for the Commission to make an adequacy decision under article 41 of the GDPR. The adequacy decision provides companies with a lawful instrument for transfers of personal data. In the *Schrems* ruling, the CJEU invalidated the current adequacy decision, i.e. the Safe Harbor, and layed down requisites, regarding the assessment of the third country's privacy protection, that must be satisfied when making an adequacy decision. The requisites for making such decision will be discussed in the following Section 6.2.

The invalidated Safe Harbor resulted in that EU and U.S. companies, engaging in transatlantic transfers of personal data, no longer have an attractive and simple instrument for such transfers. For now, companies transferring personal data across the Atlantic are left with few lawful instruments for transfers, awaiting the Safe Harbor 2.0. A "grace period" has been given, until the end of January 2016, to find alternative methods

for transfers of personal data before Member State DPAs are compelled to take all necessary and appropriate actions. This may include coordinated enforcement actions regarding the lawfulness of transfers. Additionally, the new provision of higher penalties in the GDPR, will most likely give companies an incentive to review the methods under which transfers of personal data are made. The obscure legal situation and the risk of higher penalties has placed an implicit burden of documentation on companies as legal advisors recommend them to (1) obtain an inventory over the transfers of personal data to the U.S.; (2) review under which exception the data is transferred; and (3) create an internal document, which states the assessments that have been made when transferring personal data to the U.S. However, it should be noted that all companies may not have the resources to ensure compliance or even resources to obtain legal advise. In these cases, I believe that it ultimately is the Member State DPAs that have a special responsibility to communicate the new changes to these companies.

As a result of the *Schrems* ruling, Member State DPAs are not prevented from examining a claim concerning privacy rights merely because the Commission has adopted a decision under article 41 of the GDPR. The implication that follows from this is that the transparency and certainty that made the Safe Harbor attractive can be undermined by independent DPAs as they have the ultimate power to examine if a Safe Harbor 2.0, *de facto*, provides an adequate level of protection. In my opinion, a Safe Harbor 2.0 must provide companies with transparency and certainty for their transfers of personal data. If companies cannot rely on a Safe Harbor 2.0 for transatlantic data transfers, article 41 of the GDPR will loose its character of being an attractive solution for cross-border transfers – a solution, which ultimately facilitates for transatlantic trade with regard to personal data.

6.2 The Transatlantic Discrepancy: Can the U.S Ensure an "Essentially Equivalent" Level of Protection?

The discrepancy between the two privacy regimes, the outcome in the *Schrems* case, and the proposed GDPR have made it unclear whether the U.S., at all, can ensure an adequate level of protection, i.e. an "essentially equivalent" level of protection to the EU privacy protection. The CJEU concluded, in the *Schrems* ruling, that it is the Commission's responsibility to thoroughly examine the U.S. privacy protection and conclude whether or not an adequate level of protection can be ensured. Furthermore, the Court stated that when determining whether an adequate level of protection is offered by a third country, the assessment must be made by reason of the

third country's domestic law or its international commitments. Additionally, an adequacy decision under article 41 of the GDPR require the Commission to consider, *inter alia*, respect for human rights and fundamental freedoms, relevant legislation, both general and sectorial including legislation that concerns national security, any data protection rules, professional rules and security measures, the access of public authorities to personal data, effective and enforceable rights, and the existence and effective functioning of one or more independent supervisory authorities, i.e. the FTC. The last two factors are more specifically discussed in Section 6.3.

6.2.1 The U.S. Sectorial Privacy Legislation

The EU has in its legislation acknowledged the fact that information easily can cross borders in today's information techonology society. As a result, the right to privacy and personal data has been enshrined in important legislation that protects EU citizens' fundamental rights and freedoms. Moreover, such right was strengthened through the Directive, which acknowledged that because the processing of personal data was increasing in economic and social activity online, it was important that such data-processing systems contributed to an individual's well-being and respected its fundamental freedoms, i.e. the right to privacy. Contrary to the EU privacy legislation, the U.S. patchwork of privacy legislation results in fundamental deficiencies such as a lack of a unanimous definition for "personal data". Additionally, the lack of a comprehensive privacy protection leaves U.S. citizens with torts as a cause of action for any privacy-based claims. This includes a "highly offensive" prong that must be satisfied in order to prevail in a privacy-based claim. The research has shown that in contrast to the EU privacy protection, the U.S. sectorial privacy legislation fails to provide its citizens with a unanimous comprehensive privacy protection.

Furthermore, the right to privacy was later strengthened in *Google v. AEPD*. In this case, EU citizens were given a first right to be forgotten on the Internet with regard to search results based on his or her name. The CJEU imposed an obligation on search engines to remove personal data published by third parties relating to a person even when the publications originally were lawful. The rationale for the imposed obligation was that search engines' list of results relating to a person provided easy access and played a decisive role in the dissemination of that information. According to the Court, this constituted significant interference with the data subject's fundamental right to privacy. In contrast, Section 230 of the CDA provides websites with immunity for third party content and a website has no

obligation to remove such content even when the content is of a defamatory nature.

The right to be forgotten in *Google v. AEPD* has now been extended to an express right to erasure in the GDPR. The GDPR modernizes the privacy principles set out in the Directive and focuses on "reinforcing individuals' rights, strengthening the EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards." The reform will especially ensure the protection of individuals' personal data when meeting the challenges of the borderless Internet. This EU privacy protection provides the framework for the assessment of an "essentially equivalent" level of protection. Although the White House has released a proposal that will strengthen privacy rights that translate to the dynamic environment of the Internet, the strong protection of free speech is a key rationale for why a right to be forgotten has not been accepted in U.S. law. . In connection with the White House's proposal, it has even been held that the right to be forgotten is an "impermissible antithetical". Only in cases where the personal data belongs to a minor is it possible to notice an approximation between the two privacy regimes. In some specific cases, U.S. minors have a right to be forgotten with regard to juvenile offenses and the removal of content posted by the minors themselves.

6.2.2 The Fight Against Terrorism

One important issue is the possibility for U.S. authorities to access EU citizens' personal data on a generalized basis under the Patriot Act, which may undermine the fundamental right to privacy. In the *Schrems* case, the CJEU clarified that the adequacy decision must contain findings of rules that do not interfere with EU citizens fundamental right to privacy or effective legal protection that prevent such interference. As U.S. authorities on a generalized basis can access records of personal data in accordance with the Patriot Act, the U.S. privacy protection can be undermined by the U.S.' efforts to intercept and obstruct terrorism. In addition, the CJEU held that access to individuals' personal data on a generalized basis could not be considered to respect the EU fundamental right to privacy and thus, not provide a protection that is "essentially equivalent" to the EU protection. Furthermore, article 41.2 of the GDPR specifically points out that the Commission is required to consider the possibility for a country's authorities to access personal data. Consequently, the U.S. cannot be considered to satisfy an "essentially equivalent" level of protection if U.S. authorities continuously may access individuals' personal data and process such data in a way incompatible with the original purpose. This especially,

when this is done beyond what was strictly necessary and proportionate to the protection of national security without any safeguards that would limit interference with the fundamental rights of EU citizens. Furthermore, there may be new U.S. legislation on its way offering the U.S. government, and U.S. companies, extensive protection for the sharing and monitoring of information under the proposed CISA. If the CISA becomes U.S. law, the issue will yet again concern the enforcement of EU citizens fundamental right to privacy.

6.2.3 No Respect for the EU Fundamental Rights and Freedoms

The EU offers a strong privacy protection for its citizens. Not only is the notion of privacy regarded as a broad fundamental right but the CJEU has also given EU citizens a right to be forgotten on the Internet and new strengthened privacy legislation is on its way. However, as has been concluded in Section 4, the U.S. has a fundamentally different privacy protection, and it does not recognize the right to be forgotten, which is one of the key provisions in the GDPR. If the U.S. cannot recognize one of the EU's key provisions of the privacy protection it offers to EU citizens, it can be questioned whether the U.S., at all, could ensure an adequate level of protection. In my opinion, the privacy protection of a third country is not sufficient when it can be questioned, which makes it even more important that EU citizens privacy rights are guaranteed in a Safe Harbor 2.0.

Because the U.S. does not recognize the important provision "the right to erasure", it is my opinion that the U.S. legislation fails to respect EU citizens' fundamental rights and freedoms. There is a U.S. legislation providing companies with immunity for third party postings and critique has been raised against the FTC for not properly enforcing compliance under the Safe Harbor. The *Schrems* court considered that the U.S. system did not provide any effective detection and supervision mechanism that identified and punished infringements of the Safe Harbor in practice. Because the FTC only can initiate legal proceedings against companies in order to prohibit unfair or deceptive acts or practices, it is my opinion that the U.S. fails to provide effective enforcement of privacy rights. This is true both with regard to effective and enforceable rights, and effective functioning of an independent supervisory authority. Based on the foregoing, the EU and the U.S. have many aspects to discuss before the U.S. can ensure an adequate level of protection that is "essentially equivalent" to the EU privacy protection. Although it is not reasonable that the EU should be able to dictate U.S. privacy policy, the principle of mutual recognition should apply in all situations where there is a discrepancy between two legal orders. Thus,

this thesis contends that the two privacy regimes must unite on a workable enforcement of EU citizens' right to privacy in order to guarantee an "essentially equivalent" level of protection.

6.3 The Safe Harbor 2.0

A Safe Harbor 2.0 must be based on the Commission's investigation concluding that the U.S. can ensure an adequate level of protection that is "essentially equivalent" to the EU privacy protection. Based on the conclusions made in Section 6.2, I contend that the U.S. privacy protection does not amount to a level that is "essentially equivalent" to the EU privacy protection. However, this fact should not result in a suspension of transatlantic transfers of personal data altogether. In the following, I will present consideration that, in my opinion, need to be addressed in a Safe Harbor 2.0 in light of the discrepancy between the privacy regimes, the *Schrems* ruling, and the proposed GDPR.

6.3.1 Actionable Privacy Rights

It is essential that the Safe Harbor 2.0 take into consideration the provisions set out in the proposed GDPR. The right to erasure is a fundamental right that most likely will not be compromised in the final version of the GDPR. Thus, the U.S. reluctance towards the right to be forgotten is an obstacle that has to be resolved in the EU-U.S. negotiations. EU citizens should be provided with minimum safeguards that reflect their right to erasure. This way, U.S. companies cannot circumvent and undermine EU privacy protection by making decisions based on U.S. privacy policies. As contended, with regard to the U.S. ability to provide a privacy protection that is "essentially equivalent", the Safe Harbor 2.0 needs to provide EU citizens with a workable enforcement of their right to privacy.

Transfers of personal data are key for transatlantic trade and given the discrepancy, it is obvious that compromises must be made. However, it should be a reasonable demand that EU citizens' fundamental right to privacy is not lost just because it crosses the Atlantic. Just as companies targeting U.S. citizens are expected to adhere to U.S. statutes, it is reasonable to demand that U.S. companies do the same. Most importantly, it is reasonable to demand that the U.S. government respects EU privacy law in this regard. Additionally, if the CISA becomes U.S. law, it should not be accepted that companies that comply with the program are effectively immune from all legal claims. In this regard, the EU must ensure actionable privacy rights for its citizens. Although the interception and destruction of terrrorism is an important and current issue, the U.S. should not be allowed

to undermine EU citizens fundamental right to privacy on a generalized basis. Even though the CJEU more or less rejected that the U.S. privacy protection amounted to an adequate level of protection, the EU is unlikely to be able to influence any U.S. legislation that has as its purpose to counteract terrorism. As the CJEU held in the *Schrems* case, any EU legislation protecting fundamental rights and freedoms must lay down clear and precise rules governing the scope and application of measures and impose minimum safeguards. This is necessary in order to provide EU citizens with sufficient guarantees for effective protection of their personal data against the risk and abuse and against any unlawful access and use for their data. This requirement has been met by the new article 43a of the GDPR. Nonetheless, a Safe Harbor 2.0 should also include a provision that addresses if and how U.S. courts may order a U.S. company to produce documents containing EU citizens personal data which are being stored abroad, i.e. in another jurisdiction. Needless to say, there may be situations where U.S. courts must be able to order access to personal data that U.S. companies store abroad when relevant to a specific case. However, it is unreasonable that U.S. courts extend its jurisdiction in a way that compromises EU citizens fundamental right to privacy. Hence, sufficient guarantees for effective protection are important when negotiating the Safe Harbor 2.0. A realistic Safe Harbor 2.0 provides EU citizens with efficient judicial remedies, i.e. actionable privacy rights, and should unconspicuously state the legal remedies EU citizens can pursue against both companies that unlawfully transfer personal data to the U.S. and U.S. governmental bodies that unlawfully access such data.

6.3.2 Self-Regulation and Workable Enforcement

EU privacy concerns show that self-regulation is an issue as U.S. companies can change and exercise their businesses in accordance with U.S. policies. In the *Schrems* case, the Court noted that self-certification in itself is not contrary to the requirement that a third country must ensure an adequate level of protection. However, the reliability of the U.S. system was questioned, as U.S. public authorities had no obligation to comply with the Safe Harbor. Just as the invalidated Safe Harbor, there is a risk that self-regulation cannot be properly enforced to ensure the right to privacy. In the end there is a risk that U.S. companies process EU citizens' personal data on the basis of U.S. legislation and policies. For example, article 17 of the GDPR provides an exception under which a data controller is not obligated to erase data subject to a takedown request. Consequently, a U.S. company has discretion to determine if the data can be retained in accordance with article 17.3 of the GDPR. Therefore, when determining whether or not such

obligation exists, there may be a risk that a U.S. company will make its decision based on U.S. policies and not EU law. Given that the U.S. legislator does not recognize a right to be forgotten it can be questioned whether a U.S. company will adhere to the broad EU privacy legislation. This leaves EU citizens' fundamental right to privacy in the hands of U.S. companies. Can Europeans reasonable expect or even demand that U.S. companies adhere to EU privacy law? As the U.S. privacy protection fundamentally differs from the EU view on privacy, it is also questionable whether a U.S. court will consider an alleged violation of privacy rights on the basis of the EU privacy protection when assessing the facts before the court. The *Microsoft* case further disputes U.S. courts willingness to adhere to the EU privacy standards. Additionally, the invalidated Safe Harbor decision did not only allow for companies to self-certify to the Principles, but also stated that in cases where U.S. law imposes a conflicting obligation, U.S. law precedes over the principles pursuant to the Safe Harbor. In the *Schrems* case, the Court considered this to result in that U.S. organizations, receiving personal data from the EU, were bound to disregard the Principles without limitation whenever the Principles were in conflict with U.S. law. Consequently, a Safe Harbor 2.0 must lay down clear and precise rules limiting the situations in which a U.S. company can disregard the principles of a Safe Harbor 2.0.

Furthermore, one issue is that the FTC only can initiate actions against companies in order to prohibit unfair or deceptive acts or practices. However, the EU's right to erasure is unconditional of an unfair or a deceptive act. The right of EU citizens can be exercised given that one of the grounds under article 17 of the GDPR applies to the specific situation. Hence, if a U.S. company provides its privacy policy in a transparent manner describing how personal data belonging to a user is processed and transferred, the FTC will not have jurisdiction to initiate any legal claims. In these situations, the individual's right to privacy cannot be properly enforced. That is why it is even more important that a Safe Harbor 2.0 provide EU citizens with actionable privacy rights. Earlier efforts to make the Safe Harbor truly safe have consisted of solutions for handling non-compliance among U.S. companies that misrepresented their compliance with the Safe Harbor. Additionally, the FTC has been criticized for not monitoring compliance efficiently. The risk of non-compliance and non-efficient monitoring will be difficult to completely eliminate. However, regardless the importance of the obstruction and interception of terrorism, the U.S. government or U.S. companies, EU citizens should at least have the possibility to initiate legal claims regarding their privacy rights.

6.4 Conclusion

The emergence of Big Data, the discrepancy between the EU and the U.S. privacy protection, the *Schrems* ruling, and the proposed GDPR have resulted in challenges for both legislators and companies with regard to transatlantic transfers of personal data. I contend in this thesis that the U.S. legal order does not amount to a protection that is "essentially equivalent" to the EU privacy protection. However, as the discprepancy cannot result in a suspension of transatlantic transfers of personal data, a reasonable compromise is that EU citizens should be provided with actionable privacy rights and a workable enforcement in a Safe Harbor 2.0. In my opinion, EU citizens' fundamental right to privacy is an offline right that, regardless whether or not the data cross borders, should also apply online. Lastly, when awaiting the final version of the Safe Harbor 2.0, it is important to have in mind that politics is just as much involved as law. The two privacy regimes clearly have different approaches to privacy protection and neither regime is likely to want its privacy protection dictated by another legislator.

Bibliography

Articles

Björn Johansson Heigis, *Integritet i fokus nr 3/2015*, Datainspektionens tidning

Claes Sandgren, *Är rättsdogmatiken dogmatisk?*, Tidsskrift for Rettsvitenskap 4-5/2005 pp. 648-656

Nils Jareskog, *Rättsdogmatik som vetenskap*, SvJT 2004 p. 1

Electronic Sources

Billy Ehrenberg, *How much is you personal data worth?*, The Guardian, 22 April 2014 08.17 a.m., http://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth (last accessed: 22 September 2015)

Boris Segalis, Kathryn Linsky, *Senate passes cybersecurity bill, bringing immunity for sharing cyberthreat data closer to reality*, 2 November 2015, Norton Rose Fulbright, Data Protection Blog, http://www.dataprotectionreport.com/2015/11/senate-passes-cybersecurity-bill-bringing-immunity-for-sharing-cyberthreat-data-closer-to-reality/ (last accessed: 9 December 2015)

Christopher Wolf, PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE 14-3 (Christopher Wolf ed., Practicing Law Institute 2007)

David Frydlinger – partner at Lindahl, *Frukostseminarium med Advokatfirman Lindahl om Safe Harbor-domen*, 23 October 2015, http://www.lindahl.se/se/om-oss/senaste-nytt/seminarier/2015/frukostseminarium-om-safe-harbor-domen/ (last accessed: 12 November 2015)

Der Hessiche Datenschutzbeaufragte, *Positionspapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)*, last updated: 26 October 2015, https://www.datenschutz.hessen.de/ft-europa.htm#entry4521 (last accessed: 24 November 2015)

Ewen Macaskill, Gabriel Dance, *NSA Files: Decoded – what the revelations mean for you*, The Guardian, 1 November 2013, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (last accessed: 24 November 2015)

Facebook, *Data Policy*, last revised: 30 January 2015, https://www.facebook.com/full_data_use_policy (last accessed: 22 September 2015)

Facebook, *How do we use this information?*, last revised: January 2015, https://www.facebook.com/about/privacy (last accessed: 9 November 2015)

Facebook, *How is this information shared?*, last revised: January 2015, https://www.facebook.com/about/privacy (last accessed: 9 November 2015)

Facebook, *How our global services operate?*, last revised: January 2015, https://www.facebook.com/about/privacy (last accessed: 9 November 2015)

Google, *Privacy Policy*, last revised 19 August 2015, http://static.googleusercontent.com/media/www.google.com/sv//intl/sv/policies/privacy/google_privacy_policy_sv.pdf (last accessed: 27 October 2015)

Jan Geer Ments, partner at DLA Piper, *German DPAs issue a Position Paper on Safe Harbor* (unofficial translation of ”Der Hessiche Datenschutzbeaufragte, *Positionspapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)*”, 25 October 2015, https://www.linkedin.com/pulse/german-dpas-issue-position-paper-safe-harbor-jan-geert-meents (last accessed: 24 November 2015)

Karlin Lillington, *Oracle keeps European data within its EU-based data centres*, 28 October 2015, The Irish Times, http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505, (last accessed: 12 November 2015)

Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, 12 November 2014, PewResearchCenter, http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (last accessed: 20 October 2015)

Nikolaj Nielsen, *EU-US data pact skewered in court hearing*, 25 March 2015, euobserver, https://euobserver.com/justice/128131 (last accessed: 20 October 2015)

Sam Pfeifle, *ECJ Hears Safe Harbor Arguments*, 24 March 2015, The Privacy Advisor, https://privacyassociation.org/news/a/ecj-hears-safe-harbor-arguments/ (last accessed: 20 October 2015)

Sandy Smolan, *The Human Face of Big Data*, 27 October 2014, available publically at: http://urplay.se/Produkter/190174-Big-data-sa-kartlaggs-hela-ditt-liv until 12 March 2016, thereafter (last accessed: 21 September 2015)’

The Data Inspection Board, *EU:s dataskyddsreform*, last updated March 2015, http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddsreform/ (last accessed: 30 December 2015)

The Data Inspection Board, *Kommissionens förslag till dataskyddsförordning (KOM (2012) 11 slutlig)*, dnr: 250-2012, 12 March 2012

Timothy Morey, Theodore "Theo" Forbath, and Allison Schoop, *Customer Data: Designing for Transparency and Trust,* May 2015, Harvard Business Review, https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust (last accessed: 24 September 2015)

U.S. Senator for North Carolina, Richard Burr, Debunking Myths about Cybersecurity Information Sharing Act, 20 October 2015, http://www.burr.senate.gov/press/releases/debunking-myths-about-cybersecurity-information-sharing-act- (last accessed: 23 December 2015)

World Economic Forum, *Personal Data: The Emergence of a New Asset Class*, January 2011, http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf, (last accessed: 21 September 2015)

European Community Legislation, Notices, Decisions and Reports

Article 29 Data Protection Working Party, *Adoption of guidelines on the implementation of the CJEU's judgment on the "right to be forgotten"*, 26 November 2014, Press Release, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20141126_wp29_press_release_ecj_de-listing.pdf (last accessed: 6 October 2015)

Article 29 Data Protection Working Party, *The Court of Justice of the European Union invalidates the EU Commission Safe Harbor Decision*, Press release, 6 October 2015, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151006_wp29_press_release_on_safe_harbor.pdf (last accessed: 28 October 2015)

Council of the European Union, 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) [first reading] - Analysis of the final compromise text with a view to agreement, 15 December 2015, 2012/0011 (COD)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing

of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050, 24 October 1995

European Commission, 2000/520/EC: COMMISSION DECISION of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, (notified under document number C(2000) 2441), OJ L 215, 25 August 2000

European Commission, COMMISSION DECISION of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 2010/87/EU

European Commission, *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*, 25 January 2012, Press Release Database, IP/12/46

European Commission, COMMISSION STAFF WORKING DOCUMENT, *The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*, SEC (2004) 1323, Brussels, 20 October 2004

European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final, 27 November 2013

European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL – *Rebuilding Trust in EU-US Data Flows*, COM(2013) 846 final, 27 November 2013

European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, *A Digital Single Market Strategy for Europé*, 6 May 2015, COM(2015) 192 final

European Commission, *Data Protection Eurobarometer out today*, 24 June 2015, http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm (last accessed: 14 September 2015)

European Commission, *Questions and Answers – Data protection reform*, 21 December 2015, http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm?locale=en (last accessed: 22 December 2015)

European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS 5; 213 UNTS 221

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

Meglena Kuneva, European Consumer Commissioner, *Roundtable on Online Data Collection, Targeting and Profiling*, Brussels 31 March 2009, http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm (last accessed: 20 October 2015)

Prof. Francesca Bignami, *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens*, Policy Department of the European Parliament, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU(2015)519215_EN.pdf (last accessed: 5 January 2015)

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306, 17.12.2007, p. 1–271

Viviane Reding, *A Data Protection Compact for Europe*, 28 January 2014, http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm (last accessed: 21 September 2015)

Interviews

Interview with Karl-Hugo Engdahl, Legal Counsel at Klarna AB, 27 May 2015

Interview with Karl-Hugo Engdahl, Legal Counsel at Klarna AB, 4 December 2015

Law Review Articles

Daniel R. Leathers, Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement, 41 Case W. Res. J. Int'l L. (2009)

Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 Hous. L. Rev. 717 2001-2002

MacKay Cunningham, *Diminishing Sovereignty: How European Privacy Law Became International Norm*, 11 Santa Clara J. Int'l L. 421 (2012-2013)

Michael L. Rustad, Sanna Kulevska, *Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow,* Harvard Journal of Law & Technology, Volume 28, Number 2 (2015)

Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. Rev. 1149 2004-2005

Robert G. Larson III, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech*, 18 COMMUNICATION LAW AND POLICY 91 (2013)

Literature

Brian Craig, *Cyberlaw – The Law of the Internet and Information Technology*, Pearson Education (2013)

Michael L. Rustad, *Global Internet Law,* West Academic Publishing (2014)

Swedish Legislation

The Freedom of the Press Act (sv. Tryckfrihetsförordningen) (SFS 1949:105)

U.S. Legislation, Official Documents, and Guidelines

congress.gov, *S.754 – Cybersecurity Information Sharing Act of 2015*, https://www.congress.gov/bill/114th-congress/senate-bill/754/text (last accessed: 9 December 2015)

Department of Justice, *The USA PATRIOT Act: Preserving Life and Liberty*, http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf (last accessed: 16 November 2015)

Donald T. Kramer, 2 Leg. Rts. Child. Rev. 2D § 23:18 (2d ed.) available in Westlaw Secondary Sources

export.gov, *Privacy "Seal" Programs* and *Alternative Dispute Resolution*, http://www.export.gov/safeharbor/eg_main_018241.asp (last accessed: 10 October 2015)

Federal Trade Commission, *In the Matter of Snapchat, Inc., a corporation*, docket no. 132 3078, https://www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf (last accessed: 27 November 2015)

Federal Trade Commission, *In the Matter of Snapchat, Inc., a corporation – Agreement Containing Consent Order*, file no. 132 3078, https://www.ftc.gov/system/files/documents/cases/140508snapchatorder.pdf (last accessed: 27 November 2015)

Federal Trade Commission, *Privacy & Data Security Update* (2014), http://www.ftc.gov/reports/privacy-data-security-update-2014, (last accessed: 4 October 2015)

Federal Trade Commission, *Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework*, 12 November 2013, http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf (last accessed: 4 October 2015)

Robert S. LaRussa, *Cover Letter from Acting Under Secretary for International Trade Administration*, 21 July 2000, http://export.gov/safeharbor/eu/eg_main_018494.asp, (last accessed: 16 October 2015)

SB-568 Privacy: Internet: minors.(2013-2014) An act to add Chapter 22.1 (commencing with Section 22580) to Division 8 of the Business and Professions Code, relating to the Internet, [Approved by Governor September 23, 2013. Filed with Secretary of State, 23 September 2013.], http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568 (last accessed: 23 December 2015)

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

The Children's Online Privacy Protection Act of 1998, 15 U.S.C.A. § 6501 Pub.L. 105-277, 112 Stat. (1998)

The Gramm-Leach-Bliley Act (GLB Act or GLBA), also known as the Financial Modernization Act of 1999 is codified at 15 U.S.C. §6801

The Health Information Technology ("HITECH") Provisions of American Recovery and Reinvestment Act of 2009, Title XIII, Subtitle D (Pub. L. 111-5, 123 Stat. 115, codified in relevant part at 42 U.S.C. §§ 17937 and 17954

The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. (1996)

The Privacy Act of 1974, 5 U.S.C. § 552a

U.S. Department of Commerce, *Safe Harbor Privacy Principles*, 21 July 2000, http://www.export.gov/safeharbor/eu/eg_main_018475.asp, (last accessed: 4 October 2015)

White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), http:// www.whitehouse.gov/sites/default/files/privacy-final.pdf. (last accessed: 10 October 2015)

Table of Cases

American Case Law

Bartnicki v. Vopper, 532 U.S. 514, 121 S. Ct. 1753

In Interest of John W., 300 Pa.Super. 293, 298, 446 A.2d 621

In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation, 15 F.Supp.3d 466 (S.D.N.Y. 2014)

EU Case Law

Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, 13 May 2014, ECLI:EU:C:2014:317

Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650

European Court of Human Rights

Case of Pretty v. The United Kingdom, no. 2346/02, 29 April 2002