UPPSALA
UNIVERSITET

Department of Law
Autumn Term 2015

Master's Thesis in European Union Law
30 ECTS

Protection of Personal Data, a Power Struggle between the EU and the US

What implications might be facing the transfer of personal data from the EU to the US after the CJEU's Safe Harbour ruling?

Author: Mona Strindberg
Supervisor: Professor Iain Cameron

Table of Contents

Abstract

Since the US National Security Agency's former contractor Edward Snowden exposed the Agency's mass surveillance, the EU has been making a series of attempts toward a more safeguarded and stricter path concerning its data privacy protection. On 8 April 2014, the Court of Justice of the European Union (the CJEU) invalidated the EU Data Retention Directive 2006/24/EC on the basis of incompatibility with the Charter of Fundamental Rights of the European Union (the Charter). After this judgment, the CJEU examined the legality of the Safe Harbour Agreement, which had been the main legal basis for transfers of personal data from the EU to the US under Decision 2000/520/EC. Subsequently, on 6 October 2015, in the case of *Schrems v Data Protection Commissioner*, the CJEU declared the Safe Harbour Decision invalid. The ground for the Court's judgment was the fact that the Decision enabled interference, by US public authorities, with the fundamental rights to privacy and personal data protection under Article 7 and 8 of the Charter, when processing the personal data of EU citizens. According to the judgment, this interference has been beyond what is strictly necessary and proportionate to the protection of national security and the persons concerned were not offered any administrative or judicial means of redress enabling the data relating to them to be accessed, rectified or erased. The Court's analysis of the Safe Harbour was borne out of the EU Commission's own previous assessments. Consequently, since the transfers of personal data between the EU and the US can no longer be carried out through the Safe Harbour, the EU legislature is left with the task to create a safer option, which will guarantee that the fundamental rights to privacy and protection of personal data of the EU citizens will be respected. However, although the EU is the party dictating the terms for these transatlantic transfers of personal data, the current provisions of the US law are able to provide for derogations from every possible renewed agreement unless they become compatible with the EU data privacy law. Moreover, as much business is at stake and prominent US companies are involved in this battle, the pressure toward the US is not only coming from the EU, but some American companies are also taking the fight for EU citizens' right to privacy and protection of their personal data.

Abbreviations

AG	Advocate General
BCRs	Binding Corporate Rules
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
Commission	European Commission
Convention 108	Data Protection Convention
Data Protection Directive	Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and to the free movement of such data
Data Retention Directive	Directive 2006/24/EC 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
DOC	US Department of Commerce
DPA	Data Protection Authority
DPAs	Data Protection Authorities
ECHR	European Convention on the Human Rights
ECJ	Court of Justice
ECtHR	European Court of the Human Rights
EDPS	European Data Protection Supervisor
E.O. 12,333	Executive Order 12,333
E-Privacy Directive	Directive 2002/58/EC on privacy and electronic communications
EU	European Union
FBI	Federal Bureau of Investigation
FTC Act	Federal Trade Commission Act of 1914
FTC	Federal Trade Commission
FISC	United States Foreign Intelligence Surveillance Court
FISA	Foreign Intelligence Surveillance Act
GDPR	EU General Data Protection Regulation
Member States	European Union Member States

NSA	National Security Agency
NSLs	National Security Letters
Safe Harbour Decision	Decision (2000/520/EC) of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce
SCCs	Standard Contractual Clauses
SHA	Safe Harbour Agreement
Third Countries	Non-EU countries
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
US	United States of America
WP29	Article 29 Working Party

1 Introduction

1.1 Background

The Internet is a significant contributor to the global economy. It penetrates our lives to an exceptional extent; it governs our commercial activities, but also covers a momentous part of our social sphere. In the European Union ('the EU'),[1] confidence in data processing and privacy protection is regarded as a fundamental right. Although international transfers of personal data are necessary for the expansion of international trade[2] and have thus contributed to global economic growth and efficiencies, the privacy of individuals is subjected to new and increased risks.[3] Hence, these risks make the EU responsible for guaranteeing protection for its citizens' personal data when it is transferred to third countries, in the light of the rights of the Charter of Fundamental Rights of the European Union ('the Charter').[4]

The Safe Harbour Agreement under Decision 2000/520/EC [5] ('the Safe Harbour Decision' or 'SHA') pursuant to EU Data Protection Directive 1995/46/EC ('Data Protection Directive'), which was recently declared invalid by the Court of Justice of the European Union ('the CJEU' or 'the Court'),[6] has been a framework that came to existence in order to guarantee the EU an adequate level of protection for the EU citizens' personal data when transferred to the United States of America ('the US'). It has since its emergence been maintained as the main legal basis for US companies to transfer personal data from Europe to the US. The framework has been popular and relied upon by countless international organisations due to the extensive personal data flows between these two continents.

[1] For the purposes of this thesis, the term 'EU' shall also cover the EEA. Hence, references to 'Member States' shall be understood to also cover EEA Member States.
[2] Case C-362/14 Schrems v Data Protection Commissioner (ECJ, 6 October 2015), para 48.
[3] C Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013), 2.
[4] European Union Charter of Fundamental Rights of the European Union [2000] OJ C 364/01.
[5] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p.7).
[6] The Court of Justice of the European Union (CJEU) includes the Court of Justice (ECJ), the General Court and specialized courts: TEU, art 19. In the thesis the term CJEU is used in relation to all these courts, and their predecessors.

Nevertheless, after the revelations about the US National Security Agency's ('NSA'), surveillance and data collection operations leaked by Edward Snowden, a series of attempts have been made by the EU concerning privacy protection. All these steps have been directed toward a more safeguarded and stricter path when dealing with the US. The first step took place in March 2014, when a significant majority in the European Parliament voted to suspend the SHA, upholding that secret and illegal mass-surveillance cannot be justified by the war on terrorism.[7]

Following this event, the CJEU, in *Digital Rights Ireland and Others* ('the Data Retention ruling'),[8] invalidated the Data Retention Directive 2006/24/EC,[9] which had previously required telecommunication and mobile phone companies to retain users' private data records for up to two years, allowing competent national authorities access to such data. The core issue for the Court's discussion in this case was to what extent the exchange of data should be permitted. Subsequently, the CJEU held that the Directive enabled a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary. The judgment was given a *void ab initio* effect meaning that the Directive is invalidated from the date it took effect in 2006.

Additionally, in the case of *Google Spain*, the CJEU once again highlighted the importance of Article 7 and 8 of the Charter.[10] Moreover, the latest turnout came unexpectedly two months ago, on 6 October 2015, when the CJEU in *Schrems v Data Protection Commissioner* ('the Safe Harbour ruling'),[11] ruled to invalidate the Safe Harbour Decision. The main objective for the Court's judgment in this case was the legality of Decision 2000/520/EC and the scope of the power of the Member States' Data Protection authorities ('DPAs') in connection to the transfer of EU citizens'

[7] Available at: <http://www.europarl.europa.eu/news/en/newsroom/content/20140307IPR38203/html/US-NSA-stop-mass-surveillance-now-or-face-consequences-MEPs-say> accessed 10 November 2015.
[8] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others* [2014] ECR I-238.
[9] 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 200/58/EC, (OJ 2006 L 105/54).
[10] C-131/12 *Google Spain SL and Google Inc v Agencia Espagnola de Proteccion de Datos (EPD) and Mario Costeja Gonzales* [2014] ECR I-317, paras 68-69.
[11] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015).

personal data from the EU to the US. The Court held that the existence of a European Commission ('the Commission') decision finding a third country adequate, cannot eliminate the power of the national supervisory authorities which is entrusted to them under the Charter. The Court further ruled that Decision 2000/520/EC enables interference with the fundamental rights of Articles 7 and 8 of the Charter, lacking any precise limitation necessary as to what is proportionate and is thus invalid. The Commission has since this ruling been given three months to come up with new guidelines for the transfers of personal data from EU to the US in compliance with the European Data Protection Law.

All these steps seem to indicate a power struggle between the two parties, in which they have difficulties in finding an acceptable solution for how the right to privacy of EU citizens should be protected in the midst of the differences in the level of protection provided in the privacy laws of the two regions. Whilst the EU has ultimately invalidated the SHA, and as a result sent clear signals that it will not allow violation or any jeopardisation of its citizens' privacy-rights, the US will keep maintaining a stronghold over EU citizens' private lives through its global companies e.g. Facebook, Google, Microsoft etc. As the US companies operating within the EU are currently left to either follow the EU law and be in breach of the US law or to follow the US law and break the EU law, the combination of an invalid SHA and the *de facto* possession of millions of EU users' data in the hand of the US government and corporations lead to a series of consequences. Hence, the EU legislature's task to create a new option and dictating the terms that will safeguard the protection of EU citizens' right to personal data protection and privacy is far from easy. This thesis analyses the series of actions taken by the EU by discussing the legal barriers, which have led to the current situation and which may still be a hinder for an effective and genuine renewed framework. It will furthermore discuss some relevant options in order to overcome these barriers.

1.2 Purpose and question

The aim of this thesis is to evaluate possible implications that might be facing the transfer of personal data from the EU to the US in the light of the CJEU's Safe Harbour ruling, with regard to the safeguarding and upholding human rights and the fundamental principles, mainly the right to privacy and personal data protection under Article 7 and 8

of the Charter, which have been, and still are, challenged on the basis of national security. This turnout by the CJEU could have indubitably been predicted since the Court acts in consistency with its precedents. In the case of *Digital Rights Ireland and Seitlinger and Others* invalidating the Data Retention Directive, the Court had to deal with the same matter; namely the right to privacy and protection of personal data of the EU citizens.

The main question that will be answered in this thesis is the following:
What implications might be facing the transfer of personal data from the EU to the US after the CJEU's Safe Harbour ruling?

In order to answer this question, the following sub questions are relevant:

- What is personal data?
- What is the current EU law regulating data protection?
- Why did the Safe Harbour ruling turn out the way it did?
- How will transfer of personal from EU to the US be affected by this judgment?
- Can other options for transfer of personal data to the US be regarded as safer? Is a transfer of personal data to the US safe at all?
- Is, if so, the current situation in the best interest of the EU citizens?
- If not, how can the protection of personal data be improved?

These sub questions will be answered step by step throughout the thesis.

1.3 Limitations

The thesis focuses solely on the possible future of the transfer of personal data from the EU to the US based on the CJEU's ruling in *Rights Ireland and Seitlinger and Others* and *Schrems v Data Protection Commissioner*. Since the Safe Harbour ruling came just two months ago and the Commission has been obliged to come up with new terms on how to regulate personal data transfers to the US within three months after the ruling, there might be other changes to this area by the time the paper is submitted. The discussions will cover privacy law within the EU in general, not covering any Member State's national laws thereof. Although privacy will be discussed as it is seen in the EU, the US privacy law will be discussed briefly and not in details. Furthermore, even though there are a few more Directives and Regulations within the area of IT-

protection, only the legal frameworks most relevant to the topic will be discussed in the thesis.

1.4 Method and material

This thesis is written on a topic within the area of Union law, which unavoidably affects the choice of method and material. The research is carried out from a European perspective; hence EU legislation forms the regulatory framework for it. Consequently, the method used is a legal dogmatic method, aimed at establishing how the law stands today (*de lege lata*), by using traditional legal sources. Both binding sources of law: primary law, binding secondary law, general principles and, in theory, case law from the CJEU and non-binding sources of law such as opinions of Advocate Generals, the legal doctrine and preparatory works will be taken into account.[12] Nonetheless, the sources at the top of the hierarchy of norms will be the starting point, among which, the Charter and case law from the CJEU will have a prominent position. Other sources are used as means for interpretation.

Moreover, the method used also includes comparative elements since the question deals with transatlantic personal data flow regarding the two continents, the EU and the US. Due to the significant differences governing this area within these continents, the focus will mainly be on the EU. Nevertheless, based on brief study, a short description of how privacy is seen in the US, should be appropriate for the purpose of this paper.

Although the thesis mainly analyses the current standing of the law regarding data protection *de lege lata*, the discussion will cover how it should be instead *de lege ferenda*, since the implications of the current situation give rise to an on-going discussion on how transfer of EU citizens' personal data to the US should be regulated.

The material used is in English except for one Swedish legal doctrine concerning Union law. The reference system used is based upon the Oxford University Standard for the Citation of Legal Authorities.[13] Lastly, the reader is expected to have a basic knowledge of EU Law. However, a further knowledge of EU or basic knowledge of US law is not required.

[12] J Hettne and I Otken Eriksson, *EU-rättslig metod – Teori och genomslag i svensk rättstillämpning* (2nd edn, Nordstedts Juridik AB 2011), 40.
[13] Available at <http://www.law.ox.ac.uk/published/OSCOLA_4th_edn_Hart_2012.pdf> accessed 10 November 2015.

1.5 Disposition

In Chapter 2, the general rules regarding protection of personal data and the question of competence will be briefly elaborated upon, followed by a brief discussion on how the concept of privacy is regarded in the EU with comparison to the US. In Chapter 3, a brief overview of the SHA will be provided in order to give the reader some understanding about its required procedure and obligations. Subsequently, Chapter 4 will contain a brief overview of the ruling on Data Retention Directive in the case of *Digital Rights Ireland and Others* in order to outline the steps taken by the CJEU before the Safe Harbour ruling. In Chapter 5, a detailed overview of the Safe Harbour case *Schrems v Data Protection Commissioner* will be given in order to achieve understanding about the development of EU's stand point in regards to right to privacy and protection of personal data. Additionally, in Chapter 6, the paper will turn to a detailed discussion, evaluating the current situation and the eventual future of transfer of personal data from the EU to the US with regard to the findings of the CJEU with the fundamental right of privacy in mind. Lastly, Chapter 7 will gather the thoughts and suggestions.

2 Personal Data Protection in the EU

2.1 Background

The Internet as we know it today is a joint creation of the EU and the US.[14] Prior to the EU Data Protection Law, the Member States regulated the protection of personal data in their national laws with the basis in the Council of Europe. This situation, however, had an impact on the competition and the function of EU's internal market, to the point where the EU acknowledged a need for a uniform European single market for electronic commerce and eventually strong data protection.[15] Consequently in the 90's, with the growing use of computers and the Internet, in order to strengthen the personal privacy of the citizens, the EU Commission sought to harmonise the data protection law.[16] This attempt resulted in Data Protection Directive 95/46/EC, which was adopted in 1995 and came into force in 1998, imposing that the Member States must implement it in their national laws according to the general principle of EU law. Previously, the Council of Europe had in 1981 enacted Convention 108,[17] which was a pioneer to the development of the Data Protection Directive.

Additionally, two years after the adoption of the Data Protection Directive, Directive 2002/58/EC on privacy and electronic communications (E-privacy Directive) came into existence as a continuation and complement to the Directive 95/46/EC, and not only applying to individuals but also to legal persons.[18] Thereafter, Regulation 45/2001[19] was adopted. This regulation lays down the same rights as Directive 95/46/EC with regards to protection of citizens' personal data but when it is processed by EU institutions and bodies. Eventually, in 2006, the Data Retention Directive 2006/24/EC[20] was adopted but was invalidated in 2014 by the CJEU in the case of *Digital Rights Ireland and*

[14] D W Drezner, *The Global Governance of the Internet: Bringing the State Back In* (2004), Vol. 119, No. 3, Political Science Quarterly, 477.
[15] A Savin, *EU Internet Law* (Edward Elgar publishing 2013), 3.
[16] P Carey, *Data Protection A Practical Guide to UK and EU Law* (4th edn, Oxford University Press 2015), 13.
[17] Council of Europe Convention 108, 28 January 1981, ETS 108 (1981).
[18] Council 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 L201/37, art 1(2).
[19] Regulation EC No 45/2001 of 18 December 2000, OJ L 008, 12.01.2001.
[20] Council 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, [2006] OJ L105/54.

Others. Additionally, in 2009, Directive 2009/136/EC [21] amended Directive 2002/58/EC. The most relevant frameworks of the abovementioned will be covered in the next Section.

2.2 Legal framework

2.2.1 Council of Europe

2.2.1.1 The ECHR

The right to private life is regulated in Article 8 to the European Convention for the Protection of Human Rights and Fundamental Freedoms ('ECHR'),[22] which reads as follows:

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

When applying Article 8, the European Court of Human rights ('the ECtHR')[23] typically follows a two-step approach. Firstly, the Court determines whether the case at hand constitutes an interference with any of the rights established in the ECHR. Secondly, it determines whether such interference can be regarded as legitimate.[24]

The concept of private life has eventually developed to also cover right to privacy. In the *Niemietz* ruling, a broad perspective of private life was particularly introduced by the ECtHR in which the Court concluded that the concept of private life would be too

[21] Council Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11.

[22] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

[23] The Court of the Council of Europe that hears claims of violations of rights enshrined in the ECHR.

[24] G Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Law Governance and Technology Series 16, Springer International Publishing 2014), 95. See also Case *Klass and others v Germany* [1978] app no 5029/71.

restrictive if it was only limited to the 'inner cycle' of an individual's life.[25] Additionally, in *Bensaid*, the ECtHR emphasised the width of the private-life concept by portraying it as 'not susceptible to exhaustive definition'.[26] Finally, in the landmark case *Leander*, the ECtHR concluded that storing information by the police, relating the private life of an individual, amounts to an interference with the right to respect of private life protected by Article 8 of the ECHR.[27] This judgment clearly shows that Article 8 of the ECHR also covers the right to protection of personal data. It should be noted that the CJEU often refers to the ECHR and the case law of the ECtHR in its judgments.[28]

2.2.1.2 Council of Europe Convention 108

The Council of Europe enacted Convention 108[29] ('the Data Protection Convention' or 'Convention 108') in 1981. Until now the Data Protection Convention is the only binding international treaty dealing with data protection and is regarded as a pioneer in the development of data protection as a fundamental right.[30] Even though the ECtHR has no jurisdiction to try cases according to this Convention, and it has thus no effect of judicial enforcement, this Court has in its application of Article 8 of ECHR, in some cases referred to the provisions of Convention 108.[31] In the case of *Malone,* the ECtHR when dealing with the monitoring of telephone communications by the police within the scope of criminal investigation, where information was released to the police without the consent of the subscriber, referred to the principles established by Convention 108 as criteria relevant to decide whether or not an action could be regarded as a breach of Article 8 of the ECHR.[32] It might be possible that the Strasbourg Court through its

[25] Case *Niemietz v Germany* [1992] app no 13710/88.
[26] Case *Bensaid v United Kingdom* [1992] app no 44599/98, para 47.
[27] E.g. in para 48 of the Case of *Leander v Sweden* [1987] app no 9248/81, the ECtHR states that '[i]t is uncontested that the secret police-register contained information relating to Mr. Leander's private life. Both the storing and the release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Article 8 § 1'.
[28] E.g. see Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others [2014] ECR I-238, para 35 where the Court refers to *Leander v Sweden* [1987], para 48, *Rotaru v Romania* [2000], para 46.
[29] Council of Europe Convention 108, 28 January 1981, ETS 108 (1981).
[30] L Bygrave, *Data protection Law: Approaching its Rationale, Logic and Limits* (1 edn, Kluwer Law International 2002).
[31] Case *Amann v Switzerland* [2000] app no 27798/95, para 6; Case *Rotaru v Romania* [2000] app no 28341/95, para 43.
[32] G Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Law Governance and Technology Series 16, Springer International Publishing 2014), 97. See also Case *Malone v United Kingdom* [1984] app no 8691/79, para 84.

references to Convention 108 in its cases, views Article 8 of ECHR as obliged to give effect to the provisions of Convention 108.[33]

2.2.2 EU

2.2.2.1 The Charter

The Charter of Fundamental Rights of the European Union has the status of primary law within the EU, and is thus at the top of the legal hierarchy of rules. Its role is to serve as a more effective legal force to already existing rights by enshrining them as a fundamental aspect of the EU. According to Article 52(3) of the Charter (the homogeneity clause),[34] rights in the Charter that correspond to rights guaranteed by the ECHR have the same meaning and scope as the rights in the ECHR.[35] Protection of personal data is regulated in Article 8 of the Charter and reads as follows:

> *1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with these rules shall be subject to control by an independent authority.*

With regard to the relation between Article 8 and 7 of the Charter, the Advocate General ('AG') in His Opinion to the case of *Schrems v Data Protection Commissioner* concluded that the protection of personal data provided by Article 8 of the Charter is especially important for the right to respect for private life[36] covered by Article 7 of the Charter which reads as follows:

> *Everyone has the right to respect for his or her private and family life, home and communications.*

Additionally, as these rights are regarded as fundamental, Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms

[33] C Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013), 37; and P De Hert and S Gutwirth, *Reinventing Data Protection?* (Springer 2009), 27.
[34] See the opinion of AG Kokott in Case C-110/10, para 95.
[35] See e.g. the CJEU's explanations to art 52 of the Charter in Case *Deb v Germany* [2010] ECR I-13849, paras 35 and 45-52.
[36] Opinion of AG Bot in Case C-362/14, para 192. See also joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Others* [2014] ECR I-238, para 53.

recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Furthermore, subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. The scope of these mentioned rights will be discussed in connection to the Data Retention and the Safe Harbour ruling.

2.2.2.2 Treaty on the Functioning of the European Union

The Treaty on the Functioning of the European Union ('the TFEU')[37] has likewise the Charter status of primary law within the EU. Protection of personal data is covered by Article 16(1) of the TFEU, which reads as follows:

> *Everyone has the right to the protection of personal data concerning them.*

2.2.2.3 Directive 95/46/EC

The objective of the Data Protection Directive as stated in recital 10 and Article 1 is to in accordance with Article 8 of the ECHR, Article 7 and 8 of the Charter and Article 16 of the TFEU, seek to ensure, in the EU, 'a high level of protection of fundamental rights and freedoms', mainly privacy, with regard to the processing of personal data. Article 2(a) of the Data Protection Directive defines 'personal data' as any information relating to an identified or identifiable natural person (the *data subject)* for example name or address. Furthermore, under Article 2(b) 'processing data' is any operation or set of operations performed upon personal data, regardless of usage of automatic means, 'such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.

Moreover, Article 6 of the Data Protection Directive regulates principles under which the data must be processed. According to the provisions set out in Article 6(a), the Member States must provide fair and lawful processing of personal data,[38] collected for specified legitimate purposes,[39] adequate, relevant and not excessive in relation to the purposes for which they are collected,[40] and accurate and where necessary up to date.[41]

[37] Treaty on the Functioning of the European Union [2012] OJ C326/47.
[38] Directive 95/46/EC, art 6(a).
[39] Ibid, art 6(b).
[40] Ibid, art 6(c).

In addition to this provision, Article 7 establishes the criteria for legitimate data processing, requiring that a process of the data only be done with the subject's consent notwithstanding the national-security exception, which can expunge this criterion. This exemption will be further discussed in Section 2.5 and Chapter 5.

Nonetheless, under Article 25 of Directive 95/46/EC, data can be transferred to countries outside the EU if the third country in question meets the requirements of an 'adequate' level of data protection within the meaning of Article 25(2), read in light of the fundamental right to protection of personal data guaranteed by Article 8 of the Charter. There is a two-step process for determining this. Firstly, the personal data must be legally collected and processed in compliance with the Directive and secondly there must be a legal basis for the transfer outside the EU under Article 25 or 26. Assessing an adequate level of protection was in fact one of the matters discussed by the CJEU in the case of *Schrems v Data Protection Commissioner*.

Moreover, if the third country in question does not ensure an 'adequate' level of protection under Article 25, Article 26 can be applied to permit transfer of personal data by instead allowing the use of binding contractual commitments between the data exporter and data importer. Since the SHA is invalid, Article 26 will be applicable. The Commission has approved Standard Contractual Clauses ('SCCs') and Binding Corporate Rules ('BCRs') to be used in the mean time. These alternative tools for transfer of personal data to third countries will be further discussed in Chapter 6.

2.3 Role of the competent Parties

The competence for the protection of personal data is shared between the EU and the Member States. The latter are responsible for adopting national laws pursuant to the Data Protection Directive and for setting up one or more DPAs in order to control that processing of individuals' personal data is in compliance with the protection provided by the EU law. The Commission has been conferred the role to assess whether a third country ensures an adequate level of protection in regard to the transfer of personal data. More about each party's competence in this area will be elaborated upon in the following sections.

[41] Directive 95/46/EC, art 6(d).

2.3.1 Member States and the Data Protection Authorities

The first and fourth subparagraphs of Article 32 of Directive 95/46/EC oblige each Member State to 'bring into force the laws, regulations and administrative provisions necessary to comply with the Directive', enforcing them to communicate to the Commission the text of their domestic law which they enact in the scope of the Directive. Furthermore, under the first subparagraph of Article 28(1) of Directive 95/46/EC, the Member States are obliged to provide 'one or more public authorities … responsible for monitoring the application within [their] territory for the provisions adopted by the Member States pursuant to this Directive', which according to the second subparagraph of Article 28(1) have to act with complete independence in exercising the functions entrusted to them. Practically, the Member States are required to set up a controlling authority with the competence to supervise and monitor compliance with the national laws that are created in compliance with the EU rules concerning the protection of individuals with regard to processing of their personal data. These authorities have the responsibility to check whether the transfers of personal data from their own Member States to a third country, which may be subject of a Commission decision pursuant to Article 25(6) of Directive 95/46/EC, comply with the requirements of the Data Protection Directive.

It should be mentioned that the requirement of independency of the DPAs under Article 28(2) of Directive 95/46/EC derives from the primary law of the EU, enshrined in Article 8(3) of the Charter and Article 16(2) of the TFEU. In this regard the CJEU has concluded that, '[this] guarantee … is intended to ensure the effectiveness and reliability of the supervision' and 'in order to strengthen the protection of individuals and bodies affected by [the] decisions [of those national supervisory authorities]',[42] viewing these authorities as 'guardians of fundamental rights'.[43]

Furthermore, under the first subparagraph of Article 28(4) of the Data Protection Directive, the DPAs are to hear 'claims lodged by any person … concerning the protection of his rights and freedoms in regard to the processing of personal data'. The competence of these authorities was one of the questions referred to the CJEU in the

[42] Case C-518/07 *Commission v Germany* [2010] ECR I-1885, para 25.
[43] Case C-614/10 *Commission v Austria* (ECJ, 16 October 2012), para 52; Case C-288/12 *Commission v Hungary* [2014] ECR I-237, para 53. See also the arguments of the CJEU in Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), paras 99-101.

case of *Schrems v Data Protection Commissioner*. In this respect the Court concluded that when a person lodges a claim with the Data Protection Authority ('DPA'), 'it is incumbent upon the … authority to examine the claim with all due diligence'.[44] Nevertheless, in a case where the DPA finds a claim unfounded and thus rejects it, the Member States are, according to the provision of second subparagraph of Article 28(3) of the Data Protection Directive, read in the light of Article 47 of the Charter, required to provide individuals access to judicial remedies enabling him/her to challenge such decision before the national courts.[45] According to the case law of the CJEU, the national courts are further obliged to stay proceedings and make a reference to the CJEU for a 'preliminary ruling on validity where they consider one or more grounds for validity put forward by the parties, or as the case may be, raised by them of their own motion'.[46]

Furthermore, since the NSA-leaks indicated that transfers of personal data to the US have not been safe under the Safe Harbour Decision, there has been pressure from the DPAs of the Member States to suspend the Agreement. One example is from 29 January 2015, when the current Commissioner for Data Protection of Berlin, Dr Alexander Dix, during his speech at the European Data Protection Conference in Berlin, explicitly emphasised that unless the practice of data transfers from the EU to the US is not significantly changed, the SHA should be suspended.[47] It even went so far that the German authorities started to file administrative proceeding against US companies and started to deny new permissions for data export to the US.[48] As aforementioned, the competence of the DPAs was also one of the main concerns for the CJEU in *Schrems v Data Protection Commissioner*, in which the Court explicitly underlined the supervisory role of these authorities.[49] Moreover, it should be mentioned that after the Safe Harbour ruling, the Commission has correspondingly emphasised on the 'central

[44] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), para 63.
[45] Ibid, para 64.
[46] Case C-456/13 *T & L Sugars and Sidul Acucares v Commission* (ECJ, 28 April 2015), para 48. See also the CJEU's reasoning in Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), para 64.
[47] Available at: <http://wragge-law.com/insights/rescuing-personal-data-from-an-unsafe-harbor-european-data-protection-regulators-start-taking-things/> accessed 10 November 2015.
[48] Ibid.
[49] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), paras 40, 43 and 47.

role' of the DPAs as 'the main enforcers of the fundamental rights of data subjects' in one of its recent Communication.[50]

2.3.2 EU Commission

Article 25(6) of the Data Protection Directive confers upon the Commission the power to examine '[whether] a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals'. The CJEU clarified this role in the Safe Harbour ruling, concluding that 'the legal order of the third country … must ensure an adequate level of protection' and the Commission is 'obliged to assess the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules, since it must under Article 25(2) of Directive 95/46/EC, take account of all circumstances surrounding a transfer of personal data to a third country'.[51] The Court also put upon the Commission the obligation to 'check periodically whether … the adequacy of the level of protection ensured by the third country in question is still factually and legally justified', concluding that '[s]uch a check is required, …, when evidence gives rise to a doubt in that regard'.[52]

2.3.2.1 Article 29 Working Party

The Working Party on the Protection of Individuals with regard to the Processing of Personal Data ('WP29') is an independent consultative body established under Article 29 of the Data Protection Directive. It consists of a representative from each Member State's DPA, the European Data Protection Supervisor ('EDPS') and a representative from the Commission. It has the mandate to give opinions and to make recommendations relating to the protection of individuals with regard to processing of personal data. The European Commission provides the secretariat of the WP29. Although the statements made by this body are not legally enforceable, they are

[50] 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), COM (2015) 566 final, 6 November 2015, 16.
[51] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), paras 74-75.
[52] Ibid, para 76.

considered serious.[53] Under Article 30 of Directive 95/46/EC, the WP29 as a platform for cooperation, besides providing expert-advice from the national level to the Commission on data protection matters, also seeks to promote a uniform application of Directive 95/46/EC in all Member States of the EU.

The important role of the WP29 has become more visible since the SHA has been under question. Admittedly, the AG in his opinion to *Schrems v Data Protection Commissioner*, with regard to the examination of the level of protection afforded by a third country, referred to a Working Party document,[54] concluding that 'the level of protection [ensured] by a third country [should] focus on two fundamental elements, namely the content of the applicable rules and the means of ensuring compliance with those rules'.[55] Moreover, it should be noted that after the suspension of the Safe Harbour Decision, the WP29 will have an extremely important role in helping the Commission to create a renewed transatlantic framework for the transfer and processing of EU citizens' personal data from the EU to the US that will ensure protection of privacy and personal data in the light of the Charter.

2.3.2.2 European Data Protection Supervisor

The EDPS was created on the basis of Council Decision 1247/2002/EC[56] and is an independent supervisory authority within the EU, which aims at ensuring that all EU institutions, bodies, agencies and offices respect people's right to privacy when processing their personal data. One of the main tasks of the EDPS is to examine the data protection and the impact of proposed new legislation on privacy. Many of the EDPS's tasks come from notifications of processing operations presenting specific risks that need prior checking by him. Based on the facts submitted to him, the EDPS will then examine the processing of personal data in relation to the Data Protection Regulation,[57] which provides for the supervision by the EDPS. In most cases, the examination leads to a set of recommendations that the institution or body needs to implement in order to

[53] P Carey, *Data Protection A Practical Guide to UK and EU Law* (4th edn, Oxford University Press 2015), 9.
[54] Commission Working Document WP 12, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, Adopted by the Working Party on 24 July 1998, 5.
[55] Opinion of AG Bot in Case C-362/14, para 143.
[56] Council Decision 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data protection Supervisor's duties of July 2002, OJ L 183, 12.07.2002.
[57] Regulation (EC) No 45/2001.

ensure compliance with data protection rules.[58] Besides being a member of the WP29, the EDPS also cooperates with the Commission and advises on policies and legislation that affect privacy.

2.4 General rules regarding transfer of personal data to non-EU countries

According to recital 57 of the Data Protection Directive, transfer of personal data to third countries that do not ensure an adequate level of protection is prohibited unless the third country in question ensures an adequate level of protection under Article 25(1) of Directive 95/46/EC. However, in the absence of an adequacy decision under Article 25(6) of Directive 95/46/EC, there are a few grounds set out in Article 26(1) of the Data Protection Directive that provide a derogation from this general prohibition of transferring personal data to entities established in a third country.[59] These rules will be discussed in details in connection to the overview of the cases *Digital Rights Ireland and Others* and *Schrems v Data Protection Commissioner* in Chapters 4, 5 and 6.

2.4.1 Legal basis for the Safe Harbour Agreement

The Commission Decision 2000/520/EC pursuant to Directive 95/46/EC read in the light of Article 7 and 8 of the Charter has been the legal basis for the Safe Harbour.

2.5 The National-Security exception

As it has been mentioned in Section 2.2.3, the consent of the 'data subject' under Article 7 of the Data Protection Directive can be exempted on the basis of the national-security. This exception is regulated under Article 13 (1) of Directive 95/46/EC. Likewise the fourth paragraph of Annex I to Decision 2000/520/EC provided for exemption from the safe harbour principles. Article 13 (1) of Directive 95/46/EC provides as follows:

1. *Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:*
   (a) national security;

[58] More details about the role of the EDPS is available at: <https://secure.edps.europa.eu/EDPSWEB/edps/Supervision> accessed 10 November 2015.
[59] COM (2015) 566, 8–9.

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(f) the protection of the data subject or of the rights and freedoms of other.

The fourth paragraph of Annex I to Decision 2000/520/EC read as follows:

> *Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive of Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.*

As the first abovementioned provision allows the Member States to restrict the scope of the rights and obligations protected by the Directive 95/46/EC on the basis of national security, fourth paragraph (a) of Annex I to Decision 2000/520/EC afforded third countries limitation to compliance with the safe harbour principles on the basis of 'national security, public interest, or law enforcement requirements'. It can be concluded that the wording of these provisions are vague and all too interpretive. As far as the interpretation by the Member States is concerned, it is far easier to make them accountable in a case of breach of the fundamental rights of the Charter.

However, the provision under Safe Harbour Decision has been in relation to the US and not a Member State. A breach of fundamental rights of the EU when the other party is a third country may thus not be as easily handled. The NSA leaks and the case of *Schrems v Data Protection Commissioner* brought before the CJEU, clearly show that the national-security exception in Decision 2000/520/EC has led to implications, jeopardising the fundamental rights of the Charter. In this regard, right after the NSA leaks, Viviane Reding, the EU commissioner overseeing data protection told EU ministers that 'the Safe Harbour may not be so safe after all. It could be a loophole because it allows data transfers from EU to US companies, although US data protection standards are lower than our European ones'.[60] After all, this seems to be the conclusion of the CJEU as well. It should also be noted that such provision with such vague wording with the US, as the third party in question, should have been predicted to give such consequences as the national security is a politically and judicially high priority in this country. The implications stemming from the fourth paragraph of Annex I to Decision 2000/520/EC will be further discussed in Chapters 5.

2.6 Surveillance and the Right to Privacy

2.6.1 Privacy as a legal notion with regard to personal data

The concept of privacy as informational privacy meaning 'control upon personal information' was first introduced in the US in the 70's by the writing of scholars such as Westin.[61] Furthermore, in the case of *Nixon v. Administrator of General Services* the US Supreme Court extended the scope of constitutional privacy protection to cover informational privacy, concluding that the zone of privacy protected by the constitution encompasses the 'individual interest in avoiding disclosure of personal matters'.[62] The rules in Europe constituting data protection are all attributes of the protection of privacy, which in summary can be redefined as informational privacy, with their basis in the post-Westin notion.[63]

[60] Available at: <http://www.theguardian.com/world/2013/oct/17/eu-rules-data-us-edward-snowden> accessed 10 November 2015.
[61] A F Westin, *Privacy and Freedom* (originally published in 1967, Atheneum 1970), 315.
[62] *Nixon v. Administrator of General Services* 433 U.S. 425 (1977).
[63] G Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Law Governance and Technology Series 16, Springer International Publishing 2014), 37 and 48.

2.6.2 Privacy and data protection in the US

The US does not have any general data protection law. The regulation of privacy in the US is made up of a complex web of federal and state law, stemming from case law and legislation.[64] Practically, the US legal system recognises a fundamental right of personal privacy and informational privacy is an accepted principle by the US legal system as a constitutional right, with the Bill of Rights, the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments all containing elements attributable to it. However, the constitutional privacy rights are always toward to either federal, state or government. These rights thus prevent the government from violating them but they do not require the government to protect them against third parties. The US has also personal data privacy rights outside its constitutional sphere.[65] However, the US federal legislation fails to provide a comprehensive data protection regime and likewise the State legislation.[66] Another implication with the US privacy law is that it does not offer any independent data protection authority with meaningful enforcement power as in the EU.[67] Hence, considering the foregoing reasons the US cannot be considered as offering an adequate level of protection for the processing of personal data in comparison to the EU.

2.6.3 Contractual aspects

As far as the contractual aspects are concerned, there is one great problem that will always be a threat to the consumers', (in this case the EU citizens') rights to protection of their personal data. Until Decision 2000/520/EC was valid, its fourth paragraph of Annex I enabled exemption from the fundamental rights and freedoms under the Charter on the basis of national security and public safety. The provision also afforded the US law to stand above the Safe Harbour principles in case of a conflict.

As for the current situation, the problem still remains. Looking at the company Facebook for example, which was one of the parties in the case of *Schrems v Data Protection Commissioner*, its privacy policy provided for the consumers states: 'We may access, preserve and share your information in response to a legal request (like a

[64] D J B. Svantesson, *The regulation of cross-border data flows* (2011), Vol. 1, No. 3, International Data Privacy Law, 185.
[65] A Charlesworth, *Clash of the Data Titans? US and EU Data Privacy Regulation* (2000), Vol. 6, No. 2, European Public Law, 259.
[66] Ibid, 260.
[67] K A Bamberger, D K Mulligan, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices* (2013) Vol. 81, George Washington Law Review, 1542.

search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so… Information we receive about you, including financial transaction data related to purchases made with Facebook, may be accessed, processed and retained for an extended period of time when it is the subject of a legal request or obligation, governmental investigation, or investigations concerning possible violations of our terms or policies, or otherwise to prevent harm'.[68]

The abovementioned example clearly highlights the on-going struggle of regulatory conflict, where the US law has primacy over all the contracts that the EU consumers may agree to with the US companies. Practically, it means that consumers can make all contracts they want with the US companies established in the US and believe that their personal data is protected from surveillance but the bitter truth is that when the personal data of EU citizens gets into the US companies' possession, it is subjected to US law and none of the fundamental rights respected within the EU can be expected to apply. This problem will be further collaborated upon in Chapter 6.

[68] Facebook's Privacy Policy titled *How do we respond to legal requests or prevent harm?,* available at: <https://www.facebook.com/policy.php> accessed 10 November 2015.

3 Safe Harbour under Decision 2000/520/EC

3.1 Background and overview

As aforementioned, a transfer of personal data from the EU to a third country is only allowed if the country in question offers an adequate level of protection of data in compliance with Article 25 of the Directive 95/46/EC. The US was not deemed to ensure an adequate level of protection for the transfer of personal data from the EU to the US. One of the reasons for this is because the US does not have an organised data protection system which covers both the public and the private sector, and also because it does not have an independent data protection authority.[69] Hence, in 1998, the US Department of Commerce ('DOC') and the European Commission began discussing the creation of a framework for US companies by which they would be bound to the rules set forth by the Data Protection Directive. Two years of negotiations resulted in an agreement and thus the Safe Harbour under Decision 2000/520/EC was created.[70] Pursuant to Article 288 TFEU, Decision 2000/520/EC was, until its suspension, binding on all Member States and their organs.

The Safe Harbour under Decision 2000/520/EC has until its suspension by the CJEU in the case of *Schrems v Data Protection Commissioner*, maintained the main legal basis for the US companies to receive and transfer personal data from the EU to the US. Up until its suspension, about 5000 US companies,[71] including Facebook, Microsoft and Google, had been registered under the Safe Harbour, and the framework was considered as the most vital mechanism in transferring data from the EU to the US because of its certain and liable routine.[72] Although the Safe Harbour has had a voluntary self-certification system, the companies were able to, among other alternatives, instead choose contracts to Binding Corporate Rules approved by the DPAs.[73] These other alternatives are currently being used, after the suspension of the Safe Harbour Decision.

[69] K A Bamberger, D K Mulligan *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices* (2013) Vol. 81, George Washington Law Review, 1542.
[70] D R. Leathers, *Giving Bite to the EU-US Data Privacy Safe Harbor: Model Solutions For Effective Enforcement* (2009), Vol. 41:193, No. 1, Case Western Reserve Journal of International Law, 200.
[71] Available at: <http://wragge-law.com/insights/rescuing-personal-data-from-an-unsafe-harbor-european-data-protection-regulators-start-taking-things/> accessed 10 November 2015.
[72] L Colonna, *Article 4 of the EU Data Protection Directive and the irrelevance of the EU-US Safe Harbour Program?* (2014) Vol. 4, No. 3, International Data Privacy Law, 204.
[73] Ibid, 202–204.

The Safe Harbour framework has been a set-up of several separate documents put together as one, which consisted of:

1. The Commission's Decision on the adequacy of the SHA.[74]
2. A description of the seven privacy-principle requirements that companies were entailed to follow in order to comply with the agreement.[75]
3. Fifteen frequently asked questions and answers to guide with the statuary interpretation of these seven privacy principles.[76]
4. An EU Commission memorandum on the sufficiency of the Federal Trade Commission's ('FTC') powers.[77]
5. An EU Commission memorandum on private causes of action for privacy violations obtainable within the US.[78]
6. A letter from the FTC to the European Commission describing the agency's enforcement jurisdiction.[79]
7. A letter from the Department of Transportation to the European Commission clarifying the agency's enforcement powers.[80]
8. A list of the US agencies, which the EU Commission approved to accurately enforce the requirements set forth by the agreement.[81]

The complications with Decision 2000/520/EC that resulted in the suspension of the Safe Harbour Agreement will be covered further in Chapter 5.

3.2 Procedure

3.2.1 The Notice, Choice, Onward Transfer, Security, Data Integrity, and Access Principles

Whenever a company wanted to join the Safe Harbour, it had to start off by adopting a privacy policy, which corresponded with these seven following principles: notice, choice, onward transfer, data security, data integrity, access, and enforcement.[82] The notice principle aimed to empower the data subject by requiring that she/he be informed about the purpose for which their personal data was being used, by allowing her/him to

[74] Decision 2000/520/EC.
[75] Ibid, annex I.
[76] Ibid, annex II.
[77] Ibid, annex III.
[78] Ibid, annex IV.
[79] Ibid, annex V.
[80] Ibid, annex VI.
[81] Ibid, annex I.
[82] Ibid.

choose according to the choice principle whether her/his data may be used for other purposes than they were originally collected for.[83]

Furthermore, the onward transfer principle imposed obligations on the Safe-Harbour registered company that wished to transfer data to a third party which was acting as an agent, to ensure that the personal data collected was only transferred to a third party company which was considered as 'adequate'. Additionally, a company registered with the Safe Harbour was, according to the security principle, also responsible for protecting personal data from loss, misuse, and unauthorised access. However, the data integrity principle required the company registered with the Safe Harbour to process data only with the 'purposes for which it has been collected or subsequently authorised by the individual' and accordingly ensure that the collected data was reliable for its intended use, accurate, complete, and current'. [84] Additionally, the access principle required the company to make its data available upon request to any EU citizen from whom the company had collected information. The individual was supposed to be given an opportunity to access the data, correct, amend, or delete it if needed.[85] However, as aforementioned, there have been a few exceptions to these principles under the fourth paragraph of Annex I.[86]

3.2.2 The Enforcement Principle

The enforcement principle of the Safe Harbour consisted of three components:[87]

1. A resolution system using an independent recourse mechanism.
2. A privacy handling verification mechanism.
3. An assurance to remedy

The first component obliged the company to establish an independent dispute resolution body[88] that would handle accusations of privacy infringements in order to make it easy for the individuals to easily raise complaints through an uncomplicated and affordable

[83] Decision 2000/520/EC, annex I.
[84] Ibid.
[85] Ibid.
[86] See Section 2.5.
[87] Decision 2000/520/EC, annex II, note 11. See also D R. Leathers, *Giving Bite to the EU-US Data Privacy Safe Harbor: Model Solutions For Effective Enforcement* (2009), Vol. 41:193, No. 1, Case Western Reserve Journal of International Law, 203.
[88] Decision 2000/520/EC, annex II, note 11.

process.[89] This body was supposed to correspondingly be 'readily available and affordable recourse mechanisms by which each individual's complaints and disputes are investigated'.[90] The resolution mechanism could either be provided by 'private sector self-regulatory bodies which incorporate the Safe Harbour requirements such as the US Council of Better Business Bureau ('BBB')[91] or TRUSTe,[92] or by other private sector independent recourse mechanism bodies that followed the requirements of the enforcements principle and the FAQs, or by cooperation with data protection authorities within the EU Member States[93] or lastly through legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution.[94]

The companies were furthermore required to establish a verification body to audit the company's compliance with the mentioned privacy principles either through self-assessment by performing an internal review of the extent to which it complies with the principles as reflected in its privacy policy, or by outside compliance reviews through an external reviewer.[95] Lastly, as the third component required a guarantee to remedy, the Safe-Harbour registered company was obliged to resolve any issues that were raised from a decision made by the independent recourse mechanism.[96]

3.2.2.1 The FTC and the enforcement in the US

After the company had successfully made a comprehensive data handling policy that incorporated and addressed all of the Safe Harbour's seven principles, it was required to make it publically available in order to make the data subject aware about their rights and the obligations to which the company was subjected.[97] Thereafter, after completing all these steps, the company was formally ready to join the Safe Harbour.

---

[89] K Zaidi, *Harmonizing US-EU Online Privacy Laws: Toward a US comprehensive Regime for the Protection of Personal Data* (2003), Vol. 37, No. 2, Syracuse Journal of International Law and Commerce, 169.
[90] Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM (2013) 847 final, 27 November 2013, 13.
[91] US Council of Better Business Bureau, *BBB EU Safe Harbor Program*, available at: <http://www.bbb.org/council/eusafeharbor/> accessed 10 November 2015.
[92] TRUSTe, available at: <http://www.truste.com/business-products/eu-safe-harbor-seal/> accessed 10 November 2015.
[93] Decision 2000/520/EC, annex II, note 6.
[94] D R. Leathers, *Giving Bite to the EU-US Data Privacy Safe Harbor: Model Solutions For Effective Enforcement* (2009), Vol. 41:193, No. 1, Case Western Reserve Journal of International Law, 204.
[95] Decision 2000/520/EC, annex II, note 7.
[96] Ibid, note 11.
[97] Com (2013) 847, 8.

Nonetheless, the enforcement followed when the company had to lastly self-certify its compliance with the DOC (which holds a list of all the registered companies) by providing the Department a written notification giving them contact information of the company, information about the type of personal data that it received from the EU, and also information about the privacy policy that it maintained for handling such personal data.[98] After a company had been granted membership, it was additionally required to renew its membership by self-certifying to the DOC annually. In case it failed to do so, the DOC would remove the organisation from its list and Safe Harbour benefits would then no longer apply.[99] Furthermore, if a company would choose to leave the Safe Harbour Agreement, it would still have to follow the protection rules for the personal data, which it had received while it still was registered with the Safe Harbour.[100]

Moreover, since the Safe Harbour generally relied on industry self-regulation, the government was responsible for its oversight and the enforcement of its principles.[101] The two US government agencies, FTC[102] and the Department of Transportation,[103] had guaranteed the European Commission that they would take enforcement actions against companies that failed to follow the Safe Harbour requirements that they were bound to. The FTC was considered as the major government body responsible for enforcing the Safe Harbour principles. The jurisdiction of the FTC extends to any 'unfair or deceptive acts or practices in or affecting commerce' under Section 5 of the Federal Trade Commission Act of 1914 ('the FTC Act').[104] The Agency has two responsibilities: enforcement of antitrust laws and providing consumer protection and is empowered to bring about different types of remedies on behalf of consumers ranging from administrative orders to civil penalties for violations.[105] The Department of Transportation, having its authority under Title 49 United States Code Section 41712,

[98] Decision 2000/520/EC, annex II, note 6.
[99] Ibid.
[100] Ibid. See also J T Soma, S D Rynerson, and B D Beall-Eder, *An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The US/EU E-Commerce Privacy Safe Harbor* (2004), Vol. 39, No. 2, Texas International Law Journal, 171.
[101] J Kulesza, *Walled Gardens of Privacy or 'Binding Corporate Rules?'*: A Critical Look at International Protection of Online Privacy' (2012), Vol. 34, No. 4, U. Ark. Little Rock Law Review, 747.
[102] Decision 2000/520/EC, annex V.
[103] Ibid, annex VI.
[104] 15 U.S.C. § 45(a)(1) (2006), available at: <https://www.law.cornell.edu/uscode/text/15/45> accessed 10 November 2015.
[105] R R Schriver, *You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission* (2002), Vol. 70, No. 6, Fordham Law Review, 2777.

has however in contrast to FTC had a much limited authority.[106] Nevertheless, since the FTC has been the major enforcement government agency in this area, the Department of Transportation will not be discussed any further.

Furthermore, it should also be noted that in a case of resolving a complaint, a EU citizen had to first contact the Safe-Harbour company in question. After this step he/she could seek recourse through the Enforcement Principle by referencing the Company's privacy policy and contacting the Company's independent dispute resolution. Lastly, it was only when the independent recourse mechanism failed to settle a dispute that the individuals could refer the case to the enforcement government agency. This information had to be outlined by the companies as part of their initial registration with the DOC.[107]

3.2.2.2 Complications with the FTC's oversight

In case of damages for breaches of privacy, companies registered with the Safe Harbour could be held legally liable and also civil causes of action for damages for violation of individuals' privacy was available under US common law, and likewise under some federal and state statutes on privacy.[108] However, there have been some obstacles with the role of the FTC that were acknowledged by the Commission before the suspension of Decision 2000/520/EC. One of the issues addressed was the actual scope of the enforcement power of the FTC, which as the Commission argued, was limited to deceptive practices affecting commerce, and did thus not have regulatory jurisdiction over the banking, telecommunication or employment sectors.[109]

Furthermore, the Commission was also concerned about the FTC's limited legal competence, since its enforcement of the Safe Harbour principles regarding human-resources data have not been clear. This created a problem since up to 30 percent of the companies under the Safe Harbour imported human-resources data.[110] Additionally, looking at the legislative and judicial history of Section 5 of FTC Act, the FTC's claim

[106] D R. Leathers, *Giving Bite to the EU-US Data Privacy Safe Harbor: Model Solutions For Effective Enforcement* (2009), Vol. 41:193, No. 1, Case Western Reserve Journal of International Law, 207.
[107] Ibid, 207.
[108] Decision 2000/520/EC, annex IV.
[109] Com (2013) 847, 13. See also J R Reidenberg, *E-Commerce and Trans-Atlantic Privacy* (2001), Vol. 38, No. 3, Houston Law Review, 717.
[110] Commission Staff Working Document SEC (2004) 1323 of 20 Oct. 2004 on 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 Issues by the US Department of Commerce, 10.

for jurisdiction over the safe harbour process 'is a radical departure from the stated legislative purposes of the statue and in direct opposition to the Supreme Court's restrictive interpretation of Section 5 authority' since the FTC Act has 'at no time contemplated protecting … foreign consumers'.[111]

Moreover, it should also be added that for the first ten years of the Safe Harbour's existence, the FTC received no complaints. The agency consequently decided to try to find Safe Harbour violations in 'every privacy and data security investigation it conducts',[112] which between 2009 and 2012 resulted in bringing ten enforcement actions against companies committing violations.[113] As an example, in 2012, Google agreed to pay a $22.5 million fine to settle the allegations brought by FTC because of the company's deceptive tactics toward its customers violating its own privacy policies, by launching Google Buzz. Among the charges was that the company had collected and used consumers' information for a different purpose from that for which it was collected without notifying or obtaining their permission in advance.[114]

All these concerns, of course, called the effectiveness and reality of the role of the FTC into question, especially when only ten companies out of more than 5000 companies have been charged for Safe Harbour violations. It should also be noted that most of these cases involved companies continuing to represent themselves as Safe-Harbour registered but had failed to renew their annual certification.[115] One of the main problems with regard to the US' protection of privacy and processing of personal data of the EU citizens was that the FTC does not offer any effective enforcement assurance for EU citizens. Consequently, the EU citizens were to rely on the US common law and statues for the protection of their personal data and privacy, albeit privacy is regulated differently in the US. Hence, the ineffective role of the FTC was a concern for the AG and the CJEU in the case of *Schrems v Data Protection Commissioner*. Their reasoning in this regard will be outlined in Chapter 5.

---

[111] S Mercado Kierkegaard, *Safe Harbor Agreement-Boon or Bane?* (2005), Vol. 10, Shidler Journal of Law, Commerce & Technology, 10.
[112] Com (2013) 847, 10.
[113] Ibid, 11.
[114] See FTC's Press Release of March 30, 2011, available at: <http://ftc.gov/opa/2011/03/google.shtm> accessed 10 November 2015.
[115] Com (2013) 847, 11, footnote 34.

4 CJEU's ruling on Data Retention

4.1 General remarks

How the EU's exchange of personal data with the US has been done through the Safe Harbour has previously been explained. To what extent an exchange could be done was however a point which was taken up by the CJEU in the case of *Digital Rights Ireland and Others*.[116] The Court in its judgment on 8 April 2014, ruled that the provisions in Directive 2006/24/EC (the Data Retention Directive)[117] constituted disproportionate interference with the rights to privacy and to data protection guaranteed by Articles 7 and 8 of the Charter, and Article 8 of the ECHR. This judgment has played a crucial role for the future of the Safe Harbour. Since the Court was in this case facing the same concerns involving privacy and protection of personal data, it could be predicted that the Safe Harbour would be next in line to become challenged. Although the case is very extensive and interesting, it will not be analysed in detail, since the main focus of the thesis will be on the case of *Schrems v Data Protection Commissioner*.

4.2 Overview and effects of the judgment

4.2.1 The obligation imposed on the providers

The electronic communication providers had under Article 3, 5 and 6 of Directive 2006/24/EC been obliged to retain data from individuals for a period of a minimum 6 months and a maximum of 24 months. In this regard, the CJEU concluded that this obligation constitutes an interference with the rights laid down in Article 7 of the Charter.[118] The Court viewed that the requirement by the Directive is without any distinction made between the 'categories of data … on the basis of their usefulness for the purposes of the objective pursued or according to the persons concerned' and that the determination of the retention period is not mentioned to be based on 'objective criteria in order to ensure that it is limited to what is strictly necessary'.[119] This part of the judgment may however not have affected the SHA as a whole since in the case of the Data Retention Directive, the telecommunication companies were imposed an obligations to retain the data in comparison to the the retention of personal data done by

[116] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others* [2014] ECR I-238.
[117] 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, O.J. 2006, L 105/54.
[118] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others* [2014] ECR I-238, para 34.
[119] Ibid, paras 63-64.

some Safe-Harbour registered companies. Social media corporations can be a good example of this. Whenever an individual uploads private photos on one of these websites, he/she is accepting to give access to his/her personal data to both his/her own followers and the company in question, whereas making phone calls to a friend through a telecommunication company's services is using the service right at the time of the usage because once the conversation is over there is no retention. Hence, this part of the judgment could be regarded as having effects on the Safe Harbour if the company registered with the framework had been a provider of electronic communication or public communication network, since the Data Retention Directive gave allowance to these companies to retain information from their users, as it obliged the provider to do accordingly.

4.2.2 The processing of personal data

As far as the rules relating to processing of personal data are concerned, the CJEU concluded that the provision of Directive 2006/24/EC for the processing of personal data constitutes an interference with Article 8 of the Charter.[120] The Court referred to the fact that the Data Retention Directive 'does not require the data in question to be retained within the European Union', which means that the Directive had also given the Safe Harbour companies allowance to retain data from EU citizens. Consequently, this statement by the Court has most probably created direct implications for the SHA as transfer and retention of personal data is the main conduct done through the Framework. If the decision by the CJEU would be interpreted that the transfer in itself is a breach of Article 8 of the Charter, its effect on the SHA could not be anything other than a suspension. It should also be mentioned, that the Court when referring to the AG's Opinion, concluded that the interference with the fundamental rights guaranteed by Article 7 and 8 of the Charter, caused by the Retention Directive, is 'wide-ranging' and thus should be considered as 'serious'.[121]

4.2.3 The access to the data by competent national authorities

With regard to the access to the personal data, the Court concluded that 'the access of the competent national authorities constitutes a further interference with the

[120] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others [2014] ECR I-238, para 36.
[121] Ibid, para 37. See also the Opinion of AG Cruz Villalòn in Case C‑293/12 and Case C‑594/12, paras 77 and 80.

fundamental right' protected by Article 8 of the ECHR.[122] Since, personal data of the EU citizens is retained by the Safe-Harbour registered companies and the US competent authorities thus have access to it, the Court's judgment should consequently have had an effect on the SHA, specially after the NSA leaks that proved the US's mass-surveillance. Although, it seems as if the CJEU did not suggest an absolute prohibition against the access of data by competent authorities but rather outlined a necessity for limitation to the national-security exception.

Furthermore, with regard to safeguarding national security as a reason for an exception to this provision, the Court when referring to the AG's Opinion concluded that retaining data and subsequently using it without informing the subscriber or registered user, makes the individuals feel as if 'their private lives are the subject of constant surveillance'.[123]

4.3 Concluding remarks

The fight against serious crimes such as international terrorism and ultimately protections of public security as the material objective of the Data Retention Directive[124] is viewed by the CJEU as an objective of general interest.[125] However, in addition to this, the Court concluded that this type of conduct must not exceed the limits of what is proportionate and necessary in order to achieve the objectives of the Data Retention Directive,[126] since it does not 'in itself justify a retention measure such as that established by [Data Retention Directive] being considered to be necessary for the

[122] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others [2014] ECR I-238, para 35. See also cases from the ECtHR: *Leander v Sweden* [1987], para 48, *Rotaru v Romania* [2000], para 46.
[123] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others [2014] ECR I-238, para 37. See also the Opinion of AG Cruz Villalòn in Case C‑293/12 and Case C‑594/12, paras 52 and 72. In para 72, he concludes: 'the collection and, above all, the retention, in huge databases, of the large quantities of data generated or processed in connection with most of the everyday electronic communications of citizens of the Union constitute a serious interference with the privacy of those individuals, even if they only establish the conditions allowing retrospective scrutiny of their personal and professional activities. The collection of such data establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, none the less constitutes a permanent threat throughout the data retention period to the right of citizens of the Union to confidentiality in their private lives. The vague feeling of surveillance created raises very acutely the question of the data retention period.' This reasoning has undeniably had effects on the outcome of *Schrems v Data Protection Commissioner* as the CJEU had to deal with the same matter.
[124] Directive 2006/24/EC, Article 1(1).
[125] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others [2014] ECR I-238, paras 41-42, 44.
[126] Ibid, para 46.

purpose of that fight'.[127] The Court's conclusion was that the EU legislature, by adopting Directive 2006/24/EC, exceeded the limits of proportionality in the light of Articles 7, 8 and 52(1) of the Charter in order to achieve the objective. With regard to the foregoing considerations, it could have been predicted that the SHA would face challenges after the CJEU's Data Retention ruling.

[127] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others [2014] ECR I-238, para 51.

5 CJEU's Safe Harbour-ruling

5.1 Background

The users of the social network Facebook residing in the European Union are asked to sign a contract with Facebook Ireland Ltd, which is a subsidiary of the parent company Facebook Inc. that is established in the US. Personal data belonging to the Facebook-Ireland's users is accordingly transferred to the servers of Facebook USA in the US where they are kept. In 25 June 2013, Mr Schrems, an Austrian national residing in Austria and a subscriber to Facebook since 2008, lodged a complaint with the Data Protection Commissioner, claiming that the law and practice of the US does not offer any real protection against surveillance of the personal data kept in the US. Mr Schrems' complaint was based on the revelations made by Edward Snowden, according to whom the NSA obtains unrestricted access to mass data stored on the servers in the US, under a program called 'PRISM'.

However, since the Commissioner viewed that he was not required to investigate the matters raised by Mr Schrems in the complaint, he rejected the case as unfounded. The Commissioner considered that 'there was no evidence that Mr Schrems' personal data had been accessed by the NSA [and further] added that the allegations raised by Mr Schrems in his complaint could not be profitably put forward since any question of the adequacy of data protection in the [US] had to be determined in accordance with Decision 2000/520/EC and the Commission had found in that Decision that the [US] ensured an adequate level of protection'.[128]

Consequently, Mr Schrems brought an action before the High Court of Ireland challenging the decision at hand in the main proceedings. After evaluating the evidence offered by the parties to the main proceedings, the High Court found that 'the electronic surveillance and interception of personal data transferred from the [EU] to the [US] serve necessary and indispensable objectives in the public interest'.[129] Nonetheless, the Court added that the revelations made by Edward Snowden had confirmed a 'significant over-reach' on the part of the NSA and other federal agencies,[130] concluding that 'the

[128] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), para 29.
[129] Ibid, para 30.
[130] Ibid.

mass and undifferentiated accessing of personal data is [evidently] contrary to the principle of proportionality and the fundamental values protected by the Irish Constitution'.[131]

Furthermore, according to this Court, 'if the main proceedings were to be disposed of on the basis of Irish law alone, it would then have to be found that, given the existence of a serious doubt as to whether the [US] ensures an adequate level of protection of personal data, the Commissioner should have proceeded to investigate the matter raised by Mr Schrems in his complaint and that the Commissioner was wrong in rejecting the complaint'.[132] The Irish High Court also clarified that the EU citizens have no effective right to be heard with regard to the processing of their personal data. Consequently, this Court considered that Decision 2000/520/EC does not comply with the fundamental right to respect for private life of Article 7 of the Charter, and right to protection of personal data under Article 8 of the Charter, and the principles stemming from the CJEU in the case of *Digital Rights Ireland and Others*. The High Court raised its concern about the right to respect for private life being 'rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on considerations of national security and the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards'.[133]

Although Mr Schrems had not formally contested the validity of either Directive 95/45 or Decision 2000/520/EC, the High Court viewed that he in his action raised the question of the legality of the Safe Harbour. Consequently, the question that was raised according to the Irish High Court was as to whether: 'on account of Article 25(6) of Directive 95/46, the Commissioner was bound by the Commission's finding in Decision 2000/520/EC that the [US] ensures an adequate level of protection or whether Article 8 of the Charter authorised the Commissioner to break free, if appropriate, from such a finding'.[134]

[131] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), para 33.
[132] Ibid.
[133] Ibid, para 34.
[134] Ibid, para 35.

Hence, the following questions were referred to the CJEU by the Irish High Court:

(1) The power of the national supervisory authorities; as to whether and to what extent Article 25(6) of Directive 95/46, read in the light of Article 7, 8, and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, prevents a supervisory authority of a Member State, within the meaning of Article 28 of that Directive, from being able to examine a claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

(2) Or, alternatively, may and/or must the office holder of the national supervisory authorities of the Member States conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?

5.2 Opinion of the Advocate General

5.2.1 The question of validity of Decision 2000/520/EC

The AG concluded in his opinion to the CJEU with regard to *Case C-362/14* that Decision 2000/520/EC by which the Safe Harbour is provided for, must be declared invalid since the US cannot be regarded as ensuring an adequate level of protection for personal data of the EU citizens.[135] The personal data transferred to the companies established in the US, the AG argued, undergo by the law and practice of the US, large-scale access and collection on the basis of 'national security',[136] without the Decision offering any 'appropriate guarantee for preventing mass and generalised access to the transferred data'.[137] Hence, in the way in which the Decision has been applied not having 'clear and precise rules governing the extent of the interference', it allowed the extensive and serious misconducts that violate the fundamental rights of the Charter; the

[135] Opinion of AG Bot in Case C‑362/14, para 216.
[136] Decision 2000/520/EC, point (a) in the fourth paragraph of annex I.
[137] Opinion of AG Bot in Case C‑362/14, para 202.

right to respect for private life of Article 7, and the right to protection of personal data covered by Article 8, he concluded.[138]

Subsequently, the AG evaluated whether the interference is justified in accordance with Article 52(1) of the Charter, which provides that any limitations of the rights and freedoms laid down in the Charter must be legal and respect the essence of those rights and freedoms. Nonetheless, in accordance to the principle of proportionality, a limitation may occur only if they are necessary and genuinely meet the objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others.[139] In this regard, the AG pointed out that the US intelligence authorities make these conducts in a 'generalised' and 'comprehensive' manner, 'without the requirement that the persons concerned represent a threat to national security', arguing that such 'mass, indiscriminate surveillance is inherently disproportionate'.[140] It should also be noted that before the AG represented his conclusion, he also made a reference to the access of the US authorities of the transferred data as having a 'secret nature', stating that this makes the 'interference extremely serious'.[141]

Additionally, the AG highlighted the fact that there is no independent authority within the Safe Harbour scheme, capable of confirming that exceptions from the principles within the framework are limited to what is strictly necessary. Because of this, the EU citizens are not offered any dispute resolution mechanism to request information as to whether the processing of their data is in breach of the Safe Harbour principles, given that the jurisdiction of the FTC only covers 'unfair or deceptive acts and practices in commerce and does [thus] not extend to the collection and use of personal information for non-commercial purposes'.[142] The FTC, according to AG, was 'established … to ensure fair and trustworthy commerce for consumers and not to ensure the protection of privacy right of the individuals' as it is the role of the DPAs under Article 28 of Directive 95/46/EC.

[138] Opinion of AG Bot in Case C‑362/14, para 214.
[139] Ibid, para 176.
[140] Ibid, paras 198-199.
[141] Ibid, para 171.
[142] Ibid, para 205.

Furthermore, in order to emphasise the need and purpose for such mechanism, AG Bot made a reference to the CJEU's view in the Data Retention ruling, maintaining '[it is] sufficient safeguards [with regard to] Article 8(3) of the Charter, to ensure effective protection of the [personal data] against the risk of abuse and against any unlawful access and use of that data'.[143] Moreover, he also concluded that not either the specialist dispute resolution bodies in the US such as TRUSTe and BBBOnline can be approached by the EU citizens since '[they] have no power to rule on the lawfulness of the [actions made by the US] security agencies'.[144] In addition to this he explicitly highlighted the important role of an independent authority seen from an EU perspective by referring to the case law of the CJEU[145] and by using expressions such as 'heart of the European system of personal data protection', subsequently concluding that the existence of an independent authority is necessary for finding the level of protection provided by a third country adequate.[146]

Additionally, the AG argued that the EU citizens are not offered any effective right to be heard with regard to surveillance of their data since the proceedings before the United States Foreign Intelligence Surveillance Court ('FISC') are in secret and *ex parte*, [147] and the protection against the surveillance by the government services according to the US Law:[148] only applies to US citizens and to foreigners who legally reside there permanently.[149] He also concluded that 'rules [governing] privacy in the US may be applied differently to [US] citizens and to foreign citizens'.[150] Moreover, there are neither any possibilities for the EU-citizens 'to obtain access to or rectification or erasure of data, or administrative or judicial redress' with connection to collection and further processing of their personal data in the US under US surveillance

[143] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others [2014] ECR I-238, para 66. See also opinion of AG Bot in Case C‑362/14, para 205.
[144] Ibid, para 206.
[145] Case C-614/10 *Commission v Austria* (ECJ, 16 October 2012), para 37; Case C-293/12 and C-594/12 *Digital Rights Ireland and Others* [2014] ECR I-238, para 68.
[146] Opinion of AG Bot in Case C‑362/14, para 210.
[147] Ibid, paras 172-173, 204.
[148] The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 available at: <https://www.law.cornell.edu/uscode/text/50/1801> accessed 10 November 2015.
[149] Opinion of AG Bot in Case C‑362/14, para 230.
[150] Ibid, para 213. See also C Kuner, *Foreign Nationals and Data Protection Law: A Transatlantic Analysis, Data Protection Anno 2014: How to Restore Trust?* (Intersentia 2014), 213 and 216.

programmes.[151] This condition he viewed as a violation of the EU-citizens' right to an effective remedy protected by Article 47 of the Charter.

5.2.2 The question of ensuring adequacy

Regarding the concept of ensuring an adequate level of protection under Article 25(1) of the Directive 95/46/EC, the AG argued that in order to maintain the adequate level, the third country in question must continue to guarantee such level,[152] since the word 'ensures' is in present tense and factors may change by time.[153] In addition to this, the AG concluded that the Member States and the Commission must constantly stay alert to any change of circumstance and that it is 'appropriate [to] compare [the] assessment with the new circumstances which have arisen since the adequacy decision was adopted', and given the nature of an adequacy decision, it needs to regularly be reviewed by the Commission.[154]

5.2.2.1 The implications of the National-Security exception

The AG elaborated upon the implications that are caused by the national-security exception under the fourth paragraph of Annex I to Decision 2000/520/EC, which provides that '[a]dherence to [the Safe Harbour] Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization'. In this respect, he concluded that 'the US authorities' use of the derogations' under this provision causes problem, since 'their wording is too general [and thus their] implementation … by the US authorities … not limited to what is strictly necessary'.[155] He further emphasised the lack of appropriate US-remedy offered to the EU citizens in case their personal data has been processed for purposes other than those for which it was initially collected and transferred to the US, suggesting

[151] COM (2013) 847, 7 and 2.
[152] Opinion of AG Bot in Case C-362/14, para 211.
[153] Ibid, para 160.
[154] Ibid, paras 136 and 137.
[155] Ibid, para 164.

that for requirements of national security, there should exist an independent control mechanism preventing violations of the right to private life.[156]

Furthermore, assessing whether Facebook has breached the Safe Harbour principles by handing over the personal data to the US authorities, the AG was of the view that since the Company established in the US has done so in order to comply with the US legislation, something which is accepted under the national security provision provided for in the Decision 2000/250/EC,[157] it can thus not be seen as a violation of the Safe Harbour principles.[158] This provision was later also collaborated upon by the CJEU in the Safe Harbour ruling.

5.2.3 The role of the Member State DPAs and the Commission

When referring to Article 51(1) of the Charter, the AG concluded that protection of personal data under Directive 95/46/EC and Article 8 of the Charter, places obligation on not only the Member States but also on the EU institutions.[159] He further added that in determining the level of protection ensured by the third country, the Commission is not only obliged to examine the internal laws and international commitments of the third country in question on the basis of Article 25(6) of Directive 95/46/EC, but it also has to examine the manner in which the protection of the personal data is guaranteed in practice.[160] In this regard, the AG criticised[161] the Commission for failing to suspend the SHA in the meantime negotiations were being held with the US because the adequacy had been brought into question.[162] The AG further emphasised on the Commission's duty to make amendment to the rules whenever new information has come forth concluding that the Commission's failure to act when fundamental rights of the Charter were violated, make an additional ground for the invalidation of Decision 2000/520/EC.[163]

[156] Opinion of AG Bot in Case C-362/14, para 166.
[157] Decision 2000/520 Part B of annex IV: 'Where US law imposes a conflicting obligation, US organisations whether in the safe harbor or not must comply with the law'.
[158] Opinion of AG Bot in Case C-362/14, para 168.
[159] Ibid, para 226.
[160] Ibid, para 227.
[161] Ibid, paras 229 and 234.
[162] COM (2013) 847, para 7.2.
[163] Opinion of AG Bot in Case C-362/14, paras 235-236.

Furthermore, with regard to the Member States' obligation, the AG maintained that their obligation mainly consists of ensuring compliance with the provision of Directive 95/46/EC, by the undertakings of their DPAs.[164] The Member States are also obliged to 'take the measures necessary to prevent any transfer of data … to the third country in question' if the country does not offer an adequate level of protection in accordance with Article 31(2) of the Data Protection Directive.[165]

5.3 The CJEU's ruling

In its judgement the CJEU invalidated the Safe Harbour Decision on two grounds. Firstly, the Court invalidated Article 1 of the Decision since it failed to comply with the requirements under Article 25(6) of Directive 95/46/EC, read in the light of the Charter. Secondly, it invalidated Article 3 of the Decision since it exceeded the power, which is conferred upon the Commission under Article 25(6) of Directive 95/46, read in the light of the Charter. Consequently, since these Articles were inseparable from Article 2 and 4 of that decision and the annexes, their invalidity affected the validity of the decision in its entirety.[166]

5.3.1 The question of the powers of the Data Protection Authorities

With regard to the first question raised by the Irish High Court, the CJEU concluded that no provision of Directive 95/46/EC prevents the DPAs' oversight of transfers of personal data to third countries, which have been the subject of a Commission decision. The Court thus held that the Commission did not have competence to restrict the DPAs' powers in the way it did. The CJEU further viewed that these authorities, when examining a claim within the meaning of Article 28(4) of Directive 95/46/EC, as to whether a transfer of a person's personal data to a third country is in compliance with the requirements under the Data Protection Directive, notwithstanding that the Commission has adopted a decision, must be able to act independently under Article 8(3) of the Charter.[167] In this regard, the Court referring to recital 62 in the preamble to Directive 95/46/EC stressed the fact that the establishment of the independent national supervisory authorities in the Member States is an essential component aiming to

[164] Opinion of AG Bot in Case C-362/14, para 228.
[165] Ibid, para 232.
[166] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), paras 98 and 104-105.
[167] Ibid, para 57.

strengthen the protection of individuals and bodies affected by the decisions of those authorities.[168] Moreover, the CJEU referring to the Court's settled case-law[169] according to which the EU is based on the rule of law in which all acts of its institutions are subject to review of their compatibility with, in particular, the Treaties, general principles of law and fundamental rights, emphasised that the Commission decision adopted pursuant to Article 25(6) of Directive 95/46/EC cannot be excepted from such review.[170]

Furthermore, the Court argued, with reference to Article 25 of Directive 95/46/EC and the AG Opinion, that assessing whether a third country does or does not ensure an adequate level of protection may be made by the Member States or the Commission.[171] However, the Member States cannot adopt measures contrary to the Commission decision unless the Decision is declared invalid by the CJEU since the Court alone has such jurisdiction.[172] Consequently, where a DPA or the person who has brought the matter before the DPA considers that validity of a Commission decision should be called into question, that DPA or person must be provided by the Member States the possibility to bring proceedings before the national courts. In this respect, the Court recalled that the national courts are not endowed with the power to declare a EU act invalid but they are rather able to, pursuant to Article 267 of TFEU, request for a preliminary ruling from the CJEU.[173]

5.3.2 The question of validity of Decision 2000/520/EC

After evaluating the first question, the CJEU went on to examine whether Decision 2000/520/EC complies with the requirements stemming from Directive 95/46/EC read in the light of the Charter. In this regard, the Court concluded that the Commission had the obligation to find whether the US ensures, by reason of its domestic law or its international commitments, which the Court views is clear from the wording of Article 25(6) of Directive 95/46/EC, a level of protection of fundamental rights equivalent to that guaranteed within the EU under Directive 95/46/EC read in the light of the

[168] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), paras 47, 50 and 52.
[169] See Joined Cases C-584/10 P, C-593/10 P and C-595/10 *Commission and Others v Kadi* (ECJ, 18 July 2013), para 66; Case C-583/11 *Inuit Tapiriit Kanatami and Others v Parliament and Council* [2013] ECR I-0000, para 99 and Case C-274/12 *Telefónica v Commission* [2013] ECR I-0000, para 56.
[170] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), para 60.
[171] Opinion of AG Bot in Case C-362/14, para 86.
[172] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), para 61.
[173] Ibid, para 62.

Charter.[174] The Court viewed that the Commission only examined the SHA and did not make such a finding since it did not conclude in Decision 2000/520/EC that the US in fact ensures an adequate level of protection.[175] Hence, without examining the content of the Safe Harbour principles any further, the Court concluded that Article 1 of Decision 2000/520 failed to comply with the requirements under Article 25(6) of Directive 95/46/EC, read in the light of the Charter, and it is thus invalid.[176] The Court further ruled that likewise Article 3 of the Safe Harbour Decision is invalid since it restricts the DPAs' powers with regard to examining whether a third country's ensuring adequate level of protection, if it has been called into question, is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals.[177] Hence, since Article 1 and 3 of the Decision were inseparable from Articles 2 and 4 and the annexes thereto, their invalidity affected the validity of the Decision in its entirety.[178]

5.3.2.1 Complications with the National-Security exception

The Court further observed, referring to the provision in Part B of Annex IV to Decision 2000/520 that the national security, public interest and law enforcement requirements of the US have primacy over the Safe-Harbour principles. The provision reads as follows:

> *(a) Authorization*
>
> *Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.*

This is to the extend that US companies that receive personal data from the EU are bound to without limitation disregard the Safe-Harbour principles, where US law imposes a conflicting obligation.[179] Hence, the Court referring to the 'general nature of the derogation' under fourth paragraph of Annex I to Decision concluded that the SHA enabled interference by US public authorities, with the fundamental rights of the Charter, and the Commission Decision failed to provide any reference to any

[174] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), paras 74-75.
[175] Ibid, para 97.
[176] Ibid, para 98.
[177] Ibid, paras 102-104.
[178] Ibid, para 105.
[179] Ibid, paras 85-86.

regulations in the US that can limit such interference or to provide effective legal protection against the interference.[180] Practically, the provision under Decision 2000/520/EC enabled the NSA to operate as it did under 50 U.S. Code § 1881a, which regulates procedures for targeting certain persons outside the US other than US citizens. In connection to this, the Court also emphasised the fact that when establishing the existence of interference, 'it does not matter whether the information relating to private life [of the individual] is sensitive or whether the persons concerned have suffered any adverse consequences because of the interference'.[181]

Furthermore, the Court concluded that its foregoing analysis of Decision 200/520/EC originated from the Commission's own assessment of the situation that resulted in the two Commission Communications[182] according to which 'the [US] authorities were able to access the personal data transferred from the Member States to the [US] and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security'.[183] Additionally, the Commission noted that individuals concerned had 'no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased'.[184]

Moreover, with regard to the level of protection equivalent to the fundamental rights and freedoms guaranteed within the EU, the CJEU found that, under EU law, 'legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data is transferred from the EU to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of its subsequent use, for purposes which are specific, strictly

[180] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), para 87.
[181] Ibid, para 87. See also the CJEU discussing the matter in the same way in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others [2014] ECR I-238, para 33 and Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989, para 75.
[182] Communication from the Commission to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final, 27 November 2013) and Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM(2013) 847 final, 27 November 2013).
[183] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), paras 90.
[184] Ibid.

restricted and capable of justifying the interference which both access to that data and its use entail'.[185] The Court further added that 'legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life under Article 7 of the Charter'.[186]

In connection to the foregoing reasoning, the CJEU once again referred to its previous judgment in the case of *Digital Rights Ireland and Others* where the Court argued that 'whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences'.[187] In addition to this, the Court also discussed about the existence of 'general absence of limits' in Directive 2006/24/EC, which enabled competent national authorities to interfere with fundamental rights of Article 7 and 8 of the Charter.[188] Hence, since there have been similarities between the way Directive 2006/24/EC enabled interference with the fundamental rights of Article 7 and 8 of the Charter, and Decision 2000/520/EC it could be argued that the Court has evidently followed up with its previous view which was expressed in the case of *Digital Rights Ireland and Others*.

5.3.2.2 Interference with Article 47 of the Charter

Article 47 of the Charter gives everyone whose rights and freedoms are guaranteed by the law of the EU, the right to an effective remedy and a fair trial, in case these rights have been violated. As far as Article 47 of the Charter is concerned, the Court observed that 'legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data' compromises the essence of this fundamental right,

[185] Case C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015), para 93.
[186] Ibid, para 94. See also CJEU's arguments in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others [2014] ECR I-238, para 39.
[187] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others [2014] ECR I-238, para 59.
[188] Ibid, para 60.

which is an important component of the rule of law.[189] Given that the Safe Harbour Decision did not contain sufficient finding in this regard, the CJEU concluded that the Decision also interfered with Article 47 of the Charter.

[189] Case C-362/14 Schrems v Data Protection Commissioner (ECJ, 6 October 2015), para 95.

6 Final Discussion

This thesis has demonstrated the difficulty of finding a legal and effective system for the transfer of personal data from the EU to the US, when the legal regimes governing this area in Europe and the US differ from each other. As it has been outlined, after the NSA leaks, the CJEU has examined, whether the SHA under Decision 2000/520/EC has been compatible with the fundamental rights of Article 7 and 8 of the Charter, namely the right to private life and protection of personal data. The Court's previous judgment in the case of *Digital Rights Ireland and Others* and its persistent reference to this case in the case of *Schrems v Data Protection Commissioner* proves the fact that the SHA would, as a result of the Court's consistency with its precedents, become challenged. Subsequently, as the CJEU has invalidated Decision 2000/520/EC, transfer of personal data between the EU and the US can no longer be carried out through the Safe Harbour.

However, consequently, the question after the suspension of the Safe Harbour Decision is how the transfer of personal data of EU citizens to the US can be protected from surveillance that goes beyond 'obligations on the necessary oversight of access by public authorities, on transparency, on proportionality, on redress mechanisms and on data protection rights [under EU law]'.[190] Moreover, other appropriate questions should be raised with regard to the current situation: Do the other alternatives for transatlantic transfer of EU citizens' personal data, which are being used in the meantime, offer a better protection than the Safe Harbour did? Will the personal data of the EU citizens be more protected if the personal data would be prohibited from being transferred to the US, but instead be kept and stored within the EU by US companies?

Some scholars argue that, by requiring a third country to implement an adequate data protection, the Data Protection Directive infringes the sovereignty of these nations.[191] They further view that even though the third countries are not formally required to adopt these rules to ensure adequacy, the practical effect of such a requirement is an

[190] Statement of the Article 29 Working Party of 16 October 2015 on the implementation of the judgment of the Court of Justice of the European Union of 6 October 2015 in the *Maximilian Schrems v Data Protection Commissioner* case (C-362-14), available at: <http://ec.europa.eu/justice/data-protection/article29/pressmaterial/pressrelease/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf> accessed 10 November 2015.

[191] J S Bauchner, *State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate* (2000) Vol. 26, No. 2, Brooklyn Journal of International Law, 689.

impulsion upon any third country seeking to transfer personal data from the EU.[192] This argument could be viewed as not far from the truth, however, when the fundamental rights of the individuals are at stake, maybe it is permissible to infringe the sovereignty of a third country. After all, the very primary focus of the law should not be the data or their processing but the data subject, and this fundamental right should not be protected solely through the protection of personal data but also with other means.[193]

With regard to EU's role in regulating data protection, Andrej Savin argues, that the EU's attempts to regulate the Internet may appear as confusing, with numerous instruments, difficult policies hard to distinguish, and incoherent proposals, concluding that the reason for this is not only 'systematic or bureaucratic failures', but also the fact that the Internet allows participation, '[turning] passive consumers into active players and contributors'.[194] He further refers to McLuhan's *global village*,[195] arguing that 'the implications of such a new global village for the economy and the society at large are as yet unknown'.[196] Perhaps he is right in his conclusion. The impact of this so-called global village has in fact been unknown and the EU citizens are victims of EU's failures and the outcome of the Safe Harbour Decision is a proof of that. Given such a finding of infringements of the fundamental rights of EU citizens, it is surprising that the Safe Harbour was not suspended sooner. As aforementioned reference to the Commission Vice-President Viviane Reding's presumption in her statement with regard to the Safe Harbour after the NSA leaks, she was right about the SHA being a loophole. The Safe Harbour Decision in fact turned out to be a loophole and it would be justified to examine whether the other alternative tools for transatlantic personal data transfers under Directive 95/46/EC that the Commission has imposed,[197] in the absence of an adequacy decision, are not loopholes too. And additionally, which renewed agreements

[192] L Colonna, *Article 4 of the EU Data Protection Directive and the irrelevance of the EU-US Safe Harbour Program?* (2014) Vol. 4, No. 3, International Data Privacy Law, 204.
[193] R Polcak, *Getting European data protection off the ground* (2014), Vol. 4, No. 4, International Data Privacy Law, 289.
[194] A Savin, *EU Internet Law* (Edward Elgar publishing 2013), x.
[195] McLuhan, a Canadian writer, expressed his concern about the new technologies of information and communication that will transform the world into one big village: 'Such is the character of a village or, since electric media, such is also the character of global village. And it is the advertising and PR community that is most aware of this basic new dimension of global interdependence.', McLuhan, *The Gutenberg galaxy: The making of typographic man* (McGraw-Hill 1962), 31.
[196] A Savin, *EU Internet Law* (Edward Elgar publishing 2013), x.
[197] COM (2015) 566.

would ever not be a loophole when it comes to cooperation with the US as far as the protection of privacy and personal data are concerned?

In its Communication with regard to the suspension of the Safe Harbour Decision, the Commission concludes that 'it has immediately resumed and stepped up its talks with the U.S. government in order to ensure that any new arrangement for transatlantic transfers of personal data fully complies with the standard set by the [CJEU]'.[198] Furthermore, as a basis for personal data transfers, the Commission, referring to a recent Statement from the WP29 and its own previous Communications,[199] suggests that Standard Contractual Clauses[200] and Binding Corporate Rules[201] may be used in the meantime, in compliance with Article 26 of Directive 95/46/EC.[202]

However, under Article 26(1) of Directive 95/46/EC, the suggested proposals will still provide for one of the alternative derogations from the general prohibition of transferring personal data to entities in a third country that do not offer an adequate level of protection under recital 57.[203] One ground for the derogation according to the

[198] COM (2015) 566, 3.
[199] Ibid, 4. See also the Statement of the Article 29 Working Party on the implementation of the judgment of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14), available at: <http://ec.europa.eu/justice/dataprotection/article-29/press-material/press release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf> accessed 10 November 2015.
[200] A set of four SCCs where two sets of model clauses relate to transfers between controllers. See COM (2015) 566 final, 6 November 2015, 6; Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, OJ L 181, 4.7.2001, 19 and Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 29.12.2004, 74. The other two sets of these model clauses concern transfers between a controller and a processor acting under its instructions. See Commission Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 6, 10.1.2002, 52 and Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 12.2.2010, 5. The former decision, which was repealed by the latter, applies only to contracts concluded before 15 May 2010.
[201] Intra-group transfers for multinational companies, which provide only for transfers made within the corporate group. COM (2015) 566, 7–8: 'These rules are not only binding on the members of the corporate group but, similarly to the SCCs, they are also enforceable in the EU: individuals whose data are being processed by an entity of the group shall be entitled as third-party beneficiaries to enforce compliance with BCRs by lodging a complaint before a Data and bringing an action before a Member State court. Furthermore, the BCRs must designate an entity within the EU which accepts liability for breaches of the rules by any member of the group outside of the EU which is bound by these rules.'
[202] COM (2015) 566, 8–9.
[203] Ibid.

aforementioned Article is, if 'the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims'.[204] And therein lies the on-going struggle between the EU and the US, which takes the EU back to the loophole, since the US in this case could still gain access to the EU citizens' personal data under this provision, for the purposes of national security or war on terrorism. In such case, it would be appropriate to find out whether the WP29 non-binding guidance documents[205] on the application of Article 26(1) of Directive 95/46/EC, which the Commission refers to as a safeguard,[206] will, in spite of the existence of these derogations, *de facto* help protect the fundamental rights to privacy and data protection under the Charter from being violated by the third party (in this case, the US).

Currently, the EU is working on creating a data protection reform that will result in the General Data Protection Regulation ('GDPR'), which aims to update and modernise the current data protection rules, improve the level of data protection with regard to the processing of individuals' data and increase the business opportunities within the digital single market. This reform is 'a legislative package proposed by the Commission[207] in 2012 … concern[ing] two legislative instruments: the general data protection regulation (intended to replace directive 95/46/EC) and the data protection directive in the area of law enforcement (intended to replace the 2008 data protection framework decision)'.[208] It should be noted that the WP29 has with regard to this proposal raised its concern on the current Council text of the draft directive, concluding that 'it does not ensure that interferences in the private life of individuals and in the right to protection of personal

[204] Directive 95/46/EC, art 26(1) d.
[205] Article 29 Working Party, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 November 2005, 7 and 17; Working Document: *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (WP 12), 24 July 1998; Working document *on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 November 2005. See also European Commission, *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries* (FAQ D.1 to D.9), 48–54.
[206] COM (2015) 566, 14.
[207] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final, 25 January 2012.
[208] Council of the European Union, Press Release No 951/15, Luxembourg, 18 December 2015, available at: <http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-data-protection/> accessed 10 November 2015.

data are limited to what is strictly necessary',[209] arguing that 'personal data processed in a law enforcement context could be further processed for incompatible purposes… Should these shortcomings remain in the final text of the directive, it could have highly detrimental consequences for individuals and risks that the text is contrary to both Article 8 of the European Convention of Human Rights, Articles 7 and 8 of the Charter, the European Convention for the protection of individuals with regard to automatic processing of personal data'.[210]

Among the objectives for WP29's criticism are the facts that 'there is no obligation to carry out a data protection impact assessment in advance of setting up new data processing, the rules for the transmission and use of the data to private parties and third countries are not properly defined and data could be used to create profiles or single out a person or a category of persons on the sole basis of sensitive data. Furthermore, with regard to the security of the data processing, risks posed by data breaches are left to the assessment of data controllers and logging is subject to exceptions. Finally, the powers of competent supervisory authorities are insufficiently detailed'.[211] Additionally, the WP29 concludes that 'the introduction of a strict prohibition on the massive, repeated and structured transfers of personal data to third countries authorities and reiterates that exceptions to the prohibition of transfers to inadequate countries should be interpreted restrictively', supporting 'article 36(2)(b) [in the Council text of the draft directive] as introduced by the European Parliament, which states that: "All transfers of personal data decided on the basis of derogations shall be duly justified and shall be limited to what is strictly necessary, and frequent massive transfers of data shall not be allowed"'.[212]

Going back to the loophole-discussion, as mentioned above, it would be of relevance to comprehend how much these new regulations can genuinely help the protection of the EU citizens' personal data. Most likely, the complications connected to the concept of national security will still remain. As long as the US law has primacy over the US companies, is it really possible for the EU to confer EU law on these companies and trust that they will comply with it? Would it even be possible to prohibit these

[209] Opinion 03/2015 of the Article 29 Working Party, available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf> accessed 10 November 2015, 2.
[210] Opinion 03/2015 of the Article 29 Working Party, 3.
[211] Ibid, 2–3.
[212] Ibid, 13.

companies to transfer EU citizens' personal data from the EU to the US, under any circumstances?

It may be noted that the current regulatory conflict between the EU and the US is also problematic for the US companies that have EU citizens as customers. As far as the extraterritorial reach of the US law is concerned, there is currently an on-going case between the Microsoft Corp. and the US.[213] In this case, the Microsoft Corp. has appealed the US Court of Appeals for the Second Circuit, to reverse a 2014 ruling, a search warrant from a federal judge,[214] which would allow federal agents to access a customer's private emails on a computer in Dublin, Ireland, where they are protected by Irish and EU law. Microsoft is arguing that an Act of Congress does not apply outside the US as 'a presumption against extraterritoriality', unless it clearly doesn't say so. Hence, since this warrant 'orders a law enforcement seizure in Ireland, it calls for an unauthorized extraterritorial application of § 2703(a)'.[215] For the government's part, the Department of Justice lawyers have told to the federal appeals court that the US government has the right to demand the emails of anyone in the world from any email provider headquartered within US borders.[216] It may also be mentioned that other software companies such as Apple are supporting Microsoft in this case.

The outcome of this case will be of great importance, as it will determine the extent of the territorial reach of the US law, and thus have crucial effect in regards to the creation of a renewed agreement between the EU and the US for transfers of personal data of the

[213] Microsoft Corporation v. the United States of America, Case 14-2985, Document 47, 12/08/2014, 1387372, available at: <http://www.chamberlitigation.com/sites/default/files/cases/files/2014/Appellant%20Brief%20--%20Microsoft%20Corporation%20v.%20U.S.%20(Second%20Circuit).pdf> accessed 10 November 2015.

[214] This warrant is issued under the Electronic Communications Privacy Act, 18 U.S. Code § 2703(a) which reads as follows: 'A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.' Available at: <https://www.law.cornell.edu/uscode/text/18/2703> accessed 10 November 2015.

[215] Microsoft Corporation v. the United States of America, Case 14-2985, Document 47, 12/08/2014, 1387372, 14–15.

[216] Available at: <http://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant> accessed 10 November 2015.

EU citizens. Given that this warrant would be legal, the EU law will not be able to limit the US from accessing personal data from the EU. It may be noted, that this will also have consequences for the US companies, as it will set the standards for the level of privacy protection they will be able to offer their customers. Practically, the US companies have currently two options, to either, comply with the US law and break the EU law, or to comply with the EU law and violate the US law. It is worthy to be mentioned that, the fact that Microsoft has chosen to take this battle is a positive step with regard to protection of privacy and personal data, as it shows that the US corporations have realised that the conducts of the US government is not acceptable in the EU and is putting their businesses at stake. Perhaps, this will add further pressure on the US government to change its conducts to become more in compliance with EU law.

However, there are a few more obstacles with regard to protection of privacy and personal data of EU citizens' in relation to the US. In a case of threat against the national security, there are numbers of means that the US governments is currently able to use in addition to those available in an ordinary criminal case. One of them is the National Security Letters ('NSLs'),[217] which are a specific type of administrative subpoena issued by the Federal Bureau of Investigation ('FBI') 'to wire or electronic communication service providers to obtain subscriber information, billing records, or electronic communication transaction records'.[218] These letters are issued without a warrant, subpoena, or other court supervision, usually forbidding the recipient from disclosing even the existence of it, much less the target or nature of the request.[219] The constitutionality of these nondisclosure orders has repeatedly been challenged in the US but they are still in force and their use has in fact dramatically increased[220] in the years following the adoption of the USA Patriot Act of 2001.[221] Given, the NSLs could be

[217] See 18 U.S. Code § 3511 - Judicial review of requests for information, available at: <https://www.law.cornell.edu/uscode/text/18/3511> accessed 10 November 2015 and 18 U.S. Code § 2709 - Counterintelligence access to telephone toll and transactional records, available at: <https://www.law.cornell.edu/uscode/text/18/2709> accessed 10 November 2015.
[218] European Parliament Directorate General for Internal Policies, Policy Department C: Citizens' rights and Constitutional Affairs, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*, 21, available at: <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU(2015)519215_EN.pdf> accessed 10 November 2015. See also G H Pike, *The Future of National Security Letters*, 22.
[219] G H Pike, *The Future of National Security Letters* (2013), Vol. 30, No. 5, Information Today, 22.
[220] Ibid, 22.
[221] European Parliament Directorate-General for International Policies, Policy Department C: Citizens' rights and Constitutional Affairs, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*, 21.

used by the US to receive personal data of EU citizens through US companies, specially when their use has been under question, is another threat against the protection of EU citizens' fundamental right to privacy and personal data. Especially when this can occur without the knowledge of the EU or the individual in question. It should also be noted that there are two more means that the US can use in order to access personal data of the EU citizens, in a case of threat against national security, namely through surveillance authorised under the Foreign Intelligence Surveillance Act ('FISA')[222] and Executive Order 12,333 ('E.O. 12,333').[223]

It is a major concern that the EU does not clearly point out the existence of the NSLs as constitutionally challenged mean, which might be violating EU law at this very moment without the EU even having any knowledge about it, and likewise the two other abovementioned US national security investigation measures. It is also distressing that neither the Commission nor the WP29 mention anything about the existence of these measures and the threat they are toward the protection of privacy and personal data of EU citizens, in connection to the creation of a renewed framework after the suspension of the Safe Harbour Decision. In addition, with regard to all the aforementioned shortcomings of the Safe Harbour Decision, it should have been obvious for the Commission that the SHA would enable violation of the fundamental rights of the Charter. Hence, it should have not even come to existence from the very beginning.

With regard to the forgoing considerations, it seems as if the EU has from the very beginning known about the primacy of the US judiciary over the US companies that operate within the EU and its consequences for privacy and personal data protection, but it has not wanted to officially acknowledge these facts. On the surface, with the suspension of the Data Retention Directive and the Safe Harbour Decision and all the strict-toned new proposals, it seems as if the EU is dictating the terms in this power struggle over the protection of EU citizens' personal data. However, as a matter of fact,

[222] This Act is adopted by Congress and regulates surveillance designed to protect against the activities of foreign powers or their agents inside the US. For more details see Policy Department C: Citizens' rights and Constitutional Affairs, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*, 21–22.

[223] Proclaimed by the President and regulates surveillance outside the US as well as other residual forms of surveillance. For more details see Policy Department C: Citizens' rights and Constitutional Affairs, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*, 22–27.

the party dictating the terms is the US. Could it be that the EU's reactions are perhaps a reflection of its own path toward becoming a counter terrorism actor? If that would be the case, it would of course not be appropriate to criticise the US too much.

However, it is understandable that with an unsafe world and the existence of the Internet, where a great amount of criminal activities take place, the need for strong national and international security and public safety is as vital as the protection of privacy and the personal data of the individuals. Since the recent terrorist attacks on the EU territory, it may not be unlikely that the EU will increase its anti-terrorism measures. Hence, the EU could be moving in the same direction as the US and might not be any less invasive in surveillance operations and a more invasive EU Data Protection law is most probably at hand. In such case, according to the national security exception provided for in Article 13(1) of Directive 95/46/EC, the Member States have the ability to adopt legislative measures to restrict the scope of obligations and rights of Article 6(1), 10, 11(1), 12 and 21 of the Data Protection Directive, when such restriction constitutes a necessary measures to safeguard national security, defence and public security etc.

Moreover, in this regard, the Council of the EU explains the EU counter-terrorism strategy as covering four strands of work: Prevent, Protect, Pursue and Respond, fitting its strategic commitment to combat terrorism globally while respecting human rights, and make Europe safer, allowing its citizens to live free in an area of freedom, security and justice.[224] The Member States have further the primary responsibility for combating terrorism, with the EU adding values in four main ways: strengthening national capabilities, facilitating European cooperation, developing collective capability and promoting international partnership.[225] It should be mentioned that with regard to promoting international partnership, the EU encourages Member States to particularly cooperate with the US.[226] This may also be one of the reasons for the EU's unofficial passivity with regards to protection of the EU citizens' right to privacy and personal data, in relation to the US.

[224] Council of the European Union, *EU Counter-Terrorism Strategy*, 14469/4/05 REV 4, Brussels, 30 November 2005, 3, available at: <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204> accessed 5 January 2016.
[225] Ibid, 4.
[226] Ibid.

7 Conclusions

In this thesis, the challenges facing the fundamental rights to privacy and personal data protection of the EU in their relations with the US have been described. Although on the surface it seems as if the EU is dictating the terms, the US is in fact the real dictating party in the current situation, since it is able to maintain the loopholes with its current law. As a matter of fact, the EU is way too dependent to the relations with this great Power, to on its own, make any changes that would give major economical, political and social consequences. After all, it is a matter of individuals' right versus economical might. It would not be realistic that EU citizens become prohibited from using services provided by US companies, since large numbers of EU citizens are already subscribers to American companies, which completely dominate the world market, such as Facebook and Google. Moreover, if the EU itself is taking a further step to becoming a counter-terrorism actor cooperating with the US, maybe in fact it is not that interested in pointing more fingers at the US. However, if such changes would occur with the EU law, a new transatlantic agreement would not be needed, since the protection for privacy and personal data would be at the same level in both continents.

With regard to all the foregoing considerations, a renewed EU Data Regulation will indubitably have no effect for the protection of EU citizens' personal data from access and surveillance by the US as long as the US law has primacy over US companies. As far as the global village is concerned, the Internet is here to stay and its impacts are still unknown. Hence, the only genuine options to the problem of privacy and data protection in accordance with the Charter would be if the US laws would become compatible with those of EU, or the parties would agree on an International Convention[227] with an independent tribunal, which would bind all the parties to respect the same fundamental rights. Nevertheless, it may be likely, that an invalidated Safe Harbour Decision and a need for American corporations to provide acceptable terms for their EU-users will lead to a broader anti-terrorism cooperation agreement between the EU and the US instead of a renewed data protection agreement.

[227] C Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013), 33.

Bibliography

Table of Legislation

Union Legislation

Primary law

The Charter of Fundamental Rights of the European Union [2012] OJ C326/02

Consolidated Version of the Treaty on the European Union [2012] OJ C326/01

Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/47

Secondary law

Council Regulation (EC) No 182/2011 of 16 February 2011 on laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers [2011] OJ L55/13

Council Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11

Council 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, [2006] OJ L105/54

Council 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 L201/37

Council 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, [2001] OJ L8/1

Council 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, [1995] OJ L281/31

The Council of Europe

The Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos 11 and 14 and supplemented by Protocols Nos 1, 4, 6, 7, 12 and 13 Rome 4.XI.1950

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe Convention 108), 28 January 1981, ETS 108 (1981)

Official Documents

Opinion 03/2015 of the Article 29 Working Party on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 1 December 2015

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), COM (2015) 566 final, 6 November 2015

Statement of the Article 29 Working Party on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14), 16 October 2015

European Parliament Directorate General for Internal Policies, Policy Department C: Citizens' rights and Constitutional Affairs, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*, Study for the LIBE Committee, 2015, available at: <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU(2015)519215_EN.pdf> accessed 17 November 2015

Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM (2013) 847 final, 27 November 2013

Communication from the Commission to the European Parliament and the Council entitled *Rebuilding Trust in EU-US Data Flows*, COM (2013) 846 final, 27 November 2013

Commission Memorandum *Restoring Trust in EU-US data flows – Frequently Asked Questions,* MEMO/13/1059, 27 November 2013

Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final, 25 January 2012

European Commission, *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries*, available at: <http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf> accessed 10 November 2015

Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, (notified under document C(2010) 593) (Text with EEA relevance) (2010/87/EU) OJ L 39, 12.2.2010

Article 29 Working Party, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114), 25 November 2005

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60

Council of the European Union, EU Counter-terrorism Strategy, 14469/4/05 REV 4, Brussels, 30 November 2005

Commission Decision (2004/915/EC) of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 29.12.2004

Decision NO 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data-protection Supervisor's duties, [2002] OJ L183/1

Commission Decision (2002/16/EC) of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 6, 10.1.2002

Commission Decision (2001/497/EC) of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, OJ L 181, 4.7.2001

Commission Decision (2000/520/EC) 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. OJ 2000 L 215, p.7

Article 29 Data Protection Working Party, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, at 9, (WP 168), 1 December 2009

Article 29 Working Party, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (WP 12), 24 July 1998

US law

Federal Statues

The Electronic Communications Privacy Act of 1986, 18 U.S.C § 2703, available at: <https://www.law.cornell.edu/uscode/text/18/2703> accessed 10 November 2015

The Federal Trade Commission Act of 1914, 15 U.S.C § 45, available at: <https://www.law.cornell.edu/uscode/text/15/45> accessed 10 November 2015

The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801, available at: <https://www.law.cornell.edu/uscode/text/50/1801> accessed 15 November 2015

Unfair and deceptive practices and unfair methods of competition under 49 U.S.C Code § 41712, available at: <https://www.law.cornell.edu/uscode/text/49/41712> accessed 10 November 2015

Procedures for targeting certain persons outside the United States other than United States persons under 50 U.S.C § 1881a, available at: <https://www.law.cornell.edu/uscode/text/50/1881a> accessed 27 November 2015

Judicial review of requests for information under 18 U.S. Code § 3511, available at: <https://www.law.cornell.edu/uscode/text/18/3511> accessed 10 November 2015

Counterintelligence access to telephone toll and transactional records under 18 U.S. Code § 2709, available at: <https://www.law.cornell.edu/uscode/text/18/2709> accessed 10 December 2015

Textbooks

Bygrave L, *Data protection Law: Approaching its Rationale, Logic and Limits* (1 edn, Kluwer Law International 2002)

Carey P, *Data Protection A Practical Guide to UK and EU Law* (4th edn, Oxford University Press 2015)

Gonález Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Law Governance and Technology Series 16, Springer International Publishing 2014)

Gutwirth S, Poullet Y, de Hert P, de Terwangne C and Nouwt S, *Reinventing Data Protection?* (Springer 2009)

Hettne J and Otken Eriksson I, *EU-rättslig metod – Teori och genomslag i svensk rättstillämpning* (2nd edn, Nordstedts Juridik AB 2011)

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

Kuner C, *Foreign Nationals and Data Protection Law: A Transatlantic Analysis, Data Protection Anno 2014: How to Restore Trust?* (Intersentia 2014)

McLuhan M, *The Gutenberg galaxy: The making of typographic man* (McGraw-Hill 1962)
Savin A, *EU Internet Law* (Edward Elgar publishing 2013)

Westin A F, *Privacy and Freedom* (originally published in 1967, Atheneum 1970)

Articles

Bamberger K A, Mulligan D K, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices* (2013) Vol. 81, George Washington Law Review 1529

Bauchner J S, *State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate* (2000) Vol. 26, No. 2, Brooklyn Journal of International Law

Charlesworth A, *Clash of the Data Titans? US and EU Data Privacy Regulation* (2000), Vol. 6, No. 2, European Public Law

Colonna L, *Article 4 of the EU Data Protection Directive and the irrelevance of the EU-US Safe Harbour Program?* (2014) Vol. 4, No. 3, International Data Privacy Law

Drezner D W, *The Global Governance of the Internet: Bringing the State Back In* (2004), Vol. 119, No. 3, Political Science Quarterly

Kierkegaard S M, *Safe Harbor Agreement-Boon or Bane?* (2005), Vol. 10 Shidler Journal of Law, Commerce & Technology

Kulesza J, *Walled Gardens of Privacy or 'Binding Corporate Rules?': A Critical Look at International Protection of Online Privacy'* (2012), Vol. 34, No. 4, U. Ark. Little Rock Law Review

Leathers D R, *Giving Bite to the EU-US Data Privacy Safe Harbor: Model Solutions For Effective Enforcement* (2009), Vol. 41:193, No. 1, Case Western Reserve Journal of International Law

Pike G H, *The Future of National Security Letters* (2013), Vol. 30, No. 5, Information Today

Polcak R, *Getting European data protection off the ground* (2014), Vol. 4, No. 4, International Data Privacy Law

Reidenberg J R, *E-Commerce and Trans-Atlantic Privacy* (2001), Vol. 38, No. 3, Houston Law Review

Schriver R R, *You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission* (2002), Vol. 70, No. 6, Fordham Law Review

Soma J T, Rynerson S D and Beall-Eder B D, *An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The US/EU E-Commerce Privacy Safe Harbor* (2004), Vol. 39, No. 2, Texas International Law Journal

Svantesson D J B, *The regulation of cross-border data flows* (2011), Vol. 1, No. 3, International Data Privacy Law

Zaidi K R, *Harmonizing US-EU Online Privacy Laws: Toward a US comprehensive Regime for the Protection of Personal Data* (2003), Vol. 37, No. 2, Syracuse Journal of International Law and Commerce

Table of Cases

The European Union

European Court of Justice

C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989

C-279/09 *Deb v Germany* [2010] ECR I-13849

C-518/07 *Commission v Germany* [2010] ECR I-1885

C-614/10 *Commission v Austria* [2013] 1 CMLR 23

C-584/10, C‑593/10 and C‑595/10 *Commission and Others v Kadi* (ECJ, 18 July 2013)

C-583/11 *Inuit Tapiriit Kanatami and Others v Parliament and Council* [2013] ECR I-0000

C-274/12 P *Telefónica v Commission* [2013] ECR I-0000

C-288/12 *Commission v Hungary* [2014] ECR I-237

C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECR I-238

C-131/12 *Google Spain SL and Google Inc v Agencia Espagnola de Proteccion de Datos (EPD) and Mario Costeja Gonzales* [2014] ECR I-317

C-456/13 T & L Sugars and Sidul Acucares v Commission (ECJ, 28 April 2015)

C-362/14 *Schrems v Data Protection Commissioner* (ECJ, 6 October 2015)

AG Opinions

Opinion of Advocate General Bot delivered on 23 September 2015, Case C‑362/14 *Maximillian Schrems v Data Protection Commissioner*

Opinion of Advocate General Cruz Villalòn delivered on 12 December 2013, Case C‑293/12 and Case C‑594/12 *Digital Rights Ireland and Seitlinger and Others*

Opinion of Advocate General Kokott delivered on 14 April 2011, Case C-110/10 P *Solvay v Commission*

European Court of Human Rights

Klass and others v Germany [1978] app no 5029/71

Malone v United Kingdom [1984] app no 8691/79
Leander v Sweden [1987] app no 9248/81

Niemietz v Germany [1992] app no 13710/88

Bensaid v United Kingdom [1992] app no 44599/98

Amann v Switzerland [2000] app no 27798/95

Rotaru v Romania [2000] app no 28341/95

The United States

Nixon v. Administrator of General Services*,* 433 U.S. 425 (1977), available at: <https://supreme.justia.com/cases/federal/us/433/425/case.html> accessed 10 November 2015.

Microsoft Corporation v. the United States of America, Case 14-2985, Document 47, 12/08/2014, 1387372, available at: <http://www.chamberlitigation.com/sites/default/files/cases/files/2014/Appellant%20Brief%20--%20Microsoft%20Corporation%20v.%20U.S.%20(Second%20Circuit).pdf> accessed 10 November 2015.

Websites

EU

Council of the European Union, Press Release No 951/15, Luxembourg, 18 December 2015, available at: <http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-data-protection/> accessed 5 January 2016

Council of the European Union, EU Counter-Terrorism Strategy, 14469/4/05 REV 4, Brussels, 30 November 2005, 3, available at: <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204> accessed 5 January 2016

American authorities

FTC's Press Release of March 30, 2011, available at: <http://ftc.gov/opa/2011/03/google.shtm> accessed 10 November 2015

US Council of Better Business Bureau, BBB EU Safe Harbor Program, available at: <http://www.bbb.org/council/eusafeharbor/> accessed 10 November 2015

TRUSTe, available at: <http://www.truste.com/business-products/eu-safe-harbor-seal/> accessed 10 November 2015

Media

Traynor I, *New EU rules to curb transfer of data to US after Edward Snowden revelations*, (The Guradian, 17 October 2013), available at: <http://www.theguardian.com/world/2013/oct/17/eu-rules-data-us-edward-snowden> accessed 10 November 2015

Bayer A, *Rescuing personal data from an uNSAfe Harbor - European data protection regulators start taking things into their own hands,* (Wragge Lawrence Graham & Co, 3 March 2015), available at: <http://wragge-law.com/insights/rescuing-personal-data-from-an-unsafe-harbor-european-data-protection-regulators-start-taking-things/> accessed 10 November 2015

Facebook's Privacy Policy titled *How do we respond to legal requests or prevent harm?*, available at: <https://www.facebook.com/policy.php> accessed 10 November 2015

OSCOLA Oxford University Standard for the Citation of Legal Authorities, 4th edn, available at: <http://www.law.ox.ac.uk/published/OSCOLA_4th_edn_Hart_2012.pdf> accessed 10 November 2015