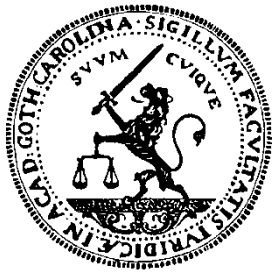

FACULTY OF LAW
Lund University

Dena Dervanović

Safe Harbor No More: Impact of the Schrems Case on EU – U.S. Personal Data Transfers

JAMM05 Master Thesis

International Human Rights Law and Intellectual Property Law
30 higher education credits

Supervisor: Ulf Maunsbach
Term: Spring 2016

To my grandparents,
whose infinite love and wisdom guide me in everything I do.

Contents

Summary

This thesis in whole is essentially envisaged to display the evolutionary process of the protection of the right to data protection, with a focus on cross-border data transfers, specifically between the EU and the U.S. post-*Schrems* case. The *Schrems* case marks a pivotal moment in the definition of the notion of privacy and data protection in many ways, among which the downfall of Safe Harbor is the most notable one. Finally, the thesis aims to provide a concise overview of the EU – U.S. Privacy Shield. All of this is looked at through the fundamental rights lens of the EU Charter.

Are data protection and privacy one and the same? How does the right to data protection balance against other fundamental rights, such as the freedom to conduct business? What was the impact of the *Schrems* case – aside from striking down Safe Harbor? In relation to that, is the EU – U.S. Privacy Shield a viable solution that provides adequate protection?

Divulging the distinction between data protection and privacy is important due to the fact that the two concepts are often treated as one concept, inseparable from one another, both in practice and in academia. Furthermore, the thesis examines the balance between the right to data protection and the freedom to conduct business since the two are in an interesting relationship, as observed from case law. Furthermore, the thesis focuses on the analysis of Safe Harbor, the *Schrems* case that had it struck down and the upcoming EU – U.S. Privacy Shield. It dissects the Privacy Shield and the European Commission's draft adequacy decision in order to see whether they do indeed fix the aforementioned flaws. This thesis juxtaposes the Privacy Shield with Safe Harbor and with the criteria set out by CJEU in the *Schrems* case. As a result of the juxtaposition and analysis, the thesis identifies the strengths and weaknesses of the Privacy Shield, along with finding that the architecture of the Privacy Shield could be ameliorated.

Sammanfattning

Denna uppsats är i sin helhet tänkt att visa den evolutionära processen för skyddet av personuppgifter, med fokus på överföring av personuppgifter från EU-medlemsstaterna till tredjeländer, och då särskillt mellan EU och USA efter *Schrems*-fallet. *Schrems*-fallet markerar en vändpunkt i definitionen av rätten till privatliv på många sätt, där ogiltigförklaringen av Safe Harbor är den mest anmärkningsvärda. Till sist syftar uppsatsen till att ge en kortfattad översikt av EU – U.S. Privacy Shield. Allt detta ses genom linsen av Europeiska Unionens stadga om de grundläggande rättigheterna.

Är dataskydd och privatliv samma sak? Hur balanseras rätten till skydd av personuppgifter mot andra grundläggande rättigheter, såsom näringsfrihet? Vad var effekten av *Schrems*-fallet - bortsett från att ogiltigförklara Safe Harbor? I förhållande till detta, är EU - US Privacy Shield en hållbar lösning som kan säkerställa en adekvat skyddsnivå?

Att klargöra skillnaden mellan begreppen dataskydd och privatlivS är viktigt på grund av det faktum att de ofta behandlas som ett och samma koncept, oskiljaktiga från varandra, både i praktiken och i den akademiska världen. Dessutom undersöker uppsatsen balansen mellan rätten till dataskydd och näringsfrihet då de har ett intressant förhållande till varandra, vilket framgår av rättspraxis. Vidare fokuserar uppsatsen på att analysera Safe Harbor, på *Schrems*-fallet som ogiltigförklarade Safe Harbor och på den kommande EU – U.S. Privacy Shield. Den dissekerar Privacy Shield och Europeiska kommissionens Draft Adequacy Decision för att se om de verkligen löser de förutnämnda bristerna. Uppsatsen placerar Privacy Shield sida vid sida med Safe Harbor och med de kriterier som fastställts av EU-domstolen i *Schrems*-fallet. Som ett resultat av analysen och jämförelsen identifierar uppsatsen styrkor och svagheter med Privacy Shield, samtidigt som den finner att dess struktur kan förbättras.

Preface

Transatlantic data transfers are essential to the EU – U.S. partnership. In the previous year, the discussion on transatlantic data transfers and data protection has reached a heightened level, with the *Schrems* case highlighting the fundamental rights aspect. Seeing as the topic is very timely, it is perhaps not very strange that I have taken it up as my thesis project. Driven by my boundless curiosity, taking on a topic that has caused such a stir in the legal community both on the old continent and across the pond was a challenge I felt ready to tackle. However, this did not come out of the blue: my tendency to research data protection had started almost two years before this thesis was written, which one might call a momentum well gained, with this thesis as a crown jewel of my unquenchable thirst for knowledge of the area.

This Master thesis has been produced during the LL.M. education at Lund University made possible by a study scholarship given by the Swedish Institute. In addition to that, this thesis was created under the sharp eye of Ulf Maunsbach, who saw that I had control over my thesis long before I saw it and whose encouragement and guidance made this thesis better. I would also like to thank Erika Wiking Häger of *Mannheimer Swartling* for taking the time out of her busy schedule to hear my thoughts on the EU – U.S. Privacy Shield and discuss it with me. I would like to thank my family and close friends who stoically stood by me throughout law school and its challenges. I am indebted to you all, especially to you Mom.

Last but not least, if this thesis journey has taught me anything, it is that *preface* is pronounced *preface.*

Abbreviations

BCRs	Binding Corporate Rules
CJEU	Court of Justice of the European Union
DoC	Department of Commerce (U.S.)
DoJ	Department of Justice
DPC	Data Protection Commissioner
DPD	Data Protection Directive
EDPS	European Data Protection Supervisor
EU Charter	EU Charter of Fundamental Rights
ECJ	European Court of Justice
EC Treaty	Treaty establishing the European Community
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
GDPR	European General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
NSA	U.S. National Security Agency
ODNI	Office of the Director for National Intelligence
PPD-28	Presidential Policy Directive 28
PRISM	Planning Tool for Resource Integration, Synchronisation and Management
SCCs	Standard Contractual Clauses
SHD	Safe Harbor Decision (Decision 2000/520/EC)
TFEU	Treaty of the Functioning of the European Union
The Court	Court of Justice of the European Union
The Shield	EU – U.S. Privacy Shield
UDHR	Universal Declaration of Human Rights
WP29	Working Party 29

Glossarium

Data subject: an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[1]

Data controller: the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.[2]

Data processor: a natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller.[3]

[1] *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,* Article 2(a)
[2] *Ibid*, Art 2(d)
[3] *Ibid*, Art 2(e)

1 Introduction

1.1 Background

Data privacy and data transfers have been an increasingly hot topic that the European and worldwide community has had to deal with from a protective, legislative perspective. In today's world, it has become inevitable for a business to conduct its activities online. In fact, for the most part it has become unnecessary to conduct a business *any other way* than online. This is rooted in a number of factors, among which lower operation costs and the expanding market are but a few.[4] Human life has gone online as a result of the technological revolution. Our music is streamed, the information flow is constant and we are given an opportunity not only to keep in touch with long lost acquaintances, do our groceries and pay our bills with just a couple of clicks but to create business opportunities as well. Social media allow over 900 million users to connect with people from all over the world, and an estimate of 360 million people take part in cross-border e-commerce.[5] All this produces an abundance of data that flows over the geographically unconcerned Internet, which, in turn, could produce various data safety risks.[6]

The digital way forward is deservedly celebrated worldwide. However, in the relay race where an abundance of startups and the ever-increasing number of multi-national corporations run to thrive on a global level thus bringing about change and developments in all aspects of human life, one indispensable member of the team is losing breath trying to catch up. The

[4] *Digital Globalization: the new era of global flows*, McKinsey & Company, (McKinsey Global Institute 2016), p.8 available at http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows [accessed 4 May 2016]

[5] *Digital Globalization: the new era of global flows*, McKinsey & Company, (McKinsey Global Institute 2016), p.8

[6] See also Viviane Reding, *The upcoming data protection reform for the European Union*, International Data Privacy Law, Vol. 1, No. 1 (Oxford University Journals 2011) p.3

underperforming member is law, carrying its [data] protection mechanisms as baton. In order not to completely undermine the underperforming member of the team, it is worth noting that law, as such, has not been sitting idly during the technological revolution.[7] It has just struggled to keep up with the pace and, as a result, it has recently been focusing a lot of efforts to catch up. This thesis shows how law has been doing that in the light of the recent events related to privacy and data protection, all the while trying to detangle the two concepts from one another. This is done through the prism [sic!] of the *Schrems* case that triggered a change in the way cross-border data transfers function. In defence of the law, the challenges we are faced with right now are not exactly simple to solve.

The thesis envisages its reader to be an LL.M. with vast knowledge in International Human Rights Law but with little to no prior knowledge in Data Protection Law. In this thesis, the reader is immersed into the issue of cross-border data transfers and the issue of "adequate" levels of protection of said data. If one places the geographically unconcerned Internet alongside cross-border data protection regulations, obvious, albeit convoluted questions taunt: How does one regulate cross-border issues of one world in a borderless Internet world? Furthermore, why is it that we need to regulate these issues at all? The world is becoming increasingly connected, and in such a world with data flows soaring over short periods of time compared to trade and finance flows on a global scale, it is inevitable that the mechanisms of regulation and protection should follow suit, in order to cover a wide range of interests at stake.[8]

The freedom to be oneself, the freedom to control one's own personal data has long been at the core of heated discussions in the modern age. Privacy, as a fundamental right, captures one of the most instinctive cravings of an

[7] See Ulf Maunsbach, 'Here Comes The Internet, And Why It Matters: Private International Law in Transition' Patrik Lindskoug, Ulf Maunsbach, Göran Millqvist, Per Samuelsson, Hans-Heinrich Vogel (eds.), *Essays in honor of Michael Bogdan* (Juristförlaget i Lund 2013), p.304

[8] *Digital Globalization: the new era of global flows*, McKinsey & Company, McKinsey Global Institute (2016), p.10

individual. What is interesting to discuss, however, is the distinction between privacy and data protection as two separate fundamental rights. This thesis enters into the specificities of this conundrum as a basic point of departure before going into cross-border data transfers. There is also mention of the theoretical and philosophical significance privacy has had on academia, for the purpose of acquainting the reader with the magnitude with which privacy has always impacted both academics and practitioners. Further on, the thesis narrows the focus down to the conundrum surrounding the aforementioned distinction, giving examples of its confounding use in both practice and academia. In order to portray the evolutionary process of data protection mechanisms in Europe, an overview of the relevant legal framework is displayed. The approach here is chronological, for the purpose of acquainting the reader with the development of privacy and data protection as fundamental rights. As the thesis goes further, the scope gets specific with the legal framework that the thesis tackles: namely, the Data Protection Directive and the Charter of Fundamental Rights of the European Union and with a brief overview of the General Data Protection Regulation.

This thesis also tries to discuss and analyze aspects of data transfers, particularly from the standpoint of the rights to privacy and data protection and the freedom to conduct business as contained in the Charter on Fundamental Rights of the European Union. This is done through the analysis of the freedom in and of itself, and continued through illustrating how this particular fundamental freedom balances against other fundamental rights and freedoms. This is done through specifically chosen case law. This is followed by focusing on a perspective of balancing the right to data protection with the freedom to conduct business. Both data protection and the freedom to conduct business can be perceived as limiting to one another, and this thesis uses the Court of Justice of the European Union (CJEU) jurisprudence to illustrate their inter-relationship in a balancing act.

Furthermore, the thesis analyses Safe Harbor, a framework that is now defunct. The invalidation of the framework echoed enormously since it

brought along serious repercussions on the safety of the personal data being transferred on the one hand, and the commercial aspects it impacted on the other. In its decision to strike Safe Harbor down, the CJEU emphasized the blurred lines in the way personal data of EU citizens was being treated when transferred across to the United States, from both a [U.S.] national security standpoint and from the corporate side of things.[9] The analysis in this thesis provides with an overview of the criticism directed at Safe Harbor, largely due to its self-certification and self-regulation properties, while also discussing the consequences of its invalidation.

In order to put everything into perspective, the thesis deals with a thorough case study. Namely, the most recent case of *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14) in front of the CJEU is analysed for the purpose of illustrating the malfunctions of Safe Harbor on the one hand, and the ever-growing importance of privacy protection in the Internet era on the other hand. The judgment in this case was delivered on 6 October 2015, striking down the Safe Harbor framework. What this case displayed was the necessity for a higher standard that should apply to the processing of the personal data [of EU data subjects] in the U.S. The invalidation of the Safe Harbor framework has had a profound impact on international data transfers, protection of privacy and the freedom to conduct business.

The idea of the thesis is to provide with a concise overview of the evolutionary process of the protection of the right to data protection in the European Union itself and in the Union's relation to the United States. As such, the thesis does not fail to take into account the EU – U.S. Privacy Shield and provide a concise overview of it. Lastly, an analysis and conclusion of the whole subject matter will ensue in the final part of the thesis, pointing out the most important findings from this thesis with respect to the research questions posed at the beginning.

[9] Henry Farrell and Abraham Newman, *The Transatlantic Data War, Europe Fights Back Against the USA*, (Foreign Affairs, 2016) https://www.foreignaffairs.com/articles/united-states/2015-12-14/transatlantic-data-war [accessed 16 May 2016]

1.2 Objective

The aim and purpose of the thesis is to illustrate and analyze the current data protection mechanisms in the specific light of the recently abolished Safe Harbor framework. The reason behind this choice lies in the fact that fundamental rights and freedoms, such as the right to data protection and the freedom to conduct business are affected by this. Moreover, the topic is timely and highly important for the effective protection of the aforementioned rights and freedoms, as envisaged by the EU Charter of Fundamental Rights.

1.3 Research questions

At its core, this thesis attempts to analyse and answer a set of questions. To start with, it is necessary to tackle the question of whether data protection and privacy are one and the same. This is an important question to address before entering the discussion on cross-border data transfers and their impact on fundamental rights. The answer to this question serves as a basis for the whole thesis.

Further on, the following question is how does the right to data protection balance against other fundamental rights such as the freedom to conduct business? This question is of importance since the balancing exercise between different fundamental rights is a conundrum that is not easy to solve, as has been shown in practice as well, but it is an important aspect to consider. Furthermore, the thesis looks at the impact of the *Schrems* case – aside from striking down the flawed Safe Harbor Framework, what other effect did it have? In relation to that, is the EU – U.S. Privacy Shield a viable solution that provides adequate protection?

The reasons behind these research questions lie in the timeliness of the issue at hand – it being unresolved at the moment of writing this thesis on the one hand, and it being extremely important for the adequate safeguarding of the right and freedom addressed in the research questions, on the other hand. It

is submitted that this kind of discussions ought to be brought into the limelight and discussed as the pressing matters they truly are. This stems from the fact that data flow, in all its vastness, is inevitable. Thus, proper protection mechanisms are of vital importance in this context.

1.4 Methodology and material

In order to answer the posed research questions, a classic legal dogmatic method is used to analyse the relevant legal framework. The normative part of the thesis is based on legal instruments used in the research and analysis whereas the empirical part is largely based on the study of the case *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14) in front of the CJEU. Throughout the thesis, a historical, chronological approach is used to effectively illustrate the ever-changing dynamics of privacy and data protection as rights in the evolving data-dominated online landscape.

A comparison between legal frameworks is done for the purpose of illustrating the aforementioned evolutionary aspect, however, it is also important to look at court practice in conjunction with the legal framework. A critical perspective dominates the thesis and the rights and freedoms examined in it will be looked at through the lens of the *Schrems* case and the balance of interests at stake. The *Schrems* case holds a vital role in the discussion on cross-border data transfers and protection. This case, brought to the CJEU by an Austrian law student Maximillian Schrems, tackled the questions of the role of Data Protection Authorities as well as the issue of the adequate level of protection afforded to personal data when transferred to third countries. In addition to that, the *Schrems* case inadvertently brought down Safe Harbor and accelerated the process of putting a better mechanism in place, which is what the Privacy Shield is intended to embody.

This thesis uses a range of different materials carefully selected for the purpose of answering the posed research questions in an adequate manner. A selection of textbooks is used mainly for laying the foundation of the

thesis, while a variety of academic journals, such as *inter alia* the Oxford University Data Protection Journal, are used to address the respective novel developments and aspects of the issues tackled in the thesis.

Seeing as the thesis deals with EU law, a variety of EU legal instruments and documents are used throughout, forming the legal framework of the thesis. In addition to that, the thesis tackles jurisprudence of the CJEU as its empirical axis. Due to the novelty of the core issue of the thesis, the thesis extends its use of materials to relevant data protection law blogs such as *inter alia* the Hunton & Williams Privacy and Information Security Law Blog. In connection to that, a limited amount of materials are relevant news outlets included in the thesis for a supporting, illustrative role. Lastly, an analysis by the law firm Hogan Lovells is used as one of the means for deconstructing the Privacy Shield along with the opinion of Working Party 29.

1.5 Delimitations

This thesis does not analyze the philosophical and theoretical definitions of privacy, but it does deal with the legal definitions of privacy and the international and relevant regional legal framework(s)**.**[10] The reason for not focusing on the philosophical and theoretical definitions is grounded in the fact that it is not utterly necessary for the proper understanding of the topic at hand.

Moreover, the relevant regional framework in question is European; in particular the regime under the EU Charter of Fundamental Rights, while the European Convention on Human Rights is mentioned in passing.

When it comes to the EU framework, it is admittedly a large corpus of instruments, which is why the thesis focuses on a selection of instruments relevant for providing proper answers to the posed research questions.

[10] **N.B.** The general international framework will not be dealt with in detail.

Namely, the thesis goes into detail when it comes to the Data Protection Directive and the Charter of Fundamental Rights of the European Union. This is done for the purpose of retaining focus to the specific scope of the thesis. The thesis does not deal with big data and the Internet of Things. Since the thesis analyses the rise and fall of the Safe Harbor framework, it does not go into an in-depth analysis of the protection measures used after the striking down of Safe Harbor and before the EU – U.S. Privacy Shield entering into force, but it properly addresses the basic idea of them.

As the thesis mainly places focus on the data protection mechanisms in the European Union, it does not go into depth of the U.S. legal system and its mechanisms. However, the thesis mentions the U.S. Judicial Redress Act and briefly describes its purpose and role, but does not go into a detailed analysis of the instrument. The reason behind this is that it is indeed valuable information for the reader to know of the changes in the U.S. domestic law prior to the EU – U.S. Privacy Shield, but its in-depth analysis falls out of the scope of this thesis.

With awareness of a labyrinth-like existence of data protection instruments, it is a conscious decision not to include all instruments that could be tied to this topic in one way or another, simply due to the desire to stay focused and keep this thesis as concise and clear as possible in its aim of getting the main point across. As part of this decision for delimitation, it is necessary that the reader is aware of the fact that save for the EU – U.S. Privacy Shield, the thesis does not go into detail of any other future/proposed framework that tackle important data protection issues not directly relevant to the topic of cross-border data transfers.

This includes but is not limited to the General Data Protection Regulation (GDPR) that is mentioned in the thesis, albeit briefly, focusing only on the information relevant to cross-border data transfers and the overall idea of the Regulation. The reasoning behind this is essentially simple: the General Data Protection Regulation is a comprehensive legislation package that

could undoubtedly be analyzed in a way that it could become another thesis, or a set of different theses, hence the scope of this thesis would go off-track with a complete in-depth analysis of the GDPR. It is important that the reader is aware of the fact that this topic has been developing at the same time as the time of writing; hence, tracking developments has been stopped on 25 April 2016.

1.6 Status of research

The topic this thesis deals with is generally a novelty in the legal world; hence the status of research pertaining to the Privacy Shield is highly limited seeing as the Privacy Shield became available to the public in March 2016. As for the Safe Harbor research status, seeing as it is an older instrument, there has been a substantial amount of research done on its characteristics; however, the research mostly deals with its importance for the transatlantic partnership and criticism of its content. The thesis places a case study as its axis: namely, the *Schrems* case in front of the CJEU. The case is fairly new as well, with the judgment dating from October 2015. However, a solid amount of research has been done in the way of analyzing the case and its outcomes for the *status quo* of transatlantic data transfers.

Lastly, this thesis tackles fundamental rights and freedoms as envisaged in the Charter of Fundamental Rights of the European Union, a subject matter fairly well addressed in academia and the jurisprudence of the Court of Justice of the European Union, which will be reflected throughout the thesis.

1.7 Structure

Chapter 2: Privacy v. Data Protection thoroughly discusses the importance of the distinction between the terms ‘privacy’ and ‘data protection’ *in abstracto* – why is it important to distinguish the two and what were their origins in legal history. Furthermore, the thesis continues by focusing on the way privacy and data protection have been dealt with in the European

Union. The chapter concludes with a focus on on cross-border data transfers and its specificities.

In *Chapter 3: Freedom to conduct business – how does it fare against other fundamental rights?* the thesis takes a turn to the freedom to conduct business as delineated in the Charter of Fundamental Rights of the European Union.

Following that, *Chapter 4: Safe Harbor, not so safe* unfolds a discussion on the Safe Harbor framework, pointing out its advantages and drawbacks, as well as the idea behind it.

Consequently, in *Chapter 5: Maximillian Schrems v. Data Protection Commissioner*, the *Schrems* case is put under the microscope, with a detailed analysis of the proceedings and the Court's findings.

The analysis of the *Schrems* case can be viewed as preparatory reading for *Chapter 6: What now? The EU – U.S. Privacy Shield.* This chapter deals with the analysis of the EU – U.S. Privacy Shield that is expected to enter into effect in June 2016. The Privacy Shield analysis serves to give an overview of its specificities, often comparing it with Safe Harbor, for a better overview of what has been done for the aim of improving a framework like that.

2 Privacy v. data protection: a distinction

2.1 Introduction: in abstracto

The matter of whether privacy and data protection are one and the same is arguably a confounding topic to discuss, given that there is no clear-cut consistency over the matter, neither in academia nor in practice. However, that does not make it any less important of a topic. From the perspective of the topic of this thesis, it seems quite important to make a distinction between the two. This is done by going through the notion of privacy first, since it chronologically came prior to data protection, and then the discussion goes into data protection more specifically.

Ever since the famous Warren and Brandeis article[11] was published in 1890, privacy has been a topic that academics, theorists and philosophers discussed thoroughly, all in the attempt of comprehending its scope and meaning. And indeed, privacy is, and has long been considered an elusive concept, subject to very individual interpretation and, overall, a very difficult concept to encapsulate in a legal definition. Privacy, in its ambiguity, has tormented theorists and philosophers as well. Namely, in the context of philosophy and theory, there has been a number of definitions[12] such as, *exempli gratia*, the "control of information about oneself"[13] or "the right to be left alone."[14] The scope of this thesis does not allow for further elaboration on these concepts, however, it is important that the reader is made aware of the nature of privacy – its ambiguity and complexity are not new issues, neither are they an Internet-caused novelty. Most notably,

[11] Samuel Warren, Louis Brandeis, *The right to privacy* (4 Harvard Law Review 193, 1890)
[12] Mathias Klang, Andrew Murray (ed.), *Human Rights in the Digital Age*, Glasshouse Press, Cavendish Publishing (2005), p. 148
[13] Alan F. Westin, *Privacy and Freedom*, (Bodley Head 1967), p.25, **quot.in.** Mathias Klang, Andrew Murray (ed.), *Human Rights in the Digital Age*, (Glasshouse Press, Cavendish Publishing 2005), p. 149
[14] Samuel Warren, Louis Brandeis, *The right to privacy* (4 Harvard Law Review 193, 1890), **quot.in.** Mathias Klang, Andrew Murray (ed.), *Human Rights in the Digital Age*, (Glasshouse Press, Cavendish Publishing 2005), p. 148

privacy is not just a theoretical, philosophical or academic issue.[15] Privacy (or the lack of it) has gained momentum as one of the fundamentals, surpassing academic discourse and immersing itself into the very centre of modern existence in an Internet-dominated world. The concepts mentioned *supra* make for important elements of privacy in its legal definition as well. Namely, it has been argued that privacy has four elements, or *"categories:"*[16]

1. "Freedom of personal autonomy;
2. The right to control personal information;
3. The right to control property;
4. The right to control and protect physical space;"[17]

These are not stand-alone and are connected in more ways than one. However, they make up for a broad delineation of what privacy, as such, is consisted of. The bottom line with privacy is that it is inextricably linked to the individual's freedom and identity.[18] Privacy was probably the reason people started building walls in the first place.[19]

On the other hand, data collection is not a new concept either – it has always been there, but it is now made easy with the Internet.[20] Changing the way all data (not just personal) is stored and accessed, from physical archives that were fairly safe from mass misuse, to a system of online archiving that brings about a series of different risks, naturally requires a different modus of protection in the legal sense. However, it is utterly important to truly understand this when discussing the topic of privacy online and data transfers in general. This very notion of the Internet having a "*panta rhei* character"[21] makes up for one of the biggest elements of difficulty for the legislators to simply keep up. The nature of Internet is one that tests the

[15] Jon L. Mills, *Privacy, The Lost Right,* (Oxford University Press 2008), p.9
[16] *Ibid,* p.13
[17] *Ibid*
[18] *Ibid*
[19] Diane Rowland, Uta Kohl and Andrew Charlesworth, *Information Technology Law, fourth edition,* (Routledge 2012), p.150
[20] *Ibid,* p.146
[21] Peter Blume, *It's Time For Tomorrow: EU Data Protection Reform And The Internet,* Journal of Internet Law, (Aspen Publishers Inc., February 2015), p.6

limits and powers of legislation.[22] There is hardly any point in debating on how much the Internet has and keeps affecting the contemporary lifestyle – the mere notion of the debate renders it redundant. Undoubtedly, a wide range of opinions could be thrown in the mix on whether these changes have impacted our lives positively or negatively, but that would be beside the point. The point is that these changes have been, and still are, thrown at us at the speed of light, whereas our adaptation to them has been a meek attempt at achieving the speed of sound, simply put. The issue in and of itself lies in the adequate and effective protection mechanisms, or the lack thereof. These mechanisms are beyond necessary in order to effectively protect the fundamental rights of Internet users. It is essential to have the mechanisms in place to cope with situations that can arise from the ubiquitous Internet usage. Seeing as most of these situations are not, at least explicitly, covered by relevant legislation, it is easy to see that there could be many challenges for courts to deal with them in a manner that will protect the fundamental rights.

Data has become ubiquitous and a whole industry depends on it and, in many ways it has become a currency, a commodity.[23] Every Internet-using individual leaves countless "digital traces" online on a daily basis.[24] This accumulation of data is overwhelming and impressive but one cannot help but think it has an *Orwellesque* feel to it. Initially, the right to privacy was envisaged as a human right that pertained to no economic context whatsoever.[25] However, when we talk about privacy, there are always two sides of the coin at stake – two sets of interests to balance: the right to privacy of the individual on the one hand, and the rights and interests of commercial actors on the other. This balance is of utmost importance for the contemporary society for the simple reason that privacy, as a concept, is evolving and changing shape.

---

[22] *Ibid*, p.10
[23] Diane Rowland, Uta Kohl and Andrew Charlesworth, *Information Technology Law, fourth edition*, (Routledge 2012), p.146-149
[24] Ibid, p.148
[25] Lilian Edwards, Charlotte Waelde, *Law and the Internet, third edition*, (Hart Publishing 2009), p. 446

This is by no means a new question, but one that has been asked many a times. The constant changing element of the said conundrum is related to the most recent societal developments that largely influence the question and the answer(s) to it.

2.2 So are privacy and data protection one and the same?

Based on what has been dissected about both of these separate notions *supra*, it could be helpful to examine the two terms in their juxtaposition. This is done for the aim of clarifying if the two belong to the same concept, do they overlap or if they are, in fact, separate from one another. It can be noted that many view the scope of the right to privacy viewed as encompassing the processing of personal data. This was noted in the *Bavarian Lager* case where ECJ stated that data protection refers to lawful processing of personal data, and makes a distinction between data protection and privacy by viewing privacy as *"protection of an individual's personal space."*[26] Processing of personal data can constitute an interference with the right as such, but seeing as the right to privacy is not absolute, there are ways to execute processing without constituting an interference with the right to privacy.[27] The predominant opinion on the correlation between privacy and data protection used to be one that says that data protection is merely a digital aspect of the right to privacy, making them inextricably linked concepts, according to some legal scholars.[28] However, the approach has undergone a mild transformation over the years, pointing to a shift in

[26] T-194/04 Bavarian Lager v. Commission (2007) ECR-II 04523, para.118, (C-28/08 P Bavarian Lager (2010) ECR I-06055) **quot.in.** Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, (Oxford University Press 2013), p.19

[27] Jan Trzaskowski, Andrej Savin, Björn Lundqvist, Patrik Lindskoug, *Introduction to EU Internet Law*, (Ex Tuto Publishing 2015), p.69

[28] Karim Benyekhlef, *Les normes internationales de protection des données personnelles et l'autoroute de l'information*, in Les Journées Maximilien-Caron, Le respect de la vie privée dans l'entreprise, (Éd. Thémis 1996), p.91, **quot.in.** Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Rights of the EU*, Law, Governance and Technology Series 16, (Springer International Publishing 2014), p.214

opinion that indicates that they might as well be two stand-alone concepts, but still so very closely-knit with one another to an extent that they are in an overlap.[29] This "overlap"[30] functions in the manner that, in some ways, data protection[31] is encompassed in the wide notion of privacy on the one hand. This is strongly linked to privacy being an evolving concept, changing with the times and technological developments. In this evolution, privacy and data protection have undergone a sort of *mitosis*, becoming two separate cells. If one were to pinpoint this exact moment in time, it would probably be the creation of the Charter of Fundamental Rights of the European Union.[32]

So how is it that these two separated then? In what way? If privacy, as envisaged by Warren and Brandeis, were "the right to be left alone"[33], it is a negative[34] form of protection against invasion; data protection is, thus, a different form of protection because it puts protection mechanisms in place that create a protective layer over our constantly moving data.[35] On the other hand, while data protection can be considered as contained in the wide notion of privacy, it has its own autonomy at the same time.[36] Data protection, in turn, refers to 'personal data' that pertains to any information that helps identify, directly or not, a natural person and it extends to "information concerning an identifiable person."[37]

As already mentioned, it is unsettled what the definition of privacy is on a universal level. That is likely to be a consequence of the fact that the content and scope of privacy are heavily influenced by individual preferences on

[29] Gloria González Fuster (2014) p.214
[30] *Ibid*
[31] Some also use the term "data privacy", see for example Diane Rowland, Uta Kohl and Andrew Charlesworth, *Information Technology Law*, *fourth edition*, Routledge (2012), p.152
[32] Stefano Rodotà, 'Data protection as a fundamental right'; eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwagne, Sjaak Nouwt, *Reinventing Data Protection?* (Springer 2009), p.79
[33] See Warren, Brandeis, *supra* note XX
[34] Stefano Rodotà (2009) p.79
[35] *Ibid*
[36] Gloria González Fuster (2014) p. 214-215
[37] Jan Trzaskowski, Andrej Savin, Björn Lundqvist, Patrik Lindskoug (2015) p.78

privacy, hence making it virtually impossible to contain in a definition.[38] What seems to be agreed upon, however, is the status that privacy enjoys in the legal world. Namely, as a [international] legal definition, privacy is mentioned in the Universal Declaration of Human Rights (hereinafter UDHR) in 1948, where it was defined in Article 12:

> "No one shall be subjected to arbitrary interference with his privacy, family, home and correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interferences or attacks."[39]

Following the UDHR, privacy was one of the rights contained in the International Covenant on Civil and Political Rights (ICCPR) in Article 17.[40] The right to privacy is contained in the European Convention on Human Rights (ECHR) under Article 8 and the general understanding of it has been largely aided by the ever-growing ECtHR jurisprudence.[41] For the purpose of this thesis, focus is placed on the Charter of Fundamental Rights of the European Union. In the EU Charter, privacy is enlisted as one of the fundamental rights, and while its status and importance are irrefutable, the right to privacy is by no means an absolute right.[42] This means that the right to privacy can be interfered with in certain circumstances, such as in instances of law enforcement and for national security purposes. The fundamental right to privacy as taken from the EU Charter is most often looked at in conjunction with the right to data protection, which is the subsequent fundamental right in the Charter.

Seeing as this thesis deals with primarily the law of the European Union, perhaps it is wise to give an overture of this specific framework when it

[38] Diane Rowland, Uta Kohl and Andrew Charlesworth (2012) p.152
[39] UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III)
[40] UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, 171
[41] Mathias Klang, Andrew Murray (ed.), *Human Rights in the Digital Age*, (Glasshouse Press, Cavendish Publishing 2005), 153
[42] Jan Trzaskowski, Andrej Savin, Björn Lundqvist, Patrik Lindskoug(2015) 69

comes to the distinction between privacy and data protection. In truth, save for the distinction contained in the EU Charter, there is little record of the two being distinctively separated both in legal norms as well as in case law of the European Union. This ambivalence started with Council of Europe's Convention 108[43] where data protection is practically in service of the right to privacy. Furthermore, *exempli gratia*, Directives such as 2001/29/EC[44], 2002/58/EC[45], also refer to data protection as part of the right to privacy. When it comes to relevant case law, *inter alia Promusicae,*[4647] *Scarlet*[48] (and subsequently *Netlog*[49]), show that not only has the Court dealt with data protection in the sense of it being a facet of the right to privacy, but it has also heavily relied on drawing a parallel with Article 8 of the ECHR (that does not explicitly mention data protection, but it is assumed that it encompasses it in its right to private and family life).[50] A deeper look at the legal frameworks and case law is focused upon *infra.*

These 'mix-ups' do not contribute to the clarity of the respective concepts; neither does the fact that the EU Charter stands alone in the explicit dedication to data protection as a separate right from privacy, at least on paper. Privacy is a much larger concept and it transcends to a vast number of aspects of human life, whereas data protection is largely quite contained in a specific setting. In this juxtaposition, as illustrated, privacy is viewed as encompassing a much broader concept than data protection itself. Having

[43] See *infra*
[44] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on The Harmonization Of Certain Aspects Of Copyright And Related Rights In The Information Society [2001] OJ L167/10
[45] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector (Directive On Privacy And Electronic Communications) [2002] OJ L 201/37
[46] C-275/06, Productores de Músicade España (Promusicae) v Telefónica de España SAU [2008] ECR 1-271, Judgment of the Court (Grand Chamber) of 29 January 2008, para. 64
[47] See also, Opinion of Advocate General Justine Kokott delivered on 18 July 2007 concerning C-275/06, Productores de Músicade España (Promusicae) v Telefónica de España SAU [2008] ECR 1-271, section C, paras. 51-56
[48] C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Judgment of the Court (Third Chamber) of 24 November 2011
[49] Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, Judgment of the Court (Third Chamber) of 16 February 2012
[50] Gloria González Fuster, (2014), p.247

said that, it is, in turn, taken that data protection is encompassed within privacy, as one increasingly important aspect of it. While the two terms and concepts are arguably inalienable from one another, at least when looked at from the perspective of protection, this thesis discusses data protection to a large extent, especially beginning with the discussion on Safe Harbor and onwards.

2.3 European timeline

In this section of the thesis focus is placed on the legal framework of privacy/data protection mechanisms in the EU from the very beginning. Since data protection law is one of the younger areas of law, it may not be so surprising for the reader that this thesis wants to encapsulate the timeline of the development of this area in the EU. Data protection was introduced in the OECD Privacy Principles[51] from 1980 and they were the first international agreement on data protection and, as such, have had plenty of success in laying the foundation of data protection and influencing national data protection laws.[52] The OECD Principles have influenced the subsequently written up legal instruments on data protection to a significant extent.[53] In continuation with the timeline, the thesis briefly mentions the Council of Europe framework and then proceeds with the EU legal framework.

2.3.1 Council of Europe

The framework of Council of Europe, while not being in main focus of this thesis, is quite important to mention. This is done with the aim of providing with the whole picture, and to aid to the understanding of the beginnings of data protection on European soil, because the instruments created under the

[51] OECD [Organization for Economic Co-Operation and Development] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) available at http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

[52] The Principles were updated in 2013. See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013) available at http://www.oecd.org/sti/ieconomy/privacy.htm

[53] Viktor Mayer-Schönberger, 'Generational Development of Data Protection in Europe', Philip E. Agre and Marc Rotenberg (eds.), *Technology and Privacy: The New Landscape*, (MIT Press 1997), p.220

Council of Europe umbrella can be said to have heavily influenced the instruments later adopted in the EU. The right to privacy was first mentioned in the European Convention on Human Rights (ECHR). However, privacy mechanisms began developing in the eighties with the Council of Europe Data Protection Convention 108/1981.[54] The Convention was a breakthrough and possibly served as an inspiration for the instruments to come. It was the first internationally binding legal instrument that deals exclusively with data protection.[55] Convention 108 was a result of a growing recognition of the role information technology would get to have. In 1999, the Convention was adapted so that the EU can become a party to the Convention, since all member states of the EU had already ratified it by then.[56] Additional Protocol to the Convention 108 was adopted in 2011, regulating international data transfers to countries outside the scope of the Convention 108, i.e. the Council of Europe countries.

2.3.2 European Union

As far as the European Union's legal framework for data protection goes, a brief overview of the development stemming from EU primary law is in order. Subsequently, we can take a look at the secondary law of the Union, specifically into directives, with a focus on the Data Protection Directive. With the EU pillar system going defunct with the Lisbon Treaty, data protection started gaining momentum in the Community – thanks to Article 286 of EC Treaty.[57] Article 286 EC Treaty was the sole article mentioning

[54] Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, (1981) ETS 108
[55] *Handbook on European data protection law*, European Union Agency for Fundamental Rights (2014), p.16
[56] *Ibid*
[57] Treaty establishing the European Community (Consolidated version 2002) - Part Six: General and Final Provisions, Article 286:
"1. From 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty.
2. Before the date referred to in paragraph 1, the Council, acting in accordance with the procedure referred to in Article 251, shall establish an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies and shall adopt any other relevant provisions as appropriate." OJ C 325, 24/12/2002 P. 0033 - 0184

data protection and it made all Community Acts regarding personal data protection applicable to the Community's institutions and bodies.[58] The then-existing acts were the Data Protection Directive, which is discussed in detail *infra,* and the e-Privacy Directive.[59] This Article also gave the basis for the foundation of the European Data Protection Supervisor (EDPS). This was done for the purposes of regulating the internal market and it was based in Article 95 EC Treaty that dealt with the approximation of laws.[60] Further acknowledgment of the importance of data protection came through the adoption of the Regulation 45/2001[61] and the Data Retention Directive.[62] Once the Lisbon Treaty entered into force, the EC Treaty morphed into the Treaty of the Functioning of the European Union (TFEU), Article 286 EC Treaty became Article 16 TFEU and Article 95 EC Treaty became Article 114 TFEU. With the Lisbon Treaty, the Charter of Fundamental Rights entered into force as well, and the Charter is one of the central instruments in this thesis, since it puts data protection on the level of a fundamental right. It is discussed in detail *infra.*

2.3.2.1 Data Protection Directive

The one directive that can be considered an axis of the data protection initiative in the EU is the Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such

[58] *Ibid*, See also Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (eds.), *The EU Charter of Fundamental Rights, A Commentary*, (Hart Publishing 2014), p.224
[59] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/07/2002 P. 0037 - 0047
[60] Treaty establishing the European Community (Consolidated version 2002), OJ C 325, 24/12/2002 P. 0033 – 0184, Article 95; see also Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (eds.), *The EU Charter of Fundamental Rights, A Commentary*, Hart Publishing (2014), p.224
[61] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
[62] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

data, dubbed as the Data Protection Directive.[63] The Data Protection Directive was created for the purpose of elaborating on the right to privacy as delineated in the Convention 108 of the Council of Europe, mentioned *supra*, as an "added protection"[64] to it. The Data Protection Directive came to be through Article 100 of the Treaty of Rome that regulated the internal market.[65] Immediately from Article 1 of the Directive, one can see the two main aims of the Directive: the first aim being the protection of fundamental rights and freedoms (**N.B.** the Directive uses the phrase "right to privacy with respect to the processing of personal data")[66] and promotion of free flow of data, thus, the second aim being of an economic nature.[67]

The overall aim of the Directive was to ensure harmonisation of the data protection laws on the national level. This would result in an equalised level of protection assured to the inevitable (and free)[68] movement of personal data between Member States of the EU. Hence, the Directive encompasses two aspects of this right: one being the fundamentality of the right to the protection of individuals' personal data and the other being a harmonization of the internal market with respect to enabling free data flow.[69] The level of protection afforded by the Directive can only be heightened but not lowered by the process of harmonisation with the national level(s), as stated by the CJEU in 2011.[70] The Directive prescribes six criteria for legitimate data processing.[71]

---

[63] Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995 (hereinafter Data Protection Directive)
[64] *Handbook on European data protection law,* European Union Agency for Fundamental Rights (2014), p.18
[65] Andrew Murray, *Information Technology Law, second edition,* (Oxford University Press 2013), p.490
[66] Data Protection Directive, Article 1(1)
[67] Data Protection Directive, Article 1(2), Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, (Oxford University Press 2013), p.20
[68] Gloria González Fuster, (2014), p.125
[69] Gloria González Fuster, (2014), p.126
[70] Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 November 2011, paras. 28-29, "[the] approximation of the national laws in this area must not result in any lessening of the protection hey afford, but must, on the contrary, seek to ensure a higher level of protection

2.3.2.2 The EU Charter of Fundamental Rights

The EU Charter, dating from 2000 was a product of a long discussion on how the EU could have an instrument of rights on its own, taking an example from the ECHR.[72] It was in 1999 that even the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (Article 29 Data Protection Working Party) stood in favour of including data protection in the list of fundamental rights.[73] This resulted in the Working Party producing a Recommendation to actually make the EU Charter of Fundamental Rights alongside urging Member States to follow suit and include data protection as a right in their national legal frameworks as well.[74] It was in this moment that data protection was gaining momentum as a fundamental right, being classified as part of the right to privacy.[75] The preamble of the Charter indicates that the whole instrument was inspired by the ECHR and EU Member States' own rights frameworks and implies that through wordings such as making rights "more visible and "reaffirming" them.[76]. The preamble is considered to make part of the general Community law principles, pursuant to ECJ's judgment in the *Fisher* case.[77] Viewed in conjunction, as the Court does when it comes to privacy, the Charter has two relevant Articles: 7 and 8. Article 7 concerns the respect for private and family life, largely reflecting and reiterating the ECHR. Article 7 of the Charter is a more broad aspect of privacy that this thesis will not specifically deal with. Article 8, however, concerns protection of personal data, a right that is relevant for the subject and purpose of this thesis. It should be noted that this particular right might as well be considered "made more visible" by

---

in the EU" **quot.in.** *Handbook on European data protection law,* European Union Agency for Fundamental Rights (2014), p.18

[71] Data Protection Directive, Section I under "Principles relating to data quality", Article 6 and 7.

[72] Gloria González Fuster, (2014), p.1

[73] Gloria González Fuster, (2014), p.193

[74] *Ibid*

[75] Draft Charter of Fundamental Rights of the European Union – New proposal for Articles 1-30 (Civil and political rights and citizens' rights), CHARTE 4284/00, CONVENT 28, (2000), 19

[76] Gloria González Fuster, (2014), p.2, *See also* Charter of Fundamental Rights of the European Union, Preamble, (2000/C 364/01)

[77] C-369/98 Fisher [2000] ECR I-6751 Judgment of the Court (Fourth Chamber) of 14 September 2000, **quot. in.** Gloria González Fuster, (2014), p.132

the Charter since it was not explicit part of, *exempli gratia*, the ECHR or other relevant instruments.[7879]

When it comes to Article 8, the Charter clearly draws inspiration from a number of instruments that precede it, such as the aforementioned Data Protection Directive and Convention 108.[80] The Charter can be considered to add a new dimension to the right to data protection: one of explicitly enumerating the components of this right that ought to be protected as a fundamental right, with the addition that protection of data is not only extended to data pertained to the notion of "private life" but all personal data.[81] This is an interesting (and important) way the Charter gives the right to protection of personal data a new scope, a new meaning. In sum, the Charter, despite having drawn inspiration from its preceding instruments, brings a unique scope of the right to protection of personal data to the table, compared to other international human rights law instruments.[82] In line with the discussion on whether privacy and data protection are one and the same, the relationship between the EU Charter's Articles 7 and 8 is interesting to look at. It has been argued that data protection is essentially reflective of having control over information about oneself, which, in turn, is a notion specific to privacy; hence it can be difficult to distinguish the two.[83] However, the right to protection of personal data as contained in the EU Charter, as well as other EU instruments such as the Data Protection Directive, see data protection as more than just the individual being in control over information about oneself, i.e. "informational self-determination."[84] That being said, these instruments expand the right to

[78] The ECHR is said to encompass the right to protection of personal data within its Article 8, however it does not mention it explicitly in the Convention text.
[79] Gloria González Fuster, (2014), p.2
[80] *See* Explanations Relating To The Charter Of Fundamental Rights Of The European Union, Text of the explanations relating to the complete text of the Charter as set out in CHARTE 4487/00 CONVENT 50, available at http://www.europarl.europa.eu/charter/convent49_en.htm [accessed 17 March 2016]
[81] Gloria González Fuster, (2014), p.205
[82] Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (eds.), *The EU Charter of Fundamental Rights, A Commentary*, Hart Publishing (2014), p.228
[83] AF Westin, *Privacy And Freedom*, Atheneum (1970), **quot.in.** Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (eds.), (2014), p.229
[84] Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (eds.), (2014), p.229

categories of lawful processing of personal data, rounding up the scope of the right in a much more comprehensive way.[85] In conclusion, the content of Article 8 reflects an unusual specificity in the way the right is to be interpreted, reflecting a system of *"checks and balances."*[86] As far as the case law goes, as explained *supra*, the relationship between privacy and data protection remains unclear from the jurisprudence of the CJEU.[87]

2.3.2.3 The European General Data Protection Regulation

The GDPR, regarded as the most complex and 'most lobbied piece of legislation'[88] in the EU, is expected to replace the Data Protection Directive in 2018. The idea of it is to harmonize EU data protection laws and act as a big upgrade from the Data Protection Directive from 1995[89] since the Data Protection Directive can be considered out-of-date and unable to efficiently cover issues arising with technological developments. The GDPR is in many ways a step forward towards assuring better levels of data protection, and its creation signifies an important shift in the way this new protection will take place. Namely, the GDPR marks a shift from a Directive-based approach to data protection to the one of Regulations,[90] meaning that the Regulations by the Commission have immediate legal force across the EU, as opposed to Directives that must be enacted by each Member State.[91] Among the many things that the GDPR will bring, one can be said to be the red thread: the GDPR will significantly increase the expectations of the standard of

[85] *Ibid*
[86] *Ibid*
[87] *See* cases such as C-465/00 Österreichischer Rundfunk [2003] ECR I-4989, C-28/08 Bavarian Lager [2010] ECR I-06055, Joined Cases C-92/09 and C-93/09 and Markus Schecke [2010] ECR I-11063; See also Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (eds.), (2014), p.230
[88] Hogan Lovells *Chronicle of Data Protection, Privacy & Information Security News & Trends*, available at http://www.hldataprotection.com/2016/01/articles/health-privacy-hipaa/the-final-gdpr-text-and-what-it-will-mean-for-health-data/ [accessed 4 May 2016]
[89] Juhi Tariq, *"NSA's Prism Program and the New EU Privacy Regulation: Why U.S. Companies with a Presence in the EU Could Be in Trouble,"* The American University Business Law Review 3.2 (2014), p.373
[90] *Ibid*
[91] On norm hierarchy, see also Jan Trzaskowski, Andrej Savin, Björn Lundqvist, Patrik Lindskoug, (2015), p.21

privacy. The GDPR draws inspiration from the Data Protection Directive, so it keeps the adequacy requirement for cross-border data transfers.[92] By placing data protection at a prioritized level for companies through increasing compliance demands to companies, the GDPR is essentially a big step in the evolution of the position of data protection overall. The GDPR does this in several ways.

Namely, the GDPR sets up a "one-stop shop", which ultimately means less administration for pan-European companies. This is done through having one independent supervisory authority monitoring one data controller or processor's activities on the Union level.[93] Through that, it also enables taking advantages of the single market.[94] Territorially, things will alter as well: if the data subject is in the EU and their data is being processed, it does not matter whether the data controller or processor is established in the EU.[95] This will apply if the data processing concerns services or goods offered to data subjects in the EU; and if the data processing concerns monitoring data subjects' behaviour so long as the said behaviour is taking place within the EU.[96] Moreover, and quite importantly, the GDPR increases sanctions for companies that are not in compliance. These sanctions can add up to 2-4% of the global yearly turnover of the incompliant company, which is definitely not something many companies will be likely to risk having to pay.[97] With regard to data transfers to third countries, the GDPR prescribes that data subjects are to receive more information, as well as references to established adequacy levels (by the European Commission) or, in general, existing safeguards.[9899]

[92] European Commission, Proposal for a *Regulation Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (2012), Recital 81 at http://ec.europa.eu/justice/data-protection/reform/index_en.htm [accessed 18 April 2016]
[93] *Ibid*, Recitals 96-98 and proposed Article 51(2)
[94] *Ibid*
[95] *Ibid*, proposed Article 3
[96] *Ibid*
[97] Ibid, proposed Article 79
[98] Ibid, proposed Article 41

2.4 Cross-border personal data transfers

2.4.1 Introduction

Personal data transfers are the focal point of this thesis, and everything in the thesis is looked at from that perspective. That being said, and with the foundation to (personal) data protection laid down in chapters *supra*, this sub-chapter serves as a bridge that leads the reader into the characteristics of personal data transfers to third countries (cross-border data transfers), i.e. non-Member States of the EU. Thus, this sub-chapter serves as the overture to the framework this thesis has promised to deal with in particular: one of Safe Harbor, its rise and its inglorious fall.

2.4.2 What are cross-border data transfers?

In today's world, data flows represent an outcome and means of the standardised way of living. It is so quotidian that it is deeply entrenched in the contemporary lifestyle. For example, buying an airplane ticket online will likely be conducted through a data transfer. Data flow, or data transfers, underpin the global economy, and with its intricate, network-based form of operation, they have become a complex and voluminous occurrence on the global market.[100] If one looks at Facebook, one of the most popular (if not the most popular) social networks, counting 1.59 billion users worldwide[101], it is safe to presume that there is a substantial amount of cross-border data transfers being executed very frequently.[102] The Data Protection Directive does not really define the term, but it regulates data transfers.[103] Data transfers are considered to be "data processing"[104] and, as such, must be in compliance with data processing requirements. The Data Protection

---

[99] For more, see IAPP, *Top 10 Operational Impacts of the GDPR* available at https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr [accessed 18 April 2016]
[100] Christopher Kuner, (2013), p.1
[101] See Statista, *Global Social Networks ranked by number of users*, available at http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ [accessed 20 April 2016]
[102] Christopher Kuner, (2013), p.119
[103] Christopher Kuner, (2013), p.11
[104] Jan Trzaskowski, Andrej Savin, Björn Lundqvist, Patrik Lindskoug, (2015), p.110

Directive is the key instrument in this regard, with its Recital 56 emphasizing the importance of cross-border data transfers for international trade.[105] Recital 56 is an introduction to Article 25 of the Data Protection Directive and it does not fail to mention the necessity of transferring data to a third country that ensures the adequate level of protection to such data.[106] Hence, Article 25 of the Data Protection Directive tackles data transfers that step out of the Directive's general, territorial scope indicating that a transfer of data in and of itself is not necessarily equal to processing, however, it is considered processing due to the likeliness of the transferred data to be processed in a third country upon transferring.[107] A note on extraterritoriality ensues by the end of this sub-chapter. Hence, in Articles 25 and 26 of the Directive, we can observe extraterritoriality – given that both the scope and effect of the Articles apply to third countries.[108] In this case, the Article 25 denotes that such data transfers are only allowed if an "adequate level of protection" is assured with regard to the said data. The necessity to have an instrument governing or guaranteeing the adequate level of protection of data in third countries was identified in the early onset from the moment the Data Protection Directive entered into force.

One of the first cases in the question of cross-border data transfers was *Bodil Lindqvist* in front of ECJ.[109] In the *Lindqvist* case, the question arose from publishing several types of personal data (such as names and addresses, medical data etc.) on a website. Publishing of that data was done without notice to the data subjects whose data was published, and without notice to the data supervision authorities. Some questions in the case were referred to the ECJ and the essence was whether posting such data on a webpage constituted a data transfer to a third country. In response to that, the Court stated that such actions do not constitute transfers to third

[105] Directive 95/46 EC, §56
[106] Diane Rowland, Uta Kohl and Andrew Charlesworth, (2012), p.162
[107] Jan Trzaskowski, Andrej Savin, Björn Lundqvist, Patrik Lindskoug, (2015), p.111
[108] Christopher Kuner, *Extraterritoriality and regulation of international data transfers in EU data protection law*, International Data Privacy Law (2015) Vol. 5, No. 4, Oxford University Journals p.239
[109] C-101/01 Bodil Lindqvist, ECR I-12971 (2003)

countries. It added that the Directive would be considered to have a global scope if publishing such data on a website were to be considered a transfer to third countries.[110] Since then, speculations about the requirement of the "adequate level of protection" have confounded scholars and practitioners alike. The interpretation of that requirement is profoundly important for the whole notion of cross-border transfers, and the Data Protection Directive is not very helpful in that regard.[111] In the many considerations and interpretations, many of them done by the Working Party 29, it was noted, however, that 'adequate' could not mean 'equivalent'[112] which the CJEU confirms in 2015. This is discussed in detail *infra*, in chapter *Schrems v. Data Protection Commissioner.*

From increased governmental cooperation, to exposing individuals to a variety of options for using a number of technological developments to their advantage and lastly, to giving companies the opportunity to take part in the global market, blurring the geographical borders are all but a few generalised benefits of cross-border data transfers.[113] Cross-border data transfers hold relevance in most socio-economic aspects, making it an integral part of a sustainable future.[114] Cross-border data transfers are, alas, not without risk. Analogously with the benefits, the risks of cross-data transfers can affect governmental cooperation by exposing data to unjustified access, individuals may be subject to inaccessibility and inability to protect their data protection rights due to insufficient redress mechanisms abroad and companies can suffer in case there are data breaches due to insufficient security measures.[115] Furthermore, with the ubiquity of cross-border data transfers, it can be next to impossible for a data subject to be aware of where their data is being processed, which countries has it been transferred to etc.[116] This is largely the problem with all internet-related

[110] Diane Rowland, Uta Kohl and Andrew Charlesworth, (2012), p.162-163
[111] *Ibid*,, p.163
[112] *Ibid*, p.164
[113] Christopher Kuner, (2013), p.102
[114] *Ibid*, p.103
[115] *Ibid*, p.104
[116] *Ibid*, p.123

issues – that the internet is geographically unconcerned, which renders jurisdictions and different legal systems somewhat obsolete. This can be cause for concern.[117]

In conclusion, it may be of illustrational importance to explain a typical data flow such as the one that was subject in the *Schrems* case that is discussed *infra.* Namely, Facebook, like other Internet giants such as Apple, Google, Microsoft and others, have European subsidiaries, mainly in Luxembourg and Ireland. *Facebook Ireland Ltd,* however, does not process the data it receives but transfers i.e. "exports" that data to the U.S. where its parent company, *Facebook Inc.* is situated. This is not a problem if the receiving country (U.S.) affords the EU-exported data an adequate level of protection, as prescribed in Articles 25 and 26 of the Data Protection Directive. However, Edward Snowden's revelations about PRISM[118] showed that the data is capable of being subject to mass and indiscriminate surveillance, hence, is not treated up to the standard required by the Data Protection Directive.[119] This becomes even more worrisome when one knows that all organisations in the PRISM[120] programme were Safe Harbor-certified organisations. To be clear, the mentions of Facebook are *not* implications that Facebook is responsible for the privacy breaches discussed in the Schrems case. The process takes on the following shape: Facebook, a Safe Harbor-certified organisation processes EU citizens' personal data and if that data is given to U.S. authorities, Facebook is not the one to place the breach onto, since Facebook (U.S.) is merely complying with its national legislation. As a reminder, the PRISM programme was enacted with The Foreign Intelligence Surveillance (FISA) Act, and it operates under the

---

[117] See also Christopher Kuner, (2013), p.123

[118] *Planning Tool for Resource Integration, Synchronisation and Management* (PRISM), a clandestine data surveillance programme by the U.S. National Security Agency (NSA) that collects telecommunications and Internet communications from U.S.-based Internet companies.

[119] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, *Opinion of Advocate General Bot*, (2015), ECLI:EU:C:2015:627, para.155

[120] Timothy B. Lee*, Here's everything we know about PRISM to date*, The Washington Post, (12th June 2013), available here: https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/ [accessed 4 April 2016]

supervision of the FISA Court. The U.S. legislation also binds the PRISM subjects with "gag orders", meaning they cannot disclose anything about the programme.[121]

Lastly, international data transfers are vital to businesses since these transfers enable exchange of various types of data: payment details i.e. transaction details, employee information, targeted advertising etc. International business and trade are largely dependent on international data transfers [data flow].[122] This is all the more true for the EU and U.S. considering the scope and size of their trade and business relationship, being each other's largest partners in that regard.[123] Commissioner Jourová called data transfers, specifically the transatlantic ones "the backbone" of EU's economy.[124] Hence, looking at the whole picture of cross-border data transfers, there seems to be some sort of a conflict between the fact that free data flow is a necessity in the global village created by the internet on the one hand, and there is a growing need to regulate such flows in order to reconcile systemic differences on the other hand.[125] In addition to that, it has been argued that we ought to stop looking at data protection laws with a black-and-white attitude. Namely, the principle of extraterritoriality might not be the best way to look at cross-border data transfers simply because it does not solve pretty much anything due to a variety of factors, out of which the one of the nature of internet is definitely not to be neglected.[126] When it comes to cross-border data protection laws, it is important to bear in mind

---

[121] Kashmir Hill, *Google Challenges Government Gag Order On National Security Requests,* Forbes.com, (18th June 2013), available at: http://www.forbes.com/sites/kashmirhill/2013/06/18/google-challenges-government-gag-order-on-national-security-requests/#2e34e9e935a3 [accessed 4 April 2016]

[122] Martin A. Weiss, Kristin Archick, *The EU – U.S. Safe Harbor Agreement on Personal Data Privacy: In brief*, (Congressional Research Service 2015), p.4

[123] Martin A. Weiss, Kristin Archick, (2015), p.4

[124] European Commission, "*First Vice-President Timmermans and Commissioner Jourová's Press Conference on Safe Harbor Following the Court Ruling in Case C-362/14 (Schrems),"* press release (October 6, 2015), **quot.in.** Martin A. Weiss, Kristin Archick, (2015), p.4

[125] Christopher Kuner, (2013), p.186

[126] Dan Jerker B. Svantesson, *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation,* International Data Privacy Law (2015) Vol. 5, No. 4, Oxford University Journals, Symposium Article, p.233

that any discussion on distinguishing territoriality and extraterritoriality is futile.[127]

2.5 Summary of the Chapter

- In an internet-dominated world, privacy has gained tremendous momentum as a fundamental right.
- In practice and academia, privacy and data protection are terms often used interchangeably, which implies they are considered one and the same. However, the two could benefit from greater distinction.
- Data protection is understood to be part of privacy, however still keeping its own autonomy. The EU Charter of Fundamental Rights mentions privacy and data protection as two rights.
- The EU data protection legislation was largely influenced by Council of Europe instruments (e.g. Convention 108) and the OECD Privacy Principles.
- The Data Protection Directive is the most important data protection instrument in present-day European Union.
- Cross-border data transfers are essentially data processing and are, as such, governed by Article 25 of the Data Protection Directive.
- Article 25 Data Protection Directive prescribes that transfers are to occur only to a third country that provides adequate protection for the transferred data.
- The EU General Data Protection Regulation, entering into force in 2018, is a long-anticipated instrument that will hopefully bridge the gap between technology and data protection mechanisms.

[127] *Ibid*

3 Freedom to conduct business - how does it fare against other fundamental rights?

3.1 Introduction

This chapter deals with the freedom to conduct business as contained in Article 16 of the EU Charter. This chapter is envisaged to give the reader a basic overview of the scope of the freedom to conduct business as a fundamental right, and to link it with the topic of this thesis. This is done to present a confounding balance that is to be stricken between data protection and the freedom to conduct business highlighting how these rights can be pulling in the same direction at times, or how they can have a more tense relationship at times as well. The chapter uses a set of CJEU cases that have highlighted the importance of striking the balance of interests among fundamental rights themselves, as read from the EU Charter.

3.2 Hanging in the balance

The freedom to conduct business is not prescribed so explicitly in international human rights law instruments as it is in the EU Charter.[128] However, the ECtHR has drawn parallels to it through the right to property contained in ECHR Article 1 of Protocol 1.[129] Despite not being a "traditional" fundamental right, the freedom to conduct business began with case law[130] of the ECJ at the same time when other human rights were gaining momentum as well.[131] The freedom to conduct business, at its core, revolves around a "principle of economic autonomy" that exists within the

[128] EU Network of Independent Experts on Fundamental Rights, *Commentary of the Charter of Fundamental Rights of the European Union* (2006), p. 158
[129] European Union Agency for Fundamental Rights, *Freedom to conduct business: exploring the dimensions of a fundamental right* (2015), p.10
[130] *Exempli gratia:* ECJ, Nold, Case 4/73 [1974] ECR 491; ECJ, Stauder v. City of Ulm, Case 29/69 [1969] ECR 419
[131] Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (eds.), (2014), p.440-441

European Economic Constitution.[132] This freedom, however untraditional, has been characterised as one of the general principles of EU law[133], and as such is subject to certain restrictions in terms of striking a balance between it and other fundamental rights and freedoms.

In relation to that, there is interesting case law dealing with the conflict between the freedom to conduct business and other rights and freedoms out of which this thesis uses merely a couple of cases in order to illustrate the scope of the freedom to conduct business in this context. The cases that illustrate this the best are *Scarlet Extended*[134] and *Netlog*.[135][136] A slightly older case of the same nature was *Promusicae*.[137] All cases dealt with an association of copyright holders trying to force intermediaries like Internet Service Providers (ISPs, *Scarlet Extended* and *Promusicae*) and Hosting Service Providers (HSPs, *Netlog*) to install costly software that would collect personal data (such as names, addresses and IP[138] addresses) of the intermediaries' users for the purpose of pursuing enforcement of the intellectual property rights of the copyright holders. Hence, the Court was tasked with striking a particular balance between several fundamental rights and, by parallel, between a set of different interests. In *Promusicae*, the CJEU withholds from making a particularly strong standpoint by holding that there is no reason to believe that EU data protection laws prevent from introducing obligations of disclosing personal data in civil proceedings or that intellectual property law provisions would impose this as an obligation

[132] Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (eds.), (2014), p.441
[133] C-283/11 *Sky Österreich v. Österreichischer Rundfunk* Advocate General Bot Opinion (2013), para.29, **quot.in.** Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (eds.), (2014), p.448
[134] C-70/10 Scarlet Extended v. SABAM (2011)
[135] C-360/10 SABAM v. Netlog (2012)
[136] **N.B.** Section 16.32 dealing with *Scarlet Extended* and *Netlog* in the EU Charter Commentary can mislead the reader into thinking that the judgments in these two cases dealt a blow to Internet freedom, which is inaccurate. The two cases have been celebrated as cases that protect free information flow and data protection on the Internet much to the chagrin of Intellectual Property Law. The source in question is: Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (eds.), (2014), p.451
[137] Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU [2008]
[138] Internet Protocol

either.[139] Focusing on the general principle of proportionality,[140] CJEU concludes the case by leaving the balancing question quite open.[141] This changes in *Scarlet Extended* and subsequently *Netlog* where the Court makes a firmer stance when it comes to the balancing question. In these two cases, the Court juxtaposes the fundamental right to property (where intellectual property is enshrined, Article 17(2) Charter) with the freedom to conduct business (Article 16 Charter) and the right to data protection (Article 8 Charter).[142] This was done because the nature of the injunction that was to be imposed on intermediaries for the protection of intellectual property rights would severely interfere with the fundamental right to data protection and the freedom to receive or impart information (Article 11 Charter)[143] and lastly, with the freedom to conduct business because the software would be quite costly and would impair the intermediaries' competitive position and would affect their conduct of business in general.[144]

Following the Court's jurisprudence in the matters relating to the freedom to conduct business it can be noted that the Court has expanded its scope and protection more than was expected to be granted to this unconventional fundamental right and this is easily deduced from the EU's strong economy-driven spirit. On the other hand, a question indubitably rises when it comes to the way the Court balances fundamental rights in the long run – will every Internet-related intellectual property claim be balanced against data protection and privacy?[145] In this case it is safe to say that it is highly likely the ruling would be in favour of data protection and privacy. Albeit, that particular balance is not the central point of this thesis so the question will

[139] C-275/06, Promusicae [2008], paras.54,59-60, **quot.in.** Christophe Geiger (Ed.), *Research Handbook on Human Rights and Intellectual Property,* (Edward Elgar Publishing 2015), p.72
[140] C-275/06, Promusicae [2008], para.63
[141] Christophe Geiger (Ed.), (2015), p.73
[142] *Ibid,* p.74
[143] *Ibid*
[144] Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (eds.), (2014), p.452
[145] Christophe Geiger (Ed.), (2015), p.129

remain unanswered for the time being but it remains relevant to the overall balancing challenge the Court is often faced with.

3.3 Linking the freedom to conduct business with data transfers

As said, both the freedom to conduct business and the right to privacy and data protection enjoy the status of fundamental rights. However, neither of the two are absolute rights. It is interesting to observe cross-border data transfers from a business perspective, mostly because it could be considered as if there is a certain conflict as was briefly illustrated *supra*. Namely, as has been argued, there is privacy protection on one side, and there is *free flow of information* on the other side, aiding businesses in harnessing the advantages of technological developments for the purpose of conducting international business.[146] Cross-border data transfers have been a quintessential element to business ever since the early stages of digitization – in fact, according to a study done as far back as 1983, an astoundingly large number of 83% of businesses depended on cross-border data transfers in at least some parts of their operations.[147] In particular, the transatlantic trade partnership relies heavily on data flow. Namely, the transatlantic partnership represents half of the global economic output and almost one trillion dollars in goods and services trade, with a wide range of businesses, from the biggest ones to the small and medium enterprises.[148] While the public sector, i.e. governments have been collecting personal data for decades, the private sector is becoming more dependent on personal data due to technological and commercial advancements and this inevitably brings about a series of privacy/data protection risks.[149] This is particularly

[146] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC: A comparative analysis of the privacy statutes of the Federal Republic of Germany, France, the United Kingdom and the Netherlands and their impact on the private sector,* (Kluwer Law and Taxation Publishers 1990), preface

[147] Business International, Transborder Data Flow, Issues, Barriers and Corporate Responses, a Business International Multiclient Study, New York (1983), p. 9, **quot. in.** A.C.M. Nugter, (1990), p.2

[148] Letter from Under Secretary for International Trade, Stefan Selig, U.S. Department of Commerce, the EU – U.S. Privacy Shield documents, Annex 1

[149] Lilian Edwards, Charlotte Waelde, *Law & the Internet, a framework for electronic commerce,* (Hart Publishing 2000), p.80-81

so since every individual's action on the Internet results in producing data.[150] This data is, in most cases of more value to businesses than to anyone else.[151] Hence, proper protection is essential to the *status quo* of trade.

3.4 Summary of the Chapter

- Freedom to conduct business is contained in Article 16 of the EU Charter.
- It is considered a general principle of the EU, but it is not an absolute right, hence it is subject to limitations.
- These limitations are shown in situations where the freedom to conduct business is to be balanced against other fundamental rights.
- Cases like *Promusicae*, *Scarlet Extended* and *Netlog* are good examples of the balance between the right to (intellectual) property on the one hand, and freedom to conduct business and the right to data protection on the other.
- *Promusicae*, *Scarlet Extended* and *Netlog* have shown that there is a strong likelihood that freedom to conduct business and data protection might prevail over a fundamental right such as property, but that brings along questions of its own for the future.
- Cross-border data transfers have been a quintessential element to business since the early stages of digitization.
- Modern businesses are dependent on data transfers. This makes for a stronger case for the necessity to extend proper protection to the data that is in constant flow.

[150] Lawrence Lessig, *Code version 2.0*, (Basic Books 2006), p. 216
[151] *Ibid*

4 Safe Harbor, not so safe

4.1 Introduction

Safe Harbor was created in 2000, with the aim to level the playing field for the aforementioned differences in the treatment of data in the EU and the U.S. respectively. It was created by the U.S. Department of Commerce and the European Commission on 1st November 2000, with consults from businesses and NGOs alike.[152] The creation of Safe Harbor was followed with a set of tense negotiations.[153] The basic justification for the necessity to produce a legal instrument of the sort was the "adequacy" criterion[154] delineated in the EU Data Protection Directive, as elaborated upon *supra.*[155] However, it is important to note that Safe Harbor was motivated by politics and trade interests, seeing as the transatlantic partnership holds a lot of commercial and trade value to both the EU and the U.S.[156] The Safe Harbor framework was adopted with a "Safe Harbor decision" of the European Commission (2000/520/EC) as its legal basis.[157] Thus, contrary to popular belief, Safe Harbor is *not* an agreement, but rather an executive decision made by the European Commission.

As mentioned, the initiative behind creating Safe Harbor was not solely the protection of privacy of EU citizens. Data being a currency of the modern age, Safe Harbor was also created for the purpose of harvesting the economic benefits of proper data transmission.[158] Thus, the way Safe

[152] Tim Kevan and Paul McGrath, *E-Mail, the Internet and the Law, Essential knowledge for safer surfing*, (EMIS Professional Publishing 2001), p.133
[153] Diane Rowland, Uta Kohl and Andrew Charlesworth, (2012), p.164
[154] Tim Kevan and Paul McGrath, (2001), p.133
[155] See Chapter 2.3.2.1
[156] Diane Rowland, Uta Kohl and Andrew Charlesworth, (2012), p.164
[157] 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 Harbor Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (notified under document number C (2000) 2441) (Text with EEA relevance.)
[158] Henry Farrell and Abraham Newman, (2016), p.130

Harbor functioned was by U.S.-based companies[159] signing up to the Safe Harbor framework via an online application form. By signing up for the Safe Harbor framework, organisations would do their business in compliance with the European data protection standards and they would likely avoid any interference by the European authorities.[160] Safe Harbor counted about 4,500 businesses that relied on its framework to transfer EU data to the U.S.[161] As noted *supra*, Safe Harbor was very important for economic reasons, and it played a significant role in enabling business and trade. Safe Harbor has seven core principles: 1) Notice; 2) Choice; 3) Onward Transfer; 4) Access; 5) Security; 6) Data integrity; 7) Enforcement. The principles will be addressed shortly for the purpose of acquainting the reader with the content of Safe Harbor. This will prove to be relevant at a later instance, with the Privacy Shield analysis.

The first principle, *Notice* merely requires that the member organisation inform data subjects on a number of things: why (for what purpose) was their data being collected, how is it being used, how data subjects can contact the organisation or issue complaints, as well as what options do data subjects have with regard to the limitation of the use of their data.[162] Second, *Choice* gives data subjects the opportunity to opt-out from disclosing their data to third parties or in cases where data is to be used in ways other than the previously stated purpose of its collection. This principle also deals with an opt-in variable, which regards sensitive data that is to be treated the same way: disclosed to third parties or used for a different purpose.[163] The third principle, *Onward Transfer*, deals with transfers to third parties, where it is prescribed that the principles Notice and Choice have to be used and adds that the third party in question is to be a Safe Harbor-certified organisation or is in some way found to be providing for an adequate level of protection to data.[164] Further on, the fourth

[159] Safe Harbor refers to businesses and companies as "organisations"
[160] Tim Kevan and Paul McGrath, (2001), p.133
[161] Martin A. Weiss, Kristin Archick, (2015), p.1
[162] U.S. – EU Safe Harbor Framework, Guide to Self-certification (2009), p.4
[163] *Ibid*, p.5
[164] *Ibid*

principle, the principle of *Access* grants data subjects the possibility of requesting the data an organisation could have on the data subject. The data subject must be able to make corrections or delete the information held by the organisation when it is inaccurate. This comes with one limitation: one that regulates the proportionality of such a request made by the data subject – the request is to be weighed against the risk of the data subject's privacy with the expense falling on the organisation for enabling that access. The fifth principle, *Security*, prescribes that organisations must undertake measures of securing the personal data that they handle against misuse or other fraudulent behaviour.[165] The sixth principle, *Data integrity*, emphasises that the purpose of the data collection must match the actual collection, adding that the purpose should be limited in its scope and should reflect the usage of that data.[166] Lastly, the seventh principle, *Enforcement* regards the ensuring of compliance with Safe Harbor. In this principle, three segments are described: a) availability of independent recourse mechanisms; b) existence of procedures that verify the proper [or improper] application of the framework; c) remedy obligations in case of incompliance.[167]

4.2 Systemic differences that create problems

Safe Harbor was initiated and completed as somewhat of a compromise between the two (EU – U.S.) systems that could be said to be initially diametrically opposed in their view [and treatment] of privacy as a whole, including data protection. While this thesis will not go deep into the U.S. system and treatment of privacy and data protection, it is perhaps interesting to juxtapose it with the EU system. This is done for the purpose of illustrating, albeit shortly, why a framework such as Safe Harbor is necessary, but also why such a framework failed. Firstly, the notions of privacy and data protection in the U.S. do not enjoy the same level of protection as it does in the EU. This is why there is a need to have a

[165] *Ibid*
[166] *Ibid*
[167] *Ibid*, p.5-6

framework that will equate the two, by elevating the level of protection (of EU data subjects) in the U.S. in the first place. Secondly, the approach to privacy protection in the U.S. is not unified under one instrument that tackles it. If there are instruments of protection, they are largely on a federal level.[168] The U.S. approach can be described as "sectoral",[169] because its privacy protection mechanisms are limited and done via *a targeting method* meaning that they tackle privacy matters in certain areas, such as child protection, healthcare etc.[170] In contrast, the EU favours the approach of effective, omnibus legislation that protects and provides for proper enforcement mechanisms. These differences are visible in the legal instruments created for the protection of privacy (data protection), with the EU beginning its protection system in the nineties and with the U.S. still refusing to take similar legislative actions.[171]

4.3 The criticism

The news that the Safe Harbor framework was abolished were not so surprising after all. The framework was flawed from the beginning in the sense that there were large discrepancies between how things should be done, on the one hand from the perspective of the European Union and, on the other hand, from the perspective of the United States. One of the things worth mentioning in that regard is that organisations were basically going through a "self-certification"[172] process to be in accordance with the framework, at least on paper. This makes for a U.S. self-regulatory way of

[168] See also Robert Hasty, Dr. Trevor W. Nagel and Mariam Subjally, White & Case, *Data Protection Law in the U.S.A.*, Advocates for International Development (2013), available at http://www.a4id.org/sites/default/files/user/Data%20Protection%20Law%20in%20the%20USA_0.pdf [last accessed 17 March 2016]; also Letter from Ambassador Aaron about Safe Harbor (November 1999) available at http://www.export.gov/safeharbor/aaron419.html [last accessed 17 March 2016]
[169] Daniel R. Leathers, *Giving Bite To The EU-U.S. Data Privacy Safe Harbor: Model Solutions For Effective Enforcement*, Case Western Reserve Journal of International Law, vol. 41 (2009), p. 197
[170] *Ibid*
[171] *Ibid*
[172] *U.S. – EU Safe Harbor Framework*, Guide to Self-certification (2009), p.4

doing things, and creates a clear distinction from the EU approach that focuses more on effective legislation.[173]

The self-certification process was not double-checked or verified by the U.S. Department of Commerce (DoC). That translated to the possibility of an organisation joining Safe Harbor without really establishing a privacy policy.[174] Further on, it provided for *too much* self-governing from the companies that were to join the Safe Harbor framework: the company has to self-regulate its privacy program and create its very own self-regulatory privacy policy. Along with that, an organisation joining the framework is required to issue a public declaration of that.[175] These criteria, among others, have been problematic from the very beginning of Safe Harbor. Namely, the Commission Staff Working Document[176] elaborates on the difficulties surrounding them. *Exempli gratia*, some organisations (companies) failed to have their privacy policy publicly available.[177] The Report went on to acknowledge the inexistence of an effective monitoring systems since many forms of monitoring would eventually submit organisations to highly costly auditing processes, for example.[178] This report had noticed many problematic aspects with the implementation of the Safe Harbor Framework and others who joined in the criticism shared that opinion by and large.

The largest issue Safe Harbor has had was the lack of proper enforcement mechanisms, which meant that organisations could easily by-pass the necessary obligations stemming from the Safe Harbor principles and make part of the framework only *de iure,* but not necessarily *de facto* as well.

---

[173] Chris Connoly, *The US Safe Harbor - Fact or Fiction?* (Galexia 2008), p.4
[174] Daniel R. Leathers, (2009), p.221
[175] *U.S. – EU Safe Harbor Framework*, Guide to Self-certification (2009), p.4
[176] Assessment after three years of implementation of Safe Harbor, 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 (20.10.2004)
[177] 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 (20.10.2004), p.6
[178] *Ibid*

Some of the things widely criticized about the framework were the ease with which organisations could simply misinform, deceit EU citizens and businesses by putting up a Safe Harbor Mark that is supposed to demarcate the organisations that make part of Safe Harbor by complying with its criteria and principles, when, in fact, they do not. Even just a couple of years after the conception of Safe Harbor, experts have called for its scrapping since it stood in the way of every solution to its own problems.[179]

Having all of the criticism in mind, it can seem quite silly, for the lack of a better word, that the U.S. Department of Commerce hailed Safe Harbor as such a success and "gold standard for data protection."[180] It seemed that Safe Harbor was a formal solution with little to no effect in real life. In fact, the very knowledge of Safe Harbor's flawed nature brings out the question why it was not abolished sooner? This likely falls into the realm of the fact that it was better for business (and data) to have *some sort of framework* instead of *no framework* at all.[181]

4.4 Alternative modes of protection

The EU and the U.S. play a vital role in each other's trade interests. There is a vast amount of data flow between the two for the purposes of business and trade. Putting that gargantuan amount of data transfers between the U.S. and EU on hold would be an unviable, bad idea. Hence, data transfers themselves did not cease with the abolishment of Safe Harbor. As an immediate consequence, it is also highly likely that there has been a number of illegal transfers right after the *Schrems* judgment was brought. Striking down Safe Harbor meant that the U.S., the EU and organisations/businesses were to work together towards not only a brand-new mechanism of providing adequate protection to the data transferred to the U.S. but also on effective interim measures that would provide protection.

[179] Daniel R. Leathers, (2009), p.222
[180] Chris Connoly, (2008), p.5
[181] Martin A. Weiss, Kristin Archick, (2015), p.10

Shortly after Safe Harbor was abolished, the Article 29 Working Party issued a statement where it emphasizes that businesses were to assess risks of data transfers and consider introducing alternative "legal and technical solutions for the purpose of respecting the EU data protection acquis."[182] The solutions were largely in the form of Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), otherwise called *derogations*.[183]

In this regard it helps to look at the European Commission's Communication[184] following the *Schrems* judgment. According to the Communication, using derogations comes with a set of conditions to be met: firstly, data can only be transferred if it was collected and processed by a relevant data controller under the respective EU national laws coherent with the Data Protection Directive[185] and secondly, in the event of a lack of adequacy of protection, data controllers are to take measures that provide safeguards in accordance with Article 26(2) of the Data Protection Directive.

To illustrate: in a multinational corporation, it is likely that Binding Corporate Rules will be the standard model of protection in order for data to be transferred within the same corporation, but to third countries, whereas Standard Contractual Clauses will be used for transfers to external companies or organisations operating in third countries.[186]

---

[182] Article 29 Working Party Statement on the Schrems Judgment (16 October 2015) available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf [accessed 25 April 2016]

[183] See also *A business guide to changes in European data protection legislation*, Cullen International S.A., Kluwer Law International (1999), p.15

[184] European Commission, *Communication From The Commission To The European Parliament And The Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*, available at: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf [accessed 25 April 2016]

[185] Ibid, p.12

[186] Jan Trzaskowski, Andrej Savin, Björn Lundqvist, Patrik Lindskoug, (2015), p.114

4.5 Summary of the Chapter

- Safe Harbor was created in 2000 by joint efforts of the European Commission and the U.S. Department of Commerce.
- The Safe Harbor Decision is the legal basis of the Safe Harbor framework. Safe Harbor (framework) is *not* an agreement.
- The adequacy criterion prescribed in the Data Protection Directive was the basic justification for creating the Safe Harbor framework, alongside business and trade motivations, seeing as the EU – U.S. partnership is very valuable.
- The many differences between the ways the EU and U.S. treat personal data made it challenging to secure an "adequate level of protection."
- Safe Harbor aimed to level the differences between the two systems.
- The aim of Safe Harbor was to ease trade and commerce between EU and the U.S.
- The criticism of Safe Harbor was based largely on its self-certificatory and self-regulatory nature.
- Without proper enforcement mechanisms in place, rules of the Safe Harbor framework were easily by-passed by organisations.
- Once Safe Harbor was abolished, in October 2015, alternative modes of protection were put in place. Namely, the Standard Contractual Clauses (SCCs) and the Binding Corporate Rules (BCRs).

5 Maximillian Schrems v. Data Protection Commissioner

5.1 Background

The case of *Maximillian Schrems v. Data Protection Commissioner*, C-362/14, in front of the Grand Chamber of the Court of Justice of the European Union is the axis of this thesis. The decision to write a thesis around this case ultimately translates to the ground-breaking importance of the said case for the awareness of privacy protection mechanisms and the way they function (or not). The judgment in this case was brought on 6th October 2015, just merely half a year before this thesis is written. The Schrems case has thrown the issue of adequate privacy protection into the spotlight because the case has brought the Safe Harbor framework to a halt, along with rendering the Decision 2000/520/EC invalid. At the time when the decision came out, the Safe Harbor regime had been an important framework that over 5,000 U.S. companies had been using for the purpose of secure data transfers from the EU.[187] However, the case originated in Ireland, which is what this thesis briefly presents *infra.*

5.2 The Irish procedure in brief

The plaintiff in the case was Maximillian Schrems, an Austrian PhD student and Facebook user, while the defendant was Helen Dixon, the Irish Data Protection Commissioner (DPC). The complaint against Facebook Ireland Ltd with the DPC was filed on 26th June 2013, and shortly after that, the DPC stated that it had no duty to investigate. The Irish case was based on judicial review at the High Court of Ireland and filed in October 2013. The bases for this judicial review were the revelations of Edward Snowden, a computer administrator whose employer was contracted to work for the U.S. National Security Agency (NSA). Snowden decided to unlawfully

[187] Dr. Nora Ni Loidean, *The End Of Safe Harbor: Implications For EU Digital Privacy And Data Protection Law*, (Journal of Internet Law 2016) Vol. 19 Issue 8, p.8

appropriate NSA files, disclosing them in several media outlets such as *The Guardian, the Washington Post* and *the New York Times*. Snowden's actions revealed evidence of mass surveillance of Internet and telecommunication systems. Schrems maintained that these revelations were evidence enough that there is no proper data protection in the United States and that the DPC should, in light of these findings, order Facebook Ireland Ltd. to stop transferring personal data to its parent company in the United States.[188]

The DPC claimed that she was not required to launch an investigation on the matter. Over the course of the proceedings, Schrems's complaints have been described as "frivolous and vexatious" by the DPC, which the High Court did not find to be true; moreover, the Court clearly stated that while Schrems was not able to provide the Court with evidence of his own personal data being used in the ways he alleged, it was not necessary for him to be able to prove his own data being subject of surveillance, given the evidence of such happenings on a mass scale [due to Snowden's revelations].[189] The High Court referred a set of questions to the CJEU, pursuant to Article 267 TFEU.

5.3 Proceedings before the Court of Justice of the European Union

The case was referred to CJEU (the Grand Chamber) on 25 July 2014, with a lodged complaint requiring the Data Protection Commissioner to prohibit *Facebook Ireland Ltd.* from transferring personal data of the Applicant, Maximillian Schrems, to the United States. The Respondent was the Data Protection Commissioner, and Digital Rights Ireland Ltd. as *amicus curiae.* An invitation for intervention was extended to the European Data Protection Supervisor (EDPS). As grounds, the complaint had the reasoning that the

[188] See High Court of Ireland, Maximillian Schrems v. Data Protection Commissioner [2013 No. 765JR], para.2
[189] See *Ibid*, paras.74-75

United States did not provide for an adequate level of protection of such data. The case, in its entirety, was grounded in the knowledge of vast surveillance activities by the U.S. public authorities as disclosed by Edward Snowden. The request for a preliminary ruling was with regard to the interpretation of the Articles 25(6) and 28 of the Data Protection Directive 95/46/EC in the light of Articles 7 and 8 of the EU Charter and to the validity of the Commission Decision 2000/520/EC (Safe Harbor Decision). There was a question of the power of national supervisory authorities as well, seeing that the Data Protection Commissioner was of the view that the complaint lacked evidence, that he was not required to launch an investigation, as well as because Decision 2000/520 determined the adequacy requirement.

5.4 Findings of the Court

Concerning the power of national supervisory authorities, as prescribed in Article 8(3) of the EU Charter, the EDPS advised that Safe Harbor cannot limit the power of data protection authorities. Furthermore, the Court reminded of the fact that Article 28 of the Data Protection Directive, Article 8(3) of the EU Charter and Article 16(2) TFEU require Member States:

"To set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of [such] data."[190]

In relation to that, the Court duly noted that these powers do not extend to personal data processed outside the respective Member State, however, it made clear that the mere transfer of personal data from a Member State to a third country constitutes "processing" within its territory.[191] In this sense, the supervisory authorities have the power to assess whether the transfers of

[190] C-362/14, Maximillian Schrems v. Data Protection Commissioner, joined party Digital Rights Ireland Ltd, [2015], ECLI:EU:C:2015:650, para.40

[191] *Ibid*, paras.44-45

personal data comply with the criteria from the Data Protection Directive.[192] The Court then engaged into a delicate balancing when it comes to supervisory authorities' powers with regard to the "adequate level of protection" afforded to personal data in third countries. Namely, the Court made clear that the Data Protection Directive with its Article 25 provides the framework for assessing the adequacy level. Hence, the Directive states that a Member State or the Commission can evaluate the adequacy of a third country, however, if the Commission should make a decision that a country provides with adequate protection, that decision is binding to all Member States and they are not to undertake measures contrary to that decision.[193]

However, the Court emphasised that this decision would not impede national supervisory authorities from performing proper oversight over transfers of personal data to the country subject of the said Commission decision.[194] In other words, the national supervisory authorities are to examine the adequacy, particularly if there is a claim that a third country does not in fact provide the adequate level of protection, like in the case of Maximillian Schrems. As the Advocate General notes, Article 25 of the Directive does not grant the Commission exclusive powers in this regard and Member States do have a role in the process as well.[195] Subsequently, the Court stressed that a claimant, like Schrems, is to have access to judicial remedies in case their claim were rejected; and, on the other hand, in case they were to be well founded, the national supervisory authority must be able to engage in legal proceedings as it is prescribed in Article 28(3) of the Directive.[196]

When it comes to the validity of the Safe Harbor Decision, the EDPS advised that a combination of the fact that Safe Harbor was always flawed with the fact that the mass surveillance in the U.S. has escalated to serious

[192] *Ibid*, para.47
[193] *Ibid*, paras.50-54
[194] *Ibid*, para.54
[195] C-362/14, Maximillian Schrems v. Data Protection Commissioner, Opinion of Advocate General Bot, para.89
[196] *Ibid*, para.65

levels could signify that Safe Harbor is, in fact, a failure with respect to Articles 7 and 8 of the Charter. In this instance of the judgment, the Court continues to tackle adequacy. In essence, the Court takes on an interesting interpretation of adequacy. It is clear that it is the Data Protection Directive that governs this, however, while it sets adequacy as a requirement, the Directive fails to explain the concept of adequate levels of protection as such. However, the Court does clarify, to a certain extent, what an "adequate level of protection" means: an adequate level of protection does not mean that the level of protection afforded to personal data in a third country is equal to the one it enjoys in the EU, but it is necessary to conduct an assessment of the levels of protection in that third country.[197] Furthermore, the Court added that the Commission is under obligation to conduct periodical checks in order to make sure that the adequate levels haven't deteriorated.[198]

The Court stressed out that interference with private life, as read from the Safe Harbor Decision Annexes I and IV, is permissible in a limited set of circumstances and it notes that the same principle applies to Safe Harbor, however, it emphasises that the interference is to be accompanied by a set of minimum safeguards as per the EU Charter. This is done so that "[t]he persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data."[199] This was not the first time that the Court was faced with this predicament. Namely, *Digital Rights Ireland [et al]* was the prior occasion where the Court was to examine a data protection mechanism from the point of view of the EU Charter. In *Digital Rights Ireland*, the Court laid down criteria that it later used in Schrems, such as the issue of lacking precise rules to regulate the scope of permissible interferences with fundamental rights, limits on data access and

[197] *Ibid*, paras.70-75
[198] *Ibid*, para.76
[199] *Ibid*, para.91; The Court refers to prior case law, notably *Digital Rights Ireland and Others*, C-293/12 and C-594/12, [2014] ECLI:EU:C:2014:238, paras.54-55

overall interference with fundamental rights.[200] All these were later used in the *Schrems* case as well.

In conclusion, the Court stressed out that national supervisory authorities are to examine claims arising from individuals which may challenge the compatibility of the Commission's adequacy findings, as read from Article 28 of the Directive, in the light of Article 8 of the EU Charter. As a result, the Court ruled that national supervisory authorities are to inspect and examine claims such as the one by Maximillian Schrems. Furthermore, the Court rendered Articles 1 and 3 of the Safe Harbor Decision invalid due to their failure to comply with the Article 25(6) of the Directive. Since these Articles are inseparable from the rest of the Decision, the whole Decision was thus rendered invalid by the Court.[201]

5.5 Analysis

The Court puts its foot down in this judgment, making it an important, pivotal moment for affording proper protection in data transfers to third countries. Schrems brought a two-fold challenge to the Court: the issue of personal data transfers from Facebook Ireland to its parent company Facebook (U.S.) encompassing a more broad issue of the level of protection afforded to personal data.[202] The Court addressed these by reading them in light of the EU Charter and the Data Protection Directive. The Court stresses the rule against fragmentation, i.e. that national courts cannot declare EU acts invalid, but also clarifies the role of the DPAs by emphasizing that they are still within their mandate to launch investigations on adequacy levels. The Court lays down the procedure of judicial remedies in cases such as *Schrems*, clarifying the role of the DPAs in the scheme of things.[203]

---

[200] C-293/12 and C-594/12, *Digital Rights Ireland and Others*, ECLI:EU:C:2014:238
[201] *Ibid*, para.107
[202] C-362/14, Maximillian Schrems v. Data Protection Commissioner, Opinion of Advocate General Bot, para.49
[203] See also, Fanny Coudert, *Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities*, (European Law Blog 2015) available at http://europeanlawblog.eu/?p=2931 [accessed 20 April 2016]

Maximillian Schrems targeted neither the Data Protection Directive nor the Safe Harbor Decision.[204] However, and quite importantly, in order to answer to Schrems's contests, the Court enters into a substantial discussion on the validity of the Safe Harbor decision, by means of positioning the Decision in the EU law structure. It juxtaposes the Decision with the Data Protection Directive and reads it in light of the EU Charter, placing tremendous focus on the value of affording protection to fundamental rights.

In this context, the Court takes up on the issue of the "adequate level of protection."[205] It takes an interpretative role after having seen that the Data Protection Directive fails to show the definition of the concept of an adequate level of protection. The Court interprets "adequate" as a standard that cannot be expected to be identical to the one provided in the EU. Thus, the standard meant by the term "adequate" is to be *essentially equivalent* to the one provided in the EU. For a standard to be essentially equivalent, it needs to provide a high level of protection in the substantial, normative sense. This is to be followed by periodic examinations[206] of the said standard in order to see whether the standard is still satisfactory. However commendable the *essentially equivalent* standard may be in theory, it is difficult to see it in practice. This is largely due to the fact that it is quite difficult to enforce it.

The Court reflected, albeit briefly, on Safe Harbor itself: it stressed that there is no need to analyse the content of its principles but it added that self-certification carries risks. By that, the Court means that self-certification can only be deemed reliable if there are efficient mechanisms of supervision in place. This would help target infringements and help maintain the adequacy

[204] C-362/14, Maximillian Schrems v. Data Protection Commissioner, Opinion of Advocate General Bot, para.121
[205] See also Steve Peers, *The party's over: EU data protection law after the Schrems Safe Harbour judgment* (EU Law Analysis 2015), available at http://eulawanalysis.blogspot.se/2015/10/the-partys-over-eu-data-protection-law.html [accessed 20 April 2016]
[206] On the adequacy decision, see C-362/14, Maximillian Schrems v. Data Protection Commissioner, Opinion of Advocate General Bot, paras.134-138

levels. One of the main flaws of Safe Harbor was exactly the lack of control mechanisms and guarantees necessary for maintaining (or attaining) the adequate level of protection.[207] This is followed by the flaws contained in the Safe Harbor Decision. Namely, the Safe Harbor Decision contains a set of derogations in Annex I, paragraph 4. This is also noted by the Advocate General in his Opinion.[208] The derogations mention limitations to adherence to Safe Harbor, such as *inter alia* matters of national security. However, because the language of the derogations is vague, the following happens: the U.S. implements those with a very wide margin, hence not limiting the scope and putting EU data subjects into a position of not being afforded a possibility of a proper remedy for such processing. This indicates a strong shortcoming of the Safe Harbor Decision and, by proxy, the Safe Harbor framework. This shortcoming could be fixed with an independent control mechanism, as the Advocate General notes.[209]

It is evident that the Court was very careful with this judgment. While the judgment is a step forward in strengthening the data protection mechanisms, it, at the same time, does not answer all questions on the manifold issues of data transfers. The intention is not to undervalue the Court's judgment, since it has had a daunting balancing task to execute with many interests to consider, mainly the interest of the fundamental right to privacy and data protection as well as the business aspect, both being quite important to the contemporary landscape of the world. The most pressing questions are whether we can realistically expect the new EU – U.S. Privacy Shield to address these issues in a proper manner? Does the U.S. fix all that led to the failure of Safe Harbor? The following chapter scrutinizes the Privacy Shield against the Safe Harbor framework while taking into consideration a wide range of circumstances surrounding the Privacy Shield's creation.

[207] *Ibid,* paras.141-144
[208] See *Ibid,* paras.161-168
[209] See *Ibid,* para.166

5.6 Summary of the Chapter

- *Maximillian Schrems v. Data Protection Commissioner* is a pivotal case that has redefined the standards of data protection in transatlantic data flows.
- The jurisprudence of CJEU in this case, and in *Digital Rights Ireland* has brought on criteria for interference with data, DPA competences, the importance of access to legal remedies, and the meaning of "adequate level of protection."
- The Court clarifies that launching investigations on adequacy levels is in the mandate of DPAs, meaning that examining claims such as the one made by Maximillian Schrems falls within their authority.
- In the Court's view, the "adequate level of protection" does not mean "equal level". It means *"essentially equivalent."*
- In order to be "essentially equivalent," a system needs to provide with a high level of protection in a normative sense.
- The Court emphasized that the self-certification system of Safe Harbor was its big weakness, along with the lack of review mechanisms.
- The language of derogations contained in Safe Harbor is vague, giving way for an [U.S.] implementation with a wide margin, limiting the scope of protection afforded to EU data subjects.
- The Court invalidates the Safe Harbor Decision, and by proxy, the Safe Harbor framework.

6 What now? The EU – U.S. Privacy Shield

6.1 Introduction

After Safe Harbor got struck down, a mild panic ensued with all parties involved. A new framework was necessary and it needed to be made quickly. The EU and the U.S. worked on a new set of principles and, as result, The EU – U.S. Privacy Shield was announced on 2 February 2016[210] and released on 29 February 2016.[211] The Shield is expected to enter into effect in June 2016. This chapter starts by briefly mentioning the role of the technology industry on the U.S. side of the situation. Namely, it briefly mentions the [U.S.] Judicial Redress Act, an undoubtedly important piece of legislation in the puzzle that is the transatlantic data flow. The chapter then continues to explore the Privacy Shield and attempts to analyse its content. This analysis is done through frequent references and comparisons to Safe Harbor as well as an overall critical approach for the purpose of revealing whether The EU – U.S. Privacy Shield actually fixes Safe Harbor's problems as well as if it ameliorates the state of the much mentioned adequate level of protection. The analysis is done principle by principle at first, and it continues with emphasizing the strong and the weak points of the Privacy Shield and concludes with an overall commentary of the document.

6.2 An erosion of trust and a restoration attempt

The Privacy Shield press release was followed by President Obama's signing of the Judicial Redress Act, and with the U.S. House of

[210] See, for example: Reuters, *New European, U.S. data transfer pact agreed* available at http://www.reuters.com/article/us-eu-dataprotection-usa-accord-idUSKCN0VB1RN [accessed 11 April 2016]
[211] The EU – U.S. Privacy Shield documents, available at https://iapp.org/resources/article/eu-u-s-privacy-shield-full-text/

Representatives passing it on 10 February 2016.[212] The Judicial Redress Act enables EU citizens to enforce their data protection rights in front of U.S. courts and it is an important tool for the Privacy Shield. This is due to the fact that the Judicial Redress Act will help the overall enforcement of the Privacy Shield.[213] What is interesting, however, is how the Judicial Redress Act was urged into existence. This is illustrative of the said panic that ensued after CJEU decided to invalidate the Safe Harbor Decision. Namely, tech industry giants urged to have the Judicial Redress Act passed through a letter addressed to the Speaker of the House John Boehner and to the Democratic Leader Nancy Pelosi of the U.S. House of Representatives. The letter[214] stresses and revolves around the decreasing trust in the U.S. followed by the Snowden revelations. The letter emphasizes the importance of rebuilding that trust in the U.S. government and the whole industry through enabling the EU citizens to enforce their rights in U.S. courtrooms.

6.3 The Shield itself

6.3.1 Introduction

The EU – U.S. Privacy Shield is essential for aiding the two systems overcome their differences for the purpose of their inextricable business and trade links. The Privacy Shield is envisaged to be an instrument of reliability when it comes to data transfers between the two systems and its purpose is to strengthen data protection in this particular EU – U.S. context. The EU DPAs have requested to review the Privacy Shield for a couple of months from the revelation of the text of the framework and the draft adequacy

[212] U.S. Judicial Redress Act, H.R.1428 available at https://www.gpo.gov/fdsys/pkg/BILLS-114hr1428enr/pdf/BILLS-114hr1428enr.pdf [accessed 11 April 2016], and https://www.congress.gov/bill/114th-congress/house-bill/1428 [accessed 11 April 2016], President Obama signed it into law on 24 February 2016.

[213] See more at *Hunton & Williams Privacy and Information Security Law Blog* https://www.huntonprivacyblog.com/2016/02/12/congress-passes-judicial-redress-act/ [accessed 11 April 2016]

[214] Letter to Speaker Boehner and Leader Pelosi, U.S. House of Representatives, available at http://www.itic.org/dotAsset/5/8/58eb178a-e926-4783-959b-60d9464248e6.pdf [accessed 11 April 2016]

decision,[215] and this thesis uses that opinion, as well as the draft adequacy decision in its analysis. The relevance of the Privacy Shield lies in one specific notion of it: its capacity or incapacity to provide for an *essentially adequate level* of protection, as elaborated upon *supra* in the Schrems case analysis.[216] An analysis conducted by Hogan Lovells, commissioned by the Information Technology Industry Council and DigitalEurope, emphasises the importance of reading the Privacy Shield Framework in conjunction with the new changes to U.S. domestic law such as *inter alia* the Presidential Policy Directive 28 and amendments to U.S. FISA.[217] According to this analysis, this is the way to properly assess the levels of protection that the Privacy Shield can provide. It is important to note that the Privacy Shield, as it is, is governed by the Data Protection Directive regime, until GDPR eventually comes to force in 2018 and replaces the Data Protection Directive altogether. This certainly makes the situation at hand that much more complex, seeing as the Privacy Shield is to be adopted under a regime that will no longer be relevant as of 2018, which means that the Shield needs to be adaptable to both the Data Protection Directive and the GDPR. This is likely to be done through the Privacy Shield review mechanism once the GDPR enters into force.

6.3.2 Analysis of the Privacy Shield

This sub-chapter focuses on the Privacy Shield and its content, rather than the surrounding circumstances of its negotiation process. It is envisaged to be a comprehensive analysis of the mechanism as a whole, including the Commission's draft adequacy decision and the Opinion of the Working Party 29, giving the reader a complete overview. The analysis begins with a principle-by-principle approach, where the Shield principles and their corresponding supplemental principles are scrutinized. Moreover, the analysis focuses on the ombudsperson mechanism and on the derogations

[215] Draft Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (2016)
[216] See *supra* chapter 5.4, the criteria by CJEU in both *Schrems* and *Digital Rights Ireland*
[217] Hogan Lovells, *Legal Analysis of the EU – U.S. Privacy Shield: an adequacy assessment by reference to the jurisprudence of the Court of Justice of the European Union* (2016), p.3

separately. Further on, the analysis morphs into a simpler presentation of the framework, by focusing on what can be seen as the Privacy Shield's strengths and weaknesses. This is done with the aim of giving a recap of the whole matter, seeing as the Privacy Shield documents are a large compilation of letters and documents.

6.3.2.1 The Privacy Shield, principle by principle

At the first glance, the structure of the Shield follows the structure of Safe Harbor, with Principles being the axis of each of these frameworks and their most evident distinctions being that Safe Harbor Principles were followed by Frequently Asked Questions (FAQs) whereas the Privacy Shield counts 7 Principles and 16 Supplemental Principles that together make up the Privacy Shield Framework. However, even at the first read, the content of the Privacy Shield comes across as a much more comprehensive document than Safe Harbor. This is largely due to the fact that most of the Principles of the framework have been significantly expanded, compared to the ones contained in Safe Harbor. However, the Privacy Shield is 16 years younger than Safe Harbor, and this is relevant for the analysis of the Shield. Namely, 16 years is quite a long time period in the world of technology and in terms of data, and this should be taken into account when analysing and possibly comparing the Privacy Shield to Safe Harbor.[218] What this note implies is that the Privacy Shield should not merely be a step better than Safe Harbor, but it should provide for a much better scope of protection fit for the necessities of today's world of increasing data mobility. In a sense, the Privacy Shield needs to be a method of 'future-proofing' data transfers – by being so comprehensive and encompassing that technological developments cannot derail it.

[218] See also Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf [accessed 18 April 2016]

To begin with, it is evident throughout the Privacy Shield that there is somewhat of a lack of consistency in the terminology used. This was also noticed by the WP29 in their opinion on the Privacy Shield.[219] Commendably, however, the Privacy Shield includes definitions of data subjects, controllers and processing in its introductory text,[220] something Safe Harbor evidently lacked.[221] These definitions correspond the Data Protection Directive in content,[222] but the Shield fails to implement the terminology of "processing" consistently throughout the document. *Exempli gratia*, in many places in the Shield terms like 'collecting' and 'using' data are used instead of the term 'processing' that is much more encompassing and accurate. WP29 described this as a risk for having "protection loopholes."[223]

It is worth looking at the content of the Shield principle by principle. This is where it can be helpful to remember the content of the Safe Harbor Principles, since the Shield is largely based on it, however significantly expanding and ameliorating the Safe Harbor content.[224] To start with, the *Notice* principle in the Privacy Shield is the same in its essence of disclosing information in privacy policies, however, the Notice principle in the Privacy Shield is much more detailed than it was in Safe Harbor, giving clarity to what exactly Notice entails. In thirteen points, the Notice principle of the Privacy Shield details on how the principle is to be complied with.[225] This includes details *inter alia* on the availability of independent dispute resolution bodies, including a hyperlink to the Privacy Shield list, the purpose of 'collecting and using' personal data and right of access.[226] This is where the term 'processing' is used in too restrictive a way, limiting its scope.

---

[219] *Ibid,* p.13
[220] The EU – U.S. Privacy Shield Principles, p.3
[221] Safe Harbor did have a Glossary, but it did not address terms like data subjects, controllers, processors etc.
[222] See supra, *Glossarium*
[223] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, p.13
[224] See supra, Chapter 4 *Safe Harbor, not so safe*
[225] See also Hogan Lovells, (2016), p.23
[226] The EU – U.S. Privacy Shield Principles, p.4

As far as the *Choice* principle goes, it remains mostly identical to the one in Safe Harbor, dealing with tackling opt-in for handling sensitive data, just like in Safe Harbor[227], as well as giving data subjects the opportunity to opt-out from disclosing their data to third parties or in cases where data is to be used in ways other than the previously stated purpose of its collection. However, while largely identical to the Safe Harbor Choice principle, the Privacy Shield also includes a clarification of a situation where disclosure of personal data is to be made to third parties. In this case, it is not required to provide the opt-out choice when the third party will be using the data on behalf and for the organisation and that is established via a contractual relationship between the two.[228] Furthermore, if one looks to the Supplemental Principles, there is an additional provision that gives the data subject the opportunity to extend the opt-out choice. Namely, a data subject can opt-out of having their data used for direct marketing.[229] Lastly, WP29 is concerned with the lack of definition of what is "materially different" from the purpose(s) that the data is processed for – and with good reason, seeing as this is very open to interpretation and could lead to challenging an organisation's compliance.[230]

The *Accountability for Onward Transfer Principle,* besides the name alteration also incorporates changes, compared to Safe Harbor, detailing the specificities of such transfers much better. In particular, this principle stresses the need to enter into a contract with a third party, which would bind the third party to treat the data pursuant to the limited purposes consistent with the subject's consent. In addition to that, the level of protection given by the third party must be at least identical to the one

[227] See supra, chapter 4 *Safe Harbor, not so safe*
[228] The EU – U.S. Privacy Shield Principles, p.5; and Hogan Lovells, (2016), p.23
[229] The EU – U.S. Privacy Shield Principles, Supplementary Principle 12(a), p.26; See also Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, p.13
[230] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision,* p.20

provided by the Privacy Shield.[231] In essence, there should not be any issues with this principle. However, WP29 has noted that it could benefit from adding another layer to it, by incorporating transfers to third countries into this principle – this way it will be possible to protect data flows much more comprehensively.[232] In addition to that, the corresponding Supplemental Principle[233] brings about one more concern. It says that intra-group transfers can rely on non-binding instruments, alongside BCRs. However, this is another potential loophole in the Shield, so the Shield would benefit from amending it to "legally binding instruments" instead.[234] *Security*, the fourth principle, remains largely unchanged from Safe Harbor and it prescribes that organisations have the obligation to take necessary measures to protect personal data from *inter alia* misuse or unauthorised access.

The fifth principle, *Data Integrity and Purpose Limitation* is significantly expanded compared to its corresponding principle in Safe Harbor. What it retains from Safe Harbor is the obligation of the organisation to take necessary steps to make sure that processing is done for the purposes it was intended for *ab initio*. The novelty in this principle is the obligation of the organisation to adhere to the Privacy Shield for the whole duration of its retention of personal data even after the organisation has left the Privacy Shield framework.[235] However, this principle could benefit from stronger language. Namely, it states "[p]ersonal information must be limited to the information that is *relevant* for the purposes of processing"[236] and it is likely that the word 'relevant' is too mild a term, and arguably quite open to interpretation. A possible replacement would be the term 'necessary.'[237]

---

[231] The EU – U.S. Privacy Shield, Annex II Principles, p.5-6; see also Hogan Lovells, (2016), p.24
[232] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision,* p.21
[233] The EU – U.S. Privacy Shield, Annex III, 10(b)
[234] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision,* p.22
[235] The EU – U.S. Privacy Shield, Annex II Principles, p.6; see also Hogan Lovells, (2016), p.24
[236] The EU – U.S. Privacy Shield, Annex II Principles, p.6, emphasis added
[237] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision,* p.23

Along the same note, corrections would be welcome to the following part: "to the extent necessary for those purposes, an organisation must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete and current."[238] This, as the WP29 stresses, would be stricter if "to the extent necessary for those purposes" would be removed, thus making sure that the data is indeed accurate and independent from processing purposes.[239] Lastly, this principle mentions processing that is "incompatible with the purposes" which, looked at together with "materially different" from the *Choice* principle, shows a certain discrepancy in the language and more importantly, without clarification as to what the meaning(s) of these terms are.[240]

Further on, the next principle, *Access*, remains essentially unchanged from the Safe Harbor version. Access refers to the data subjects having access to the personal data about them at an organisation that is processing that data. This means that organisations are to create a mechanism through which data subjects can access the data and be able to make corrections, amendments or delete the data where inaccurate or processed in violation of the Privacy Shield.[241] The principle of proportionality applies here: the expense of providing access is weighed against the actual risk to the data subject's privacy or violations of other subjects' rights, so the organisation can decline access in such circumstances.[242]

Lastly, the seventh principle, *Recourse, Enforcement and Liability* stands significantly developed compared to the corresponding principle in Safe Harbor. It provides with information on recourse mechanisms that are to be made available to data subjects, such as an arbitration mechanism and a larger role of the FTC in dispute resolution of compliance matters.[243] When

[238] The EU – U.S. Privacy Shield, Annex II Principles, p.6
[239] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision,* p.23
[240] *Ibid,* p.24
[241] The EU – U.S. Privacy Shield, Annex II Principles, p.6
[242] *Ibid*
[243] Hogan Lovells, (2016), p.24

it comes to individual redress mechanisms, it is worth looking at the Principle 7(a)(i) together with the Supplemental Principle 11(d). Namely, data subjects can raise complaints to the organisations themselves before going to an independent recourse mechanism – and the organisation is obliged to provide with a response within 45 days from receiving the complaint.[244] Subsequently, like in Safe Harbor, a Privacy Shield-certified organisation is obligated to have an independent recourse mechanism that has to be impartial, available and free for the complainant[245] and the organisation is to provide with information on how the procedure will look like, as well as a whole set of information that the organisation is obligated to provide, such as *inter alia* the link to the Privacy Shield's Principles, descriptions on how to file a complaint and information about the complaint mechanism being free for the complainant.[246]

Furthermore, in situations where claims still remain unresolved (i.e. "a residual claim"[247]), a data subject is entitled to use the arbitration model[248] contained in the Annex 2 of the Privacy Shield documents. Focus will be given to the particularities of the arbitration model in this instance, to give a general overview of its content. A data subject can use the Privacy Shield arbitration model only for purposes of the aforementioned residual claims, in situations where a Privacy Shield organisation has not adhered to the framework in relation to the data subject.[249] The arbitration panel is not to be used for adequacy assessments.[250] While initiating the arbitration process is an entirely voluntary action by the data subjects, the decision of the arbitration panel is binding on all parties involved and the data subject loses the option to discuss the same claim thereof, even in other forums, unless the remedy was not complete. In that case, the claim for damages remains, however, in courts, not with the arbitration panel.

[244] The EU – U.S. Privacy Shield, Annex II, III Supplemental Principle 11(d)(i), p.22
[245] Hogan Lovells, (2016), p.25
[246] The EU – U.S. Privacy Shield, Annex II, III Supplemental Principle 11.d. (i)(ii), p.22-23
[247] *Ibid*, Annex I Arbitration Model, (A)
[248] *Ibid*, Annex I Arbitration Model
[249] *Ibid*, Annex I Arbitration Model, (A)
[250] *Ibid*, (A)

The Shield could benefit from clearer language when it comes to arbitration procedures[251] since it says that a data subject can initiate arbitration by delivering a "Notice" to the Shield organisation. As mentioned *supra,* Notice is the name of the first Principle of the Privacy Shield and it signifies something very different from the "Notice" in the arbitration context. Perhaps a suitable substitution could be "Notification" in order to avoid confusion and be more accessible to data subjects who wish to file a claim. Lastly about the arbitration model, the procedure as a whole is foreseen to take place in the U.S. – the panel is based in the U.S. and so are the relevant courts. This can be problematic and European DPAs might want to be able to be of assistance to claimants in the arbitration setting.[252]

Furthermore, under the *Recourse, Enforcement and Liability* principle, organisations can opt to work together with the European DPAs for the aim of putting into force proper mechanisms for compliance with the Privacy Shield.[253] Neither the Privacy Shield nor the draft adequacy decision help clarify how this co-operation will function in practice, and that would be very helpful to have more information on.[254] The Recourse, Enforcement and Liability principle deals with compliance verification and consequences for non-compliance as well.[255] When it comes to compliance verification, detailed information is found in Supplemental Principle *Verification*, where self-assessment is one of the routes towards compliance verification, and the other is outside compliance reviews. Self-assessment entails assessing the organisation's privacy policy and information provided to individuals regarding avenues for redress.

[251] The EU – U.S. Privacy Shield, Annex 2, G.1.
[252] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision,* p.28
[253] The EU – U.S. Privacy Shield, Annex II, III.5
[254] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision,* p.27
[255] The EU – U.S. Privacy Shield, Annex II, 7.a(ii)(iii)

This self-assessment is done once a year and records of it must be kept and made available in the context of complaints. Self-assessment is not exactly the best way forward, since cases of incompliance could be come across too late and infringement of fundamental rights of data subjects could be vast by the time of discovery.[256] The DoC is to have a monitoring role in checking results of the self-assessments. However, the WP29 argues that this is not going to suffice and the DoC should take upon a bigger role than "mere document checking."[257]

Lastly and analogously with the self-assessment procedure, the content of verification is the same when it comes to outside compliance reviews, with the addition of a non-exhaustive list of ways to perform such reviews, e.g. *inter alia* through auditing.

The final points in the Recourse, Enforcement and Liability principle deals with remedies, or consequences for non-compliance and the role of the FTC, for which it is worth looking at Supplemental Principle 11 *Dispute Resolution and Enforcement* (e) Remedies and Sanctions and (f) FTC action. Essentially, remedies should consist of reversing the effects of non-compliance to the extent possible and ceasing processing a data subject's data if possible and appropriate.[258] When it comes to FTC action, it amounts to reviewing allegations of non-compliance from a number of different actors, such as the EU Member States, the DoC, and self-regulatory privacy organisations and independent dispute resolution bodies.[259] The FTC can, where necessary, prohibit the alleged incompliances through taking the matter to a federal district court.[260] This can aid transparency since this

[256] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision,* p.28
[257] *Ibid,* p.28, Draft Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (2016), §34
[258] The EU – U.S. Privacy Shield, Annex II, III Supplemental Principle 11.e (i), p.24
[259] *Ibid*, Annex II, III Supplemental Principle 11.f (i), p.24
[260] *Ibid*

instance would obligate the allegedly incompliant organisation to make compliance assessments publicly available.[261]

6.3.2.2 Ombudsperson mechanism

The ombudsperson mechanism regarding signals intelligence bases itself in the [U.S.] Presidential Policy Directive 28 and it is put in place to warrant an avenue for data subjects to file complaints. The purpose of the Ombudsperson mechanism is revealed in the letter from Secretary of State John Kerry, where he wrote that the Ombudsperson would be a contact point for EU authorities for submitting requests regarding U.S. signals intelligence practices.[262] This is done on behalf of EU data subjects. While the Ombudsperson is envisaged to work closely with officials and relevant department, it is also said to be independent from the Intelligence community.[263]

There is a prescribed set of conditions for a EU data subject's request to be complete,[264] however that is not the most important part of this mechanism. Namely, upon receiving a complete request, the Ombudsperson will respond that the process has been properly investigated and that the safeguards under U.S. law have been complied with. In case they have not been complied with, the Ombudsperson will inform of the remedies used for such incompliance. Essentially, the Ombudsperson will *neither confirm nor deny* whether the EU data subject has been a subject of surveillance and it will not detail into which remedy has been used in the data subject's case.[265] The Ombudsperson will only tackle requests dealing specifically with signals

[261] *Ibid*
[262] The EU – U.S. Privacy Shield, Letter from U.S. Secretary of State John Kerry
[263] The EU – U.S. Privacy Shield, Annex A: Ombudsperson Mechanism, 1. The Privacy Shield Ombudsperson
[264] *Ibid,*, 3. Submitting requests
[265] *Ibid,*, 4. Commitments to Communicate with Submitting EU Individual Complaint Handling Body (e)

intelligence.[266] In addition, the Ombudsperson will have a scope slightly larger than just the Privacy Shield. Namely, the Ombudsperson will accept requests by data subjects whose data has been transferred through SCCs or BCRs.

In conclusion, the Ombudsperson mechanism is most certainly a welcome mechanism for EU data subjects. It has potential to be a relevant actor in the whole protection scheme. Alas, the Ombudsperson does not seem to be having sufficient authority, mandate or even independency.[267] It is also unclear what happens if a data subject is dissatisfied with the response given by the Ombudsperson.

6.3.2.3 Public security limitations

In principle, interference with fundamental rights is possible for legitimate reasons, such as law enforcement or national security matters. This is grounded in the limitations of the fundamental rights as well as the jurisprudence of both the CJEU and ECtHR and it is emphasised in the European Essential Guidelines compiled by the WP29.[268] The Commission's draft adequacy decision tackles the mechanisms existing in the U.S. law dealing with public security, an issue that was the culprit behind the downfall of Safe Harbor. The relevant Privacy Shield documents are the Office of the Director of National Intelligence (ODNI) Letter, Department of Justice Letter (DoJ) and the Ombudsperson Letter where the U.S. provides a deeper insight into its legislation dealing with public security issues.

---

[266] Hogan Lovells, *Legal Analysis of the EU – U.S. Privacy Shield: an adequacy assessment by reference to the jurisprudence of the Court of Justice of the European Union* (2016), p.34

[267] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision,* p.4

[268] See Working Party 29, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data *(European Essential Guarantees)*, WP 237

In those letters, the U.S. elaborates on how it has fortified the framework compared to the one it had before Safe Harbor got debunked – with instruments such as the Judicial Redress Act or the Presidential Policy Directive 28. Characteristics of the PPD-28 are elaborated upon in the ODNI Letter, with an emphasis on collection limitations and existing safeguards. However extensive the elaborations on these safeguards are, they remain unclear as to the subjects this legal framework refers to. Namely, and as the WP29 notes, it is unclear that these safeguards would protect non-U.S. data subjects.[269] Furthermore, the DoJ letter deals with specificities of the Fourth Amendment of the U.S. Constitution and the "investigative tools" that help authorities gain access to various types of data under the umbrella of public interest and safety, as well as criminal proceedings. In addition, the draft adequacy decision notes that the Fourth Amendment applies only to U.S. citizens and residents, but it also mentions that EU data subjects can still benefit from the protections contained in the Fourth Amendment through the fact that U.S.-operating data controllers and/or processors are subject to the Fourth Amendment.[270]

However, it is doubtful that this type of "indirect protection" is effective in reality seeing that it is practically impossible to challenge the investigative tools or have access to remedies.[271] Lastly, while there are a number of avenues for remedies available to data subjects for Privacy Shield breaches, there seems to be no accessible, available remedy avenue in the situations of interferences done by the U.S. authorities, even if one takes into account the existence of the Judicial Redress Act. WP29 seems to take a strong stance that this is not an adequate way of dealing with this aspect of the interference with fundamental rights.[272]

---

[269] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, p.54
[270] Draft Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (2016), §108; Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, p.55
[271] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, p.55
[272] *Ibid*, p.56

6.3.2.4 Adequate level of protection?

As mentioned *supra* in the Schrems case study, CJEU has put Safe Harbor to a test of the adequate level of protection in order to determine whether it, in fact, provides such an adequate level for the transferred data. Safe Harbor underperformed on the test, and it can be useful to examine whether Privacy Shield would have a better result. This can be done through looking at the criteria set by CJEU that, ideally, the Privacy Shield should fulfil in order for it to be considered a proper framework for EU – U.S. data transfers. Firstly, the Court stressed out the importance and mandate of DPAs, their monitoring as well as their investigation in relation to complaints. Judging by the Privacy Shield Supplemental Principle 5, the role of DPAs seems to be satisfactory.[273] This is further confirmed in the draft adequacy decision.[274] Secondly, the Privacy Shield will be subject to periodic review, which satisfies the Court's criterion. This way, the levels of protection will be verified on a regular basis.[275] Thirdly, when it comes to interferences with fundamental rights, this is where it could prove to be unlikely that the Privacy Shield provides the required level of protection. The biggest criticism by the WP29 was directed to the part of the limitations that allow the U.S. to conduct bulk collection of data.[276] As noted *supra,* there is still space for unjustified, unlawful interference in the present-day content of the Shield. One may also want to take into account the aforementioned changes in U.S. domestic law – especially considering these changes had not been in place at the time of the CJEU judgment in the *Schrems* case.[277] When it comes to interference, the problematic part extends itself into the criterion of

[273] See also Hogan Lovells, (2016), p.41
[274] Draft Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (2016), §44
[275] See Chapter 5. Maximillian Schrems v. Data Protection Commissioner, *supra*; Draft Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (2016), Art 4; Hogan Lovells, (2016), p.42
[276] See Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*
[277] Hogan Lovells, (2016), p.42-43

proportionality, and it is questionable whether the collection limitations of signals intelligence as described in the ODNI Letter fulfil this criterion in a proper manner.[278] When it comes to interference, proportionality alone will not do: it is important that this interference is necessary, that it has a specific purpose and that it is lawful. When looking at the Privacy Shield as a whole, it could be construed that this is satisfactory, but it is not very evident in the sense that it is bulletproof, so to speak.

On the contrary, it seems as it could be amended to fulfil these criteria much better. It is also important to remember that CJEU did not even consider the Safe Harbor Principles at all, because it focused on the Safe Harbor Decision which ultimately means that the Privacy Shield draft adequacy decision needs to be very robust in order to be strong enough should it be challenged in front of CJEU. Lastly, CJEU emphasized the necessity of having available and accessible redress mechanisms in place. Safe Harbor did not have this, and the Privacy Shield certainly fixes that mistake. However, this is met with criticism as well, seeing as the Privacy Shield is seen as giving too many redress avenues, as elaborated upon *infra* in the following sub-chapter. Overall, the Privacy Shield is more capable of fulfilling the CJEU criteria of adequacy, but it is questionable whether it actually does so without problems. The following sub-chapter deals with the Privacy Shield's overall commentary.

6.4 Commentary

After having gone through the Privacy Shield principle-by-principle all the while relying on the Privacy Shield decision, the WP29 Opinion and the Hogan Lovells legal analysis and drawing comparisons to Safe Harbor, it can be useful to recapitulate on the main takeaways from analysing the extensive Privacy Shield documents. In sum, the Privacy Shield has several weaknesses and strengths. When it comes to its strengths, those can be considered the following:

[278] The EU – U.S. Privacy Shield Principles, ODNI Letter, p.3

The regular compliance review system, since it will provide for much better control and oversight of compliance compared to its predecessor Safe Harbor. This review system will be very important when GDPR enters into force, because the GDPR is a very comprehensive package that expands the understanding of data protection on many levels, and the Privacy Shield will need to be reviewed so as to fit the GDPR. Furthermore, it is quite commendable that the basic definitions of personal data, data processing, who are controllers etc are included in the beginning of the Privacy Shield documents.[279] This gives more clarity to the terms in the context of the Privacy Shield. Moreover, the Privacy Shield seems to place significant focus on organisations to have publicly available privacy policies and a hyperlink to the Privacy Shield itself, which increases accessibility to information and transparency. The Privacy Shield seems to place many more obligations on organisations than Safe Harbor did, and this can be seen as its strength because it impacts compliance on a large scale. Lastly, compared to Safe Harbor, the Privacy Shield offers avenues for redress, which is something that is utterly necessary in a framework like this one.

Although the redress avenues are a strong point of the Shield, they represent a weak point at the same time. Namely, the redress mechanisms are far too many; they are, to a large extent, incomprehensible and fail to convey the proper way to make use of them. In addition to that, the redress routes are largely placed within the U.S., which can prove to be problematic. Furthermore on the side of the weaknesses of the Privacy Shield: there is a significant lack of clarity and consistency in the Privacy Shield. Most such instances were already pointed out in the principle-by-principle analysis *supra*, such as the concept of "processing" versus "collecting" and "using" and other inconsistencies. Along the same line, the Privacy Shield would significantly benefit from implementing stronger language in several instances noted *supra,* for the purpose of minimizing the risk of having loopholes. Furthermore, and still relating to the lack of clarity: it seems

[279] See The EU – U.S. Privacy Shield Principles, p.3

unclear to whom the Privacy Shield applies – is it solely EU citizens, or is it EU residents?[280] This is quite an important question, and providing an answer to it should be prioritized. Additionally, the question of onward transfers in the Privacy Shield as it is right now is limited to transfers to third parties, but it would be preferable to be expanded to third countries as well.

Furthermore, while the establishment of an Ombudsperson is a welcome development, it seems as if the Ombudsperson does not really have a lot of authority, which makes it fall back on the weak side of the Privacy Shield. Moreover, the legitimate interferences with fundamental rights as done by the U.S. authorities seem to not be addressing the issue adequately, and do not seem to offer sufficient safeguards to EU data subjects. Here we can see yet another confounding instance of the use of unclear language with the word "access." Namely, and as WP29 points out, the word "access" is used in the Privacy Shield principles to describe access of data subjects to their personal data.[281] Subsequently, the word "access" is then used to refer to U.S. authorities getting a hold of personal data for national security purposes.

Architecturally, the Privacy Shield documents are not very intuitive. It takes a lot of time to go through the material due to its strange structure. One of the ways to remedy this is to alter the structure of the Supplemental Principles so that they intuitively follow the order in which their corresponding Principles are set. It is difficult to imagine a data subject not well versed in *legalese* reading the Privacy Shield and actually understanding their rights and available redress mechanisms. This will be the result of (hyper)linking the Privacy Shield to an organisation's privacy policy, which is commendable, but in order for it to be effective and fulfil its purpose, it seems like it could benefit from a better architecture. Aiding

[280] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision,* p.14
[281] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision,* p.13

the confounding aspect of the structure, it looks somewhat unorthodox to see so many letters being an integral component and a representation of legality for a framework like this. The Commission's draft adequacy decision considers that the U.S. is legally bound by the letters in the Privacy Shield. However, it is questionable whether these letters can have such binding authority. When it comes to the adequacy of the level of protection afforded by the Privacy Shield, it is a question that still remains in the air. In line with the criticism *supra*, the Privacy Shield could also use more clarity in its provisions to achieve proper protection levels so that it would not relive the fate of Safe Harbor.

In conclusion, the Privacy Shield is not flawless, and it is certainly an improvement from Safe Harbor. A framework of its kind must be put in place, because it is simply becoming impossible to live in a globalised, Internet-run world without migrating data all the time. Failing to have a framework such as the Privacy Shield will create panic with companies who rely on data transfers quite heavily. Moreover, it is perhaps important to keep in mind that a framework with such a big role in transatlantic trade is unlikely to ever be perfect due to the fact that its task is to be a bridge between two very different approaches to data protection. The biggest challenge will be its enforcement – as is the case with most cross-border data flow regulation, seeing as it is very difficult to monitor compliance when cross-border data transfers take up on the volume they usually do.[282] Regardless of that, the Privacy Shield needs to be as good as it possibly can be – and its current state has not yet reached full potential. It makes little sense to speculate on how things will work in practice, or if they will work at all. Despite the Shield's various drawbacks mentioned *supra*, it is very unlikely that renegotiations would start, even though the possibility exists.

Hence, the Privacy Shield will probably be effective soon, and then it remains to be seen how it functions as a framework. Lastly, as mentioned

[282] Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford University Press (2013), p.144

supra, the Privacy Shield has a review mechanism that is arguably one of its most important features, giving the Shield a chance to get better and keep an adequate level of protection. Lastly, it remains to be seen whether the Privacy Shield will be challenged in court and end up having the same fate as Safe Harbor.

6.5 The road forward

As thoroughly discussed *supra*, the deliberation of WP29 ended with a negative opinion on the levels of protection provided by the Privacy Shield.[283] The opinion of the DPAs is not an obligatory one, but it is expected to resonate within the European Community. It is in this moment that we can, once more, witness the involvement of the tech industry in the whole matter. The industry, along with consumer organisations, are urging to have the Privacy Shield adopted swiftly in order to cease the state of legal uncertainty over transatlantic data transfers all the while emphasizing the importance of the EU – U.S. partnership and the digital single market.[284] The WP29 opinion on the Privacy Shield could theoretically trigger renegotiations, although the chances that the EU will be willing to enter renegotiations are small. Renegotiations would undoubtedly bring about a new wave of panic within the industry, and it would be somewhat strange behaviour on behalf of the Commission, seeing that its reasoning for not suspending Safe Harbor in 2013 was taking into account the reasons of adverse effects that suspension would have on businesses.[285]

---

[283] Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf [accessed 18 April 2016]

[284] See, for example: John Frank, Vice President EU Government Affairs, Microsoft, letter http://blogs.microsoft.com/eupolicy/2016/04/11/microsofts-commitments-including-dpa-cooperation-under-the-eu-u-s-privacy-shield/; John Higgins, DigitalEurope http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2151&PortalId=0&TabId=353; BEUC The European Consumer Organisation http://www.beuc.eu/publications/beuc-x-2016-035_mgo_letter_on_eu-us_privacy_shield_proposal_to_ms_falque-pierrotin.pdf [all accessed 18 April 2016]

[285] Hogan Lovells, (2016), p.9

What remains to be done for the Privacy Shield to be in effect is for approval of the Article 31 Committee.[286] The Committee is established via the Data Protection Directive and it is made up from representatives of Member States with the mandate to deliver opinions on the drafts of the relevant decisions,[287] which would in this case be the draft adequacy decision on the Privacy Shield. After that, it is solely up to the European Commission to vote (or not) for the adoption of the Privacy Shield. The European Parliament will not have a say[288] but some MEPs have been trying to organise a plenary vote on it.[289]

6.6 Summary of the Chapter

- The EU – U.S. Privacy Shield is crucial to levelling the playing field between the two systems, but the Privacy Shield documents and the draft adequacy decision were not well received by WP29.
- Stronger oversight and review mechanisms are in place, as well as several redress mechanisms and an ombudsperson mechanism.
- However, the redress mechanisms may be too many and the ombudsperson mechanism does not seem to have a lot of authority and independence.
- The U.S. has amended its domestic laws with regard to interferences with fundamental rights, but there is room for further delimiting the possibilities of bulk collection in the Privacy Shield.
- The Privacy Shield could benefit from greater clarity and consistency. Structurally, it could benefit from improvements for a more intuitive architecture.
- It is still questionable whether the Privacy Shield provides an adequate level of protection.

[286] See IAPP, *The Next 4 steps for the Privacy Shield*, available at https://iapp.org/news/a/the-next-four-steps-for-the-privacy-shield/ [accessed 27 April 2016]
[287] Data Protection Directive, Article 31
[288] See Ars Technica, *EU data watchdogs: Privacy Shield needs fixes*, available at: http://arstechnica.com/tech-policy/2016/04/privacy-shield-us-surveillance-eu-article-29-working-party/ [accessed 27 April 2016]
[289] See EurActiv, *MEPs battle to get their vote on Privacy Shield*, [accessed 29 April 2016]

7 Conclusion

This thesis has an objective of illustrating and analyzing the current data protection mechanisms all the while taking into consideration the recently refuted Safe Harbor framework, the *Schrems* case that caused it and the upcoming Privacy Shield framework. All of this is looked at through the fundamental rights lens. This thesis attempts to answer the following questions:

Are data protection and privacy one and the same? How does the right to data protection balance against other fundamental rights, such as the freedom to conduct business? What was the impact of the *Schrems* case – aside from striking down Safe Harbor? In relation to that, is the EU – U.S. Privacy Shield a viable solution that provides adequate protection?

At its core, the thesis helps divulge the distinction between privacy and data protection, for the purpose of laying the groundwork of understanding the relationship between the two. In essence, privacy is regarded as an age-old notion stemming from one of the most instinctive human needs that accomplished a codified status of a fundamental right at the very advent of human rights.

One of the aspects of privacy is autonomy, or control over information about oneself – which is where data protection comes into play. It is known that data collection has existed for a very long time, but it has changed its *modus operandi* with the emergence of the Internet. It has suddenly become ubiquitous, all too easy to perform and it gained an economic value to it – a facet that privacy, as a right, was not envisaged having. As a result, personal data has become challenging to protect. The issue at hand is whether data protection can be equalized with privacy, or not. Privacy is imagined as a wide concept, and most importantly, a concept that is very dependent on

one's own perception of it, and that it is very difficult to contain in a specific definition.

However, one obvious distinction appears: privacy encompasses personal space, private life, family life and is subject to different interpretations, whereas data protection encompasses personal data flowing online, hence, it 'only'[290] addresses an individual's online presence in a way that ought to protect that individual from unjustified and unlawful interferences. In the course of examining the relevant legal framework a partial answer to the said distinction problem arises: the one where most international and regional human rights law instruments have been created years, if not decades, before data protection came to be in the way we see it today. This instantly points to the reason why this distinction is so challenging to make, there is hardly a way to make a clear cut between privacy and data protection simply due to the fact that most relevant human rights instruments interpret the right to privacy as encompassing the right to data protection as well, such as, *exempli gratia*, the ECHR. This is repeatedly proven through court jurisprudence as well. Data protection had started developing in Europe with the OECD Privacy Principles, followed by the Council of Europe Convention 108 and the EU Data Protection Directive. The legal instrument that places data protection and privacy into two separate fundamental rights is the EU Charter, a relatively young instrument. However, even in the CJEU jurisprudence, the two are usually looked at in conjunction, hence blurring the lines once again. Over the course of the last few years, data protection has gained a lot of momentum and has become central to many discussions on the adequacy of protection mechanisms.

One such discussion is the one this thesis has dealt with, specifically pertaining to data protection in the context of cross-border data transfers. Cross-border data transfers are essential to business and trade and it is

[290] "Only" is slightly paradoxical in this context, seeing as an online presence of a single individual can be a very broad collection of information

difficult to imagine the global economy without it. They happen on a daily basis in incomprehensible volumes all around the globe. This brings about issues concerning the safety of such data flows and the accessibility to redress mechanisms if data has been breached. Hence, while it is important to continue with such data flows for economic reasons, it is equally important that these data flows provide protection against unlawful access or any sort of interference with personal data. In the EU legal framework, the most valuable instrument in this context is the Data Protection Directive (and, in two years time, the General Data Protection Regulation) that regulates data transfers to third countries and it prescribes that EU data must be treated with an adequate level of protection while being transferred to, or processed in, third countries. This is not easy to monitor and it can easily be said that jurisdictional matters play little to no role in the Internet world, which is why there has been so much discussion on these issues in the past years. In the transatlantic context, between the EU and the U.S., the discussion reached a new level after Edward Snowden's revelations of the existence and scope of the PRISM Programme.

Furthermore, this thesis posed other questions that were equally exciting to find answers to. Namely, the examination of the question of the balance between the right to data protection against other fundamental rights such as the freedom to conduct business led to interesting case law. Seeing that the volume of e-commerce is gargantuan, it was important to examine the interplay between fundamental rights, such as the one between the right to data protection with the freedom to conduct business. A select number of cases were used to illustrate that the right to data protection has an interesting impact when juxtaposed with other fundamental rights and freedoms. Cases like *Promusicae, Scarlet Extended* and *Netlog* all dealt with this balance. They dealt particularly with the right to [intellectual] property on the one hand and freedom to conduct business and the right to data protection on the other. CJEU made a firm stance in these cases, judging in favour of the latter. This raises a question: how frequently will freedom to conduct business be used this way? A fairly reasonable estimate

is that it might be used more and more often indeed, seeing as it is increasingly more intertwined with the right to data protection.

Going back to transatlantic data transfers, the undoubtedly important partnership between the EU and the U.S. gave way for a self-certification framework called Safe Harbor in 2000. The aim of Safe Harbor was to give the "adequate level of protection" prescribed by the Data Protection Directive. The economic benefits of safe data transfers were the main motivator for Safe Harbor. Safe Harbor was created to perform a very difficult task – to make a compromise between two substantially different legal systems, especially with regards to privacy and data protection. As expected, Safe Harbor was a flawed framework from the very beginning. It relied heavily on self-certification, provided no redress mechanisms and was not properly monitored, hence becoming easily challengeable in court, which is exactly what happened with the *Schrems* case.

In the *Schrems* case, in front of the Grand Chamber of the CJEU, the Court addressed a set of questions. Namely, it was asked to interpret Articles 25(6) and 28 of the Data Protection Directive in the light of Articles 7 and 8 of the EU Charter and to the validity of the Safe Harbor Decision. In addition to that, the Court also investigated the role and authority of the DPAs when it comes to addressing claims such as the one of Maximillian Schrems. In its deliberation, the Court clarified the role of DPAs by explaining that they cannot go against decisions of the Commission, but they can and should investigate adequacy levels.

Furthermore, the Court enters into an interpretation of the Safe Harbor Decision by reading it in the light of the EU Charter and juxtaposing it with the Data Protection Directive, hence focusing on the importance of respecting and protecting fundamental rights. Hence, it is safe to say that aside from striking down Safe Harbor, the case impacted the whole cross-border data transfers discussion with one interesting consideration: the one of adequacy. This is an important moment because the Court clarified that

the Data Protection Directive fails to elaborate on the concept of an "adequate level of protection" so the Court makes its own estimation of what that entails. Namely, the Court stressed that an "adequate level" cannot be an "equal level" but must be "essentially equivalent" instead, meaning that it provides a high level of protection in the normative sense. This is essential for understanding what the Directive really prescribes; however, it is difficult to understand how this will work in practice. The Court strikes down the Safe Harbor Decision in its judgment, and by proxy, the whole Safe Harbor framework due to a failure to comply with Article 25(6) of the Data Protection Directive.

Following the Court's decision in *Schrems*, and in absence of a functioning framework, alternative modes of protection were in place: the Standard Contractual Clauses and the Binding Corporate Rules. This 'framework vacuum' leads us to the final question: now that the EU – U.S. Privacy Shield is published and scheduled to be in effect in June 2016, is it a viable solution that provides adequate protection?

The Privacy Shield Principles draw inspiration from Safe Harbor in terms of structure. When it comes to content, a first look at the Privacy Shield reveals a similarity with Safe Harbor, but it immediately gives off an impression of a higher comprehensiveness compared to its predecessor. To begin with, the Privacy Shield offers definitions of crucial terms, such as *data subject*, *data controller* and *processing* which indicates intent of clarity. However, the Privacy Shield fails to project clarity throughout the whole document in several instances of unclear text that can prove to be "protection loopholes," as the WP29 called them.

Overall, the Privacy Shield is not easy to navigate, and this can prove to be an issue both for data subjects and for businesses that are to adhere to the Privacy Shield. This can be considered a big flaw of the whole framework, simply because it gives way for mistakes and incompliance. On the other hand, the Privacy Shield learns from the mistakes made with Safe Harbor

and establishes an Ombudsperson mechanism as well as provides with various redress avenues. Both of these improvements are welcome, however, at the same time, they represent significant flaws of the Privacy Shield since the Ombudsperson mechanism seems to not have much authority or independence, and the redress avenues are far too many and far too difficult to navigate. The Privacy Shield also implements a review mechanism, something that will prove to be vital in its upkeep.

In *Schrems*, the Court examined Safe Harbor based on a set of criteria. For one, the role of DPAs seems to be clarified in the Privacy Shield documents. The second criterion was that a transatlantic framework ought to have a review mechanism – a criterion the Shield satisfies. The third criterion tackles the interferences with fundamental rights and it is manifold – the interferences ought to be provided by law, proportionate, strictly necessary, limited and must provide minimum safeguards and guarantees for protection against personal data abuse or misuse. This criterion is where the Privacy Shield remains doubtful in its capacity of fulfilling it. This is largely due to public security limitations, since they seem to leave space for interferences that would fail to comply with the Court's criterion for interferences. Despite its flaws and drawbacks, the Privacy Shield is a much anticipated, very welcome framework in the business world. It is very unlikely that its flaws would trigger renegotiations; hence it is safe to assume that the Privacy Shield will, indeed, enter into effect in June 2016. It remains to be seen whether it gets challenged in court and whether the review mechanism will work as intended.

Bibliography

Books

Cullen International S.A., *A business guide to changes in European data protection legislation*, (Kluwer Law International 1999)

Edwards L, Waelde C, *Law & the Internet, a framework for electronic commerce*, (Hart Publishing 2000)

Edwards L, Waelde C, *Law and the Internet, third edition*, (Hart Publishing 2009)

Fuster GG, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Law,

Governance and Technology Series 16, (Springer International Publishing 2014)

Geiger C (Ed.), *Research Handbook on Human Rights and Intellectual Property*, (Edward Elgar Publishing 2015)

Karim Benyekhlef, *Les normes internationales de protection des données personnelles et l'autoroute de l'information*, in Les Journées Maximilien-Caron, Le respect de la vie privée dans l'entreprise, Montréal, Éd. Thémis (1996)

Kevan T and McGrath P, *E-Mail, the Internet and the Law, Essential knowledge for safer surfing*, (EMIS Professional Publishing 2001)

Klang M, Murray A (ed.), *Human Rights in the Digital Age*, (Glasshouse Press, Cavendish Publishing 2005)

Kuner C, *Transborder Data Flows and Data Privacy Law*, (Oxford University Press 2013)

Lessig L, *Code version 2.0*, (Basic Books 2006)

Lindskoug P, Maunsbach U, Millqvist G, Samuelsson P, Vogel H-H (eds.), *Essays in honor of Michael Bogdan*, (Juristförlaget i Lund 2013)

Mayer-Schönberger V, 'Generational Development of Data Protection in Europe', Agre PE and Rotenberg M (eds.), *Technology and Privacy: The New Landscape*, (MIT Press 1997)

Murray A, *Information Technology Law, second edition*, (Oxford University Press 2013)

Nugter A.C.M., *Transborder Flow of Personal Data within the EC: A comparative analysis of the privacy statutes of the Federal Republic of Germany, France, the United Kingdom and the Netherlands and their impact on the private sector*, (Kluwer Law and Taxation Publishers 1990)

Peers S, Hervey T, Kenner J, Ward A (eds.), *The EU Charter of Fundamental Rights, A Commentary*, (Hart Publishing 2014)

Rowland D, Kohl U and Charlesworth A, *Information Technology Law, fourth edition*, (Routledge 2012)

Trzaskowski J, Savin A, Lundqvist B, Lindskoug P, *Introduction to EU Internet Law*, (Ex Tuto Publishing 2015)

Westin AF, *Privacy and Freedom,* (Bodley Head 1967)
Westin AF, *Privacy And Freedom,* Atheneum (1970)

Articles

Blume P, *It's Time For Tomorrow: EU Data Protection Reform And The Internet,* Journal of Internet Law, (Aspen Publishers Inc., February 2015)
Connoly C, *The US Safe Harbor - Fact or Fiction?* (Galexia 2008)
Juhi T, *"NSA's Prism Program and the New EU Privacy Regulation: Why U.S. Companies with a Presence in the EU Could Be in Trouble,"* (The American University Business Law Review 3.2 2014) p. 371-389
Kuner C, *Extraterritoriality and regulation of international data transfers in EU data protection law,* International Data Privacy Law, Vol. 5, No. 4, (Oxford University Journals 2015) p. 235-245
Leathers DR, *Giving Bite To The EU-U.S. Data Privacy Safe Harbor: Model Solutions For Effective Enforcement*, (Case Western Reserve Journal of International Law, vol. 41 2009), p. 193-242
Loidean NN Dr., *The End Of Safe Harbor: Implications For EU Digital Privacy And Data Protection Law,* (Journal of Internet Law 2016) Vol. 19 Issue 8, p.8-14
Maunsbach U, 'Here Comes The Internet, And Why It Matters: Private International Law in Transition', in Lindskoug P, Maunsbach U, Millqvist G, Samuelsson P, Vogel H-H (eds.), *Essays in honor of Michael Bogdan*, (Juristförlaget i Lund 2013), p. 293-307
Mills JL, *Privacy, The Lost Right*, (Oxford University Press 2008)
Reding V, *The upcoming data protection reform for the European Union*, International Data Privacy Law, Vol. 1, No. 1 (Oxford University Journals 2011), p. 3-5
Rodotà S, *Data protection as a fundamental right*; eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Terwagne CD, Nouwt S, *Reinventing Data Protection?* (Springer 2009)
Svantesson DJB, *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation*, International Data Privacy Law,Vol. 5, No. 4, (Oxford University Journals 2015 Symposium Article) p. 226-234
Warren S, Brandeis L, *The right to privacy* (4 Harvard Law Review 1890)
Weiss MA, Archick K, *The EU – U.S. Safe Harbor Agreement on Personal Data Privacy: In brief*, (Congressional Research Service 2015)

News articles and blogs

Ars Technica, *EU data watchdogs: Privacy Shield needs fixes*, available at: http://arstechnica.com/tech-policy/2016/04/privacy-shield-us-surveillance-eu-article-29-working-party/ [accessed 27 April 2016]

Coudert F, *Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities*, (European Law Blog 2015) available at http://europeanlawblog.eu/?p=2931 [accessed 20 April 2016]

EurActiv, *MEPs battle to get their vote on Privacy Shield*, available at: https://www.euractiv.com/section/digital/news/meps-battle-to-get-their-vote-on-privacy-shield/?mkt_tok=eyJpIjoiWmpNMk0yWTFZVGswWmpNeiIsInQiOiJua2RmK1YrVStHVFpDV0VGNlJZRjhyd1ZjUnYrbVMyQXBNbWJqd3ozOGdEc3pLNUp2T28rR0s1VzdBTEhYU3djQStpekJYWDY4Z0NoRTd5VE1yYmtKYWJSZkdpWGU1N3lkNTdzc0VLU3hGQT0ifQ%3D%3D [accessed 29 April 2016]

Farrell H and Newman A, *The Transatlantic Data War, Europe Fights Back Against the USA*, (Foreign Affairs 2016) <https://www.foreignaffairs.com/articles/united-states/2015-12-14/transatlantic-data-war> [accessed 16 May 2016]

Hasty R, Dr Nagel TW and Subjally M, White & Case, *Data Protection Law in the U.S.A.*, Advocates for International Development (2013), available at http://www.a4id.org/sites/default/files/user/Data%20Protection%20Law%20in%20the%20USA_0.pdf [accessed 17 March 2016]

Hogan Lovells *Chronicle of Data Protection, Privacy & Information Security News & Trends*, available at <http://www.hldataprotection.com/2016/01/articles/health-privacy-hipaa/the-final-gdpr-text-and-what-it-will-mean-for-health-data/> [accessed 4 May 2016]

Hill K, *Google Challenges Government Gag Order On National Security Requests*, Forbes.com, (18th June 2013), available at <http://www.forbes.com/sites/kashmirhill/2013/06/18/google-challenges-government-gag-order-on-national-security-requests/#2e34e9e935a3> [accessed 4 April 2016]

Hunton & Williams Privacy and Information Security Law Blog https://www.huntonprivacyblog.com/2016/02/12/congress-passes-judicial-redress-act/ [accessed 11 April 2016]

International Association of Privacy Professionals (IAPP) Top 10 Operational Impacts of the GDPR <https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr> [accessed 18 April 2016]

Lee TB, *Here's everything we know about PRISM to date*, The Washington Post, (12th June 2013), available at <https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/> [accessed 4 April 2016]

Peers S, *The party's over: EU data protection law after the Schrems Safe Harbour judgment* (EU Law Analysis 2015), available at

http://eulawanalysis.blogspot.se/2015/10/the-partys-over-eu-data-protection-law.html [accessed 20 April 2016]

Reuters, *New European, U.S. data transfer pact agreed* available at http://www.reuters.com/article/us-eu-dataprotection-usa-accord-idUSKCN0VB1RN [accessed 11 April 2016]

International Association of Privacy Professionals (IAPP) Top 10 Operational Impacts of the GDPR <https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr> [accessed 18 April 2016]

Lee TB, *Here's everything we know about PRISM to date*, The Washington Post, (12th June 2013), available at <https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/> [accessed 4 April 2016]

Statista, *Global Social Networks ranked by number of users*, available at <http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> [accessed 20 April 2016]

Transborder Data Flow, Issues, Barriers and Corporate Responses, a Business International Multiclient Study, (Business International 1983) IAPP, *The Next 4 steps for the Privacy Shield*, available at https://iapp.org/news/a/the-next-four-steps-for-the-privacy-shield/ [accessed 27 April 2016]

Reports, press releases and handbooks

EU Network of Independent Experts on Fundamental Rights, *Commentary of the Charter of Fundamental Rights of the European Union* (2006)

European Commission, "*First Vice-President Timmermans and Commissioner Jourová's Press Conference on Safe Harbor Following the Court Ruling in Case C-362/14 (Schrems),"* press release (October 6, 2015)

Handbook on European data protection law, European Union Agency for Fundamental Rights (2014)

European Union Agency for Fundamental Rights, *Freedom to conduct business: exploring the dimensions of a fundamental right* (2015)

McKinsey & Company, *Digital Globalization: the new era of global flows*, McKinsey Global Institute (2016), p.8 available at <http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>[accessed 4 May 2016]

Letter to Speaker Boehner and Leader Pelosi, U.S. House of Representatives, available at http://www.itic.org/dotAsset/5/8/58eb178a-e926-4783-959b-60d9464248e6.pdf [accessed 11 April 2016

Table of Legislation

UN

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

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

EU

Treaty establishing the European Community (Consolidated version 2002), OJ C 325, 24/12/2002 P. 0033 – 0184

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonization Of Certain Aspects Of Copyright And Related Rights In The Information Society [2001] OJ L167/10

Explanations Relating To The Charter Of Fundamental Rights Of The European Union, Text of the explanations relating to the complete text of the Charter as set out in CHARTE 4487/00 CONVENT 50 available at http://www.europarl.europa.eu/charter/convent49_en.htm [accessed 17 March 2016]

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector (Directive on Privacy And Electronic Communications) [2002] OJ L 201/37

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on The Protection Of Individuals With Regard To The Processing Of Personal Data By The Community Institutions And Bodies And On The Free Movement Of Such Data

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention Of Data Generated Or Processed In Connection With The Provision Of Publicly Available Electronic Communications Services Or Of Public Communications Networks And Amending Directive 2002/58/EC

Draft Charter of Fundamental Rights of the European Union – New proposal for Articles 1-30 (Civil and political rights and citizens' rights), CHARTE 4284/00, CONVENT 28, (2000), 19

European Commission, Proposal for a *Regulation Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (2012) available at http://ec.europa.eu/justice/data-protection/reform/index_en.htm [accessed 18 April 2016]

OECD

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), available at <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm> [accessed 15 March 2016]

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013) available at <http://www.oecd.org/sti/ieconomy/privacy.htm> [accessed 15 March 2016]

Council of Europe

Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, (1981) ETS 108

Relevant EU – U.S. documents

Safe Harbor Principles (2000)

U.S. – EU Safe Harbor Framework, Guide to Self-certification (2009)

U.S. Judicial Redress Act, H.R.1428 available at https://www.gpo.gov/fdsys/pkg/BILLS-114hr1428enr/pdf/BILLS-114hr1428enr.pdf [accessed 11 April 2016], and https://www.congress.gov/bill/114th-congress/house-bill/1428 [accessed 11 April 2016]

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 Harbor Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (notified under document number C (2000) 2441) (Text with EEA relevance)

Letter from Ambassador Aaron about Safe Harbor (November 1999) available at http://www.export.gov/safeharbor/aaron419.html [accessed 17 March 2016]

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 (20.10.2004)

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 (20.10.2004)

EU – U.S. Privacy Shield documents (2016) available at https://iapp.org/resources/article/eu-u-s-privacy-shield-full-text/

Draft Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (2016)

Assessment after three years of implementation of Safe Harbor, Commission Staff Working Document

Frank J, Vice President EU Government Affairs, Microsoft, *Microsoft's commitments, including DPA cooperation, under the EU-U.S. Privacy Shield* available at: http://blogs.microsoft.com/eupolicy/2016/04/11/microsofts-commitments-including-dpa-cooperation-under-the-eu-u-s-privacy-shield/ [accessed 18 April 2016]

Hogan Lovells, *Legal Analysis of the EU – U.S. Privacy Shield: an adequacy assessment by reference to the jurisprudence of the Court of Justice of the European Union* (2016)

Article 29 Working Party Statement on the Schrems Judgment (16 October 2015) available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf [accessed 25 April 2016]

European Commission, *Communication From The Commission To The European Parliament And The Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*, available at: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf [accessed 25 April 2016]

Working Party 29, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), WP 237

Working Party 29, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf [accessed 18 April 2016]

Higgins J, DigitalEurope, *Future Adoption of the draft EU-US Privacy Shield Adequacy Decision (Article 31 Committee)* available at http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2151&PortalId=0&TabId=353 [accessed 18 April 2016]

BEUC The European Consumer Organisation, *EU-US Privacy Shield proposal letter* available at http://www.beuc.eu/publications/beuc-x-2016-035_mgo_letter_on_eu-us_privacy_shield_proposal_to_ms_falque-pierrotin.pdf [accessed 18 April 2016]

Frank J, Vice President EU Government Affairs, Microsoft, *Microsoft's commitments, including DPA cooperation, under the EU-U.S. Privacy Shield* available at: http://blogs.microsoft.com/eupolicy/2016/04/11/microsofts-commitments-including-dpa-cooperation-under-the-eu-u-s-privacy-shield/ [accessed 18 April 2016]

U.S. Judicial Redress Act, H.R.1428 available at https://www.gpo.gov/fdsys/pkg/BILLS-114hr1428enr/pdf/BILLS-114hr1428enr.pdf [accessed 11 April 2016] and https://www.congress.gov/bill/114th-congress/house-bill/1428 [accessed 11 April 2016], President Obama signed it into law on 24 February 2016

Letter to Speaker Boehner and Leader Pelosi, U.S. House of Representatives, available at http://www.itic.org/dotAsset/5/8/58eb178a-e926-4783-959b-60d9464248e6.pdf [accessed 11 April 2016]

Table of Cases

C-362/14, Maximillian Schrems v. Data Protection Commissioner, joined party Digital Rights Ireland Ltd, ECLI:EU:C:2015:650, [2015]

C-362/14, Maximillian Schrems v. Data Protection Commissioner, Opinion of Advocate General Bot, ECLI:EU:C:2015:627 [2015]

C-293/12 and C-594/12, Digital Rights Ireland and Others, ECLI:EU:C:2014:238 [2014]

C-275/06, Productores de Músicade España (Promusicae) v Telefónica de España SAU ECR 1-271 [2008]

Opinion of Advocate General Justine Kokott delivered on 18 July 2007 concerning C-275/06, Productores de Músicade España (Promusicae) v Telefónica de España SAU ECR 1-271 [2008]

C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) [2011]

C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV [2012]

Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado [2011]

C-28/08 P Bavarian Lager ECR I-06055 [2010]

C-369/98 Fisher ECR I-6751 [2000]

C-465/00 Österreichischer Rundfunk ECR I-4989 [2003]

C-283/11 Sky Österreich v. Österreichischer Rundfunk Advocate General Bot Opinion [2013]

C-101/01 Bodil Lindqvist, ECR I-12971 [2003]

Joined Cases C-92/09 and C-93/09 and Markus Schecke ECR I-11063 [2010]

Case 4/73, Nold, ECR 491 [1974]

Case 29/69, Stauder v. City of Ulm, ECR 419 [1969]

High Court of Ireland, Maximillian Schrems v. Data Protection Commissioner [2013 No. 765JR]