Maastricht University

Maastricht Centre for European Law

Maastricht Centre for European Law

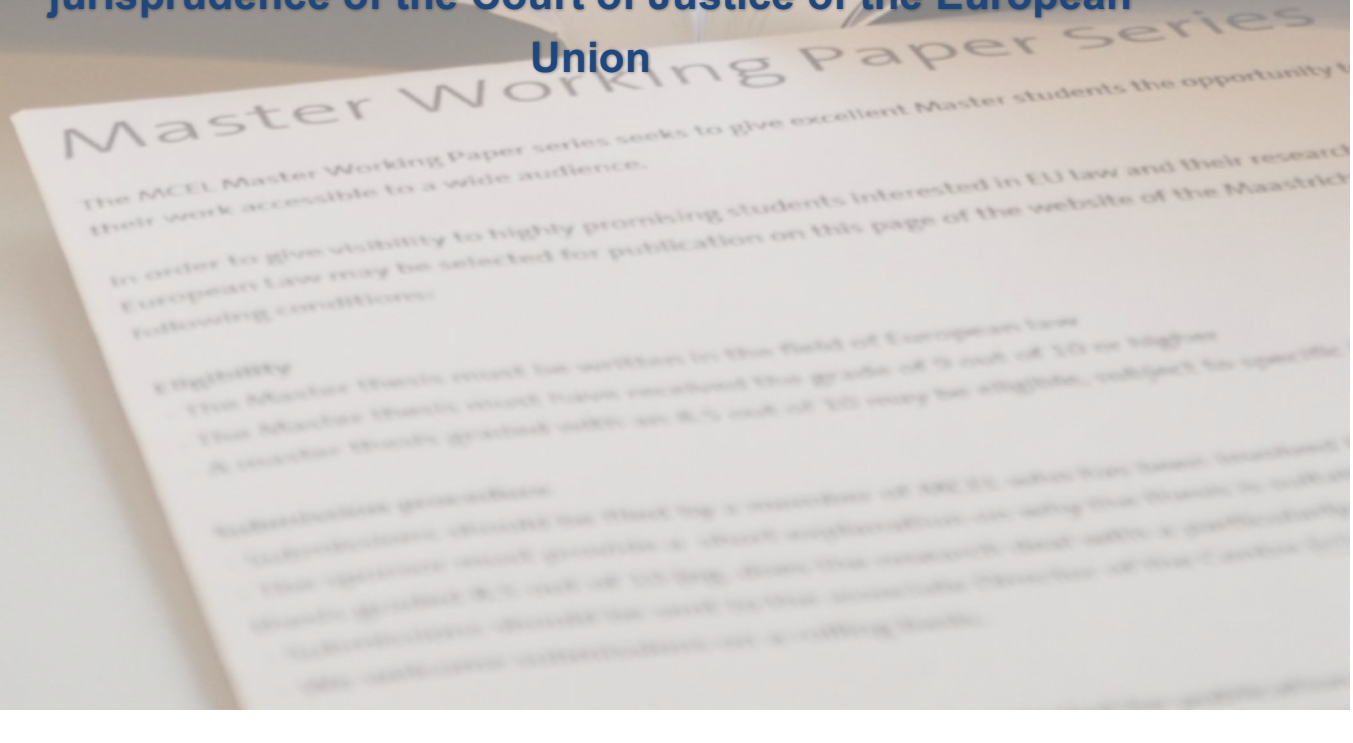
Master Working Paper

2017/1

Sarah Wagner

The Future of Transatlantic Data Flows: Privacy Shield or Privacy Sieve?

An adequacy assessment by reference to the jurisprudence of the Court of Justice of the European Union



The MCEL Master Working Paper series seeks to give excellent Master students the opportunity to publish their final theses and to make their work accessible to a wide audience. Those wishing to submit papers for consideration are invited to send work to: mcel@maastrichtuniversity.nl

Our submission guidelines and further information are available at: http://www.maastrichtuniversity.nl/web/Institutes/MCEL/Publications1/MasterWorkingPapers.htm

Published in Maastricht, April 2017

Faculty of Law

Maastricht University

Postbox 616

6200 MD

Maastricht

The Netherlands

This paper is to be cited as MCEL Master Working Paper 2017/1

Table of Contents

1. Introduction

> The only part of the conduct of any one, for which he is amenable to society, is that which concerns others. In the part, which merely concerns himself, his independence is, of right, absolute. Over himself, over his own body and mind, *the individual is sovereign*.[1] John Mill

On 6 October 2015, the Court of Justice of the European Union invalidated in *Schrems vs. Data Protection Commissioner*[2] the Commission Decision 2000/520/EC[3] approving the adequacy of the level of protection provided by the so-called EU-US Safe Harbour framework. Based on Article 25 (6) of the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data, the Commission may find that a third country ensures an adequate level of protection by reason of its domestic law or its international commitments.[4] Unless the third country in question can ensure an adequate level of protection, Member States must prevent the transfer of data.[5]

The Safe Harbour framework, comprising the Safe Harbour Privacy Principles and the related Frequently Asked Questions issued by the US Department of Commerce,[6] enabled US-based organizations to legally transfer personal data from the European Union (hereafter 'EU') to the US as long as they complied with the Safe Harbour Privacy Principles on a voluntary basis.[7] Adherence to these principles could be limited under certain circumstances, *inter alia* where necessary on grounds of national security, public interest requirements of domestic law.[8] However, following the Snowden revelations in 2013, the Commission questioned whether the large-scale collection and processing of personal data under US surveillance programmes was necessary and proportionate to meet the interests of national security.[9]

---

[1] J. S. Mill, *On Liberty* (6th edition, Green, Reader & Dyer, Longmans, London, 1869), p. 22 (emphasis added).
[2] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd.* [2015] CJEU, ECLI:EU:C:2015:650.
[3] 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 [2000] OJ L 215.
[4] 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 L 281/32, Article 25 (6).
[5] Ibid, Article 25 (1).
[6] Commission Decision 2000/520/EC, Annex I-VII.
[7] The Safe Harbour framework is a based on a system of self-certification by which US organizations commit to the so-called Safe Harbour Privacy Principles in accordance with the Frequently Asked Questions. Ibid, recital 5.
[8] Commission Decision 2000/520/EC, Annex I.
[9] Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-U.S. Data Flows, COM (2013) 846 final.

Consequently, the Court of Justice of the European Union found in *Schrems vs. Data Protection Commissioner*[10] that, in light of the general nature of these derogations, the Commission Decision 2000/520/EC enabled the interference with the fundamental rights to privacy and data protection of the persons whose data could be transferred from the EU to the US under the Safe Harbour framework.[11] It criticized that the Commission decision lacked sufficient findings regarding the existence of US rules intended to limit such interference; interference which US authorities would be authorised to engage in when pursuing legitimate objectives such as national security.[12] The Commission would also fail to make reference to the existence of effective legal protection against such interference.[13] The Court found that the Commission decision did not state that US laws and practices 'ensured "in fact"'[14] an adequate level of protection of fundamental rights that was 'essentially equivalent'[15] (hereafter 'essentially equivalent' test) to that guaranteed within the European Union under Directive 95/46/EC and interpreted in light of the Charter of Fundamental Rights of the European Union[16] (hereafter 'EU Charter') and the European Convention on Human Rights[17] (hereafter 'ECHR').

In order to meet the requirements of adequacy under Article 25 (6) of Directive 95/46/EC as interpreted by the Court of Justice of the European Union in *Schrems vs. Data Protection Commissioner*[18], the EU and the US agreed on a new framework, the so-called EU-US Privacy Shield after two years of lengthy negotiations on 2 February 2016.[19] The framework consists of the so-called Privacy Shield Principles

---

[10] The Court had to deal with the regulation of personal data transfers to a third country, in this case the US, for the first time. See Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd.*
[11] Ibid*,* para. 87.
[12] Ibid, para. 88.
[13] Ibid, para. 89.
[14] Ibid*,* para. 97.
[15] Ibid, para. 96 reads that 'in order for the Commission to adopt a decision pursuant to Article 25 (6) of Directive 95/46, it must find, duly stating reasons, that the third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order […]'.
[16] Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.
[17] European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.
[18] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd.*
[19] Europa Rapid Press Release, *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*, 2 February 2016, IP/16/216.

and official written commitments by various US authorities.[20] On 12 July 2016, the Commission approved this framework with a new adequacy decision, concluding that the US ensured an adequate level of protection for personal data transferred from the EU to self-certified organizations established in the US under the Privacy Shield framework.[21]

The question arising is whether the new framework really meets the requirements to truly protect the fundamental rights to respect for privacy and data protection of EU data subjects today and in the future.[22] Since the Court of Justice of the European Union (hereafter 'CJEU') has the power to overrule the new adequacy decision if the Privacy Shield framework fails to meet the new standards, there is a need to assess the adequacy of the level of protection provided by the Privacy Shield framework. Does the new framework really illustrate a privacy shield or is it rather a privacy sieve? Accordingly, this paper analyses whether it was right of the Commission to approve the Privacy Shield framework by adopting the new adequacy decision and whether it could survive a legal challenge in the future. The research question guiding this paper is:

To what extent does the Privacy Shield framework meet the criteria for adequacy under Article 25 (6) of Directive 95/46/EC as interpreted by the CJEU in *Schrems vs. Data Protection Commissioner*[23]?

In other words, this paper explores whether the US, by reason of its domestic law or international commitments, provides a level of protection that is essentially equivalent to that provided in the EU. The criteria laid down in *Schrems vs. Data Protection Commissioner*[24] serve as a benchmark against which the equivalence of the level of protection afforded in the US can be compared.[25] Accordingly, this paper evaluates the current US legal framework and the practices of US intelligence agencies, as described in the new adequacy decision and the attached annexes, as well as the

[20] Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C (2016) 4176 final, recital 12 and Annex I-VII.
[21] Commission Implementing Decision C (2016) 4176 final, Article 1.
[22] Charter of Fundamental Rights of the European Union, Articles 7 and 8.
[23] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd.*
[24] Ibid.
[25] The details of the 'Schrems' judgement are depicted in chapter 2.3.

conditions under which they permit interference with the fundamental rights to respect for private life and data protection as guaranteed in the EU legal order. To be precise, this paper examines whether any interference for the purpose of national security can be justified in light of European jurisprudence on fundamental rights and whether US law contains sufficient limitations on the access and use of personal data by US authorities for national security purposes. In this regard, it investigates whether sufficient safeguards in form of oversight and redress mechanisms are in place that are capable of providing effective legal protection against interference of that kind.

The criteria for assessing adequacy are more specific following the CJEU's clarification in *Schrems vs. Data Protection Commissioner*[26]*.* Nevertheless, it must be noted that they continue to give some leeway of interpretation as they do not go beyond stating the need to set limitations and standards and to respect the principles of necessity proportionality. The precise structural framework for the 'essentially equivalent' test guiding this paper is delineated in chapter 3.1.

Given the complexity of the topic, this paper cannot offer a comprehensive analysis of all elements of the Privacy Shield framework. A thorough assessment of the commercial aspects[27] and the content of the Privacy Shield Principles would go beyond the scope of this paper and should be addressed in future research. Instead, this paper focuses on the derogations to the Privacy Shield Principles, which enable interference with the fundamental rights to privacy and data protection of EU data subjects whose data is or could be transferred under the Privacy Shield. Although not complete in every detail, this paper presents a fair picture of the level of protection of the fundamental rights to data protection and privacy provided under the Privacy Shield framework. A second remark regards the terminology used in this paper. The somewhat inconsistent usage is a necessary consequence of the inconsistent use of language in the analysed documents.[28] Additionally, the meaning of the term *Privacy Shield framework* can be confusing at times. While the Privacy Shield framework consists of the Privacy Shield Principles as well as various commitments and

[26] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd.*
[27] Such as new obligations for companies, monitoring mechanisms or redress possibilities in case of non-compliance.
[28] This issue is discussed in detail in chapter 3.2.3.

representations by US authorities, it is not a separate document. Instead, it is added to the new adequacy decision in form of seven annexes.[29] It is hence often referred to as *the Annexes* to the adequacy decision.

Lastly, put into a broader perspective, this paper also draws attention to differences of data protection regulation between the EU and the US in light of global developments.[30] It evaluates whether the Commission is truly capable of promoting and upholding EU data protection standards outside the EU following the approval of the Privacy Shield framework. In this respect, the paper makes also reference to the successor of Directive 95/46/EC, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereafter 'General Data Protection Regulation', in short 'GDPR'), which comes into effect in May 2018.[31] It examines the impact of the GDPR on the adequacy assessment procedure and on the Privacy Shield framework as such. Is the Privacy Shield framework capable of safeguarding the future of transatlantic data flows in the long run?

In the following, first, chapter two traces the historical and legal roots of the Privacy Shield framework. Chapter 2.1. outlines the data protection regime in the EU, with particular focus on the provisions on the transfer of personal data to third countries. Reference is made to relevant sections of Directive 95/46/EC and its successor, the GDPR. While chapter 2.2. presents the key characteristics of the Safe Harbour framework, chapter 2.3. depicts the main reasons for the invalidation of the first Commission adequacy decision, approving the Safe Harbour framework, and sets out the legal test created by the CJEU, which is likely to be used to determine the validity of the Privacy Shield framework in the future. Chapter 2.4. presents the GDPR and assesses its the future impact on the adequacy assessment procedure and the Privacy Shield framework, respectively. Next, chapter 2.5. delineates the worldwide influence of Commission adequacy decisions on data protection standards in general. The third chapter illustrates the main analysis of this paper, focussing on

[29] This issue is discussed in detail in chapter 3.2.1.
[30] I. Tourkochoriti, 'The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide between U.S.-E.U. in Data Privacy Protection', 36 *University of Arkansas at Little Rock Law Review* (2014).
[31] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC [2016] OJ L 119.

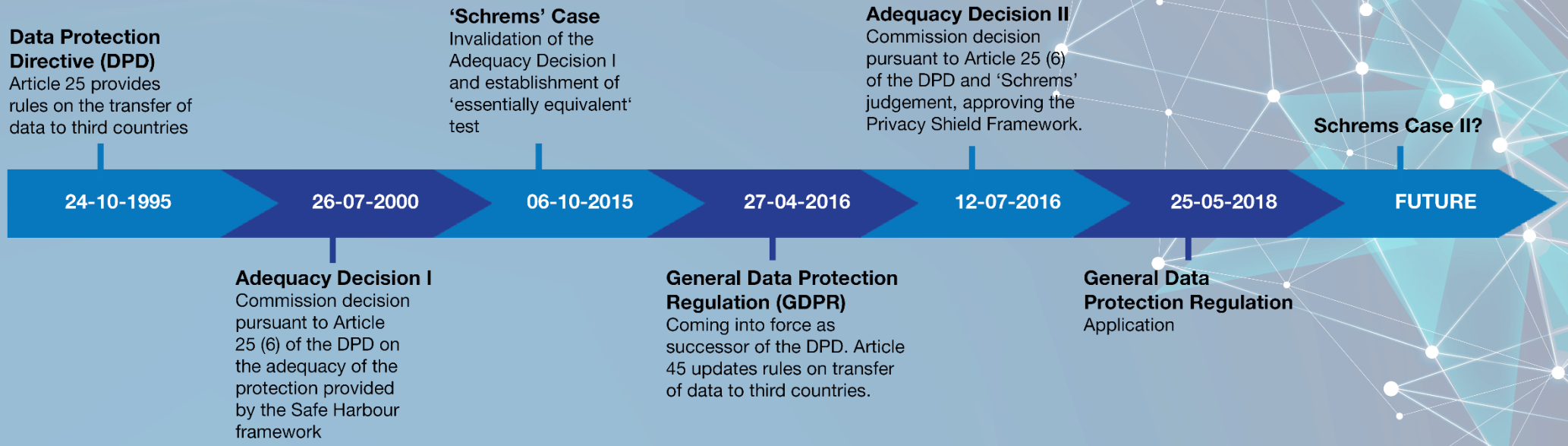
the adequacy assessment of the recently approved Privacy Shield framework. While chapter 3.1. sketches the structural framework, chapter 3.2. discusses whether relevant US laws and the form in which they are presented in the Privacy Shield framework are sufficiently clear and specific. Chapter 3.3. examines whether US law, illustrating the legal basis for the access and use of personal data by US authorities, has in fact a limited scope in line with the criteria of necessity and proportionality. Chapter 3.4. assesses whether the Privacy Shield framework provides effective legal protection through sufficient redress and independent oversight mechanisms. Chapter 3.5. summarizes the findings of chapter three. The last chapter demonstrates the different approaches between the US and EU towards data protection regulation and identifies possible solutions for more regulatory coherence in the transatlantic dialogue on data protection in the future. The conclusion recapitulates the main findings.

2. Legal Limbo: Tracing the Roots of the Privacy Shield

This chapter gives an overview of the EU data protection regime with respect to the transfer of personal data to third countries before and after *Schrems vs. Data Protection Commissioner*[32] (hereafter 'Schrems' ruling). Chapter 2.1. makes reference to Directive 95/46/EC (hereafter 'Data Protection Directive', in short 'DPD') and the provisions on data transfer to third countries in particular. Chapter 2.2. presents the features of the Safe Harbour framework (hereafter 'Safe Harbour') before chapter 2.3. delineates the reasons of the CJEU for invalidating the first Commission adequacy decision (hereafter 'Adequacy Decision I') and the legal requirements it would use to assess the adequacy of the level of protection provided by the Privacy Shield framework (hereafter 'Privacy Shield'). Chapter 2.4. presents the post-'Schrems' regime on data protection in the EU, while considering the potential impact of the GDPR on both future adequacy assessments and the Privacy Shield. To conclude, chapter 2.5. depicts the global influence of Commission adequacy decisions in general. The following timeline (Figure 1) illustrates the presented developments in chronological order.

[32] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd.*

Figure 1


Data Protection Directive (DPD)
Article 25 provides rules on the transfer of data to third countries
24-10-1995
26-07-2000
Adequacy Decision I
Commission decision pursuant to Article 25 (6) of the DPD on the adequacy of the protection provided by the Safe Harbour framework
'Schrems' Case
Invalidation of the Adequacy Decision I and establishment of 'essentially equivalent' test
06-10-2015
27-04-2016
General Data Protection Regulation (GDPR)
Coming into force as successor of the DPD. Article 45 updates rules on transfer of data to third countries.
Adequacy Decision II
Commission decision pursuant to Article 25 (6) of the DPD and 'Schrems' judgement, approving the Privacy Shield Framework.
12-07-2016
25-05-2018
General Data Protection Regulation
Application
Schrems Case II?
FUTURE

2.1. Pre - 'Schrems' Protection of Personal Data in the EU

In 1995, the EU adopted the comprehensive Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter 'Data Protection Directive', in short 'DPD').[33] Its objective is twofold: It aims at ensuring a high level of protection of fundamental rights and freedoms, particularly of the right to privacy with respect to the processing of personal data.[34] By harmonising the different levels of protection of these fundamental rights in the EU Member States, the DPD seeks to complement the realisation of the EU internal market, in which personal data can flow freely between Member States.[35] To reach this goal, it sets strict limits on the collection and use of personal data and requires each Member State to establish an independent supervisory authority.[36]

The DPD was adopted at a time when only one percentage of the EU population used Internet; Google had not even launched its service yet.[37] Since then, a substantial increase in cross-border flows, sharing and collection of personal data as well as technological developments in a globalising world have encompassed a seismic shift in landscape, posing fundamental challenges for data protection regulation today.[38] Thus, in order to reform and establish more uniform rules for data protection in the EU,[39] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereafter 'General Data Protection Regulation', in short 'GDPR') was adopted on 27 April 2016.[40] Whereas it already entered into force on 25 May 2016, it will only apply from 25 May 2018 onwards, following a two-year transition period. It aims at more

[33] Directive 95/46/EC; The Directive has EEA relevance as EU data protection legislation is covered by the EEA Agreement. The EEA includes all EU countries and the non-EU countries Iceland, Liechtenstein and Norway. See Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI to the EEA Agreement [2000] OJ L296/41 and Agreement on the European Economic Area [1994] OJ No L 1.
[34] Directive 95/46/EC, recitals 2 and 10, Article 1 (1).
[35] Ibid, recitals 7 and 8, Article 1 (2).
[36] Ibid, Articles 6, 7 and 28.
[37] European Rapid Press Release, *V. Reding on the Outdoing Huxley: Forging a High Level of Data Protection for Europe in the Brave New Digital World*, 18 June 2012, SPEECH/12/464.
[38] O. Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, Oxford, 2015).
[39] EU regulations are directly applicable in all EU Member States without the need for further implementation in national legislation. See Consolidated Version of the Treaty on the Functioning of the European Union, 2008 O.J. C 115/47 (hereafter 'TFEU'), Article 288.
[40] Regulation (EU) 2016/679.

coherence between national provisions and a less fragmented implementation of data protection across the EU.[41]

Both the DPD and the GDPR contain provisions regulating the transfer of personal data to third countries, to be outlined in the following. The Commission perceives the need for these 'special precautions' due to the increasing globalization of data flows, through which the high European level of protection could be easily undermined or circumvented.[42]

The standards for the transfer of personal data to third countries under the DPD are divisible into three parts. First, Article 25 (1) provides the default rule stipulating that EU Member States may only allow the transfer of personal data to a third country when the third country in question 'ensures an adequate level of protection'.[43] Second, Article 26 (1) lists exceptions that can justify the (small-scale) transfer of data in absence of an adequate level of protection.[44] For instance, such transfer can take place when the data subject has given its unambiguous consent to the transfer or when it is necessary for the conclusion of a contract entered into by the data subject or concluded in its interest.[45] Lastly, Article 26 (2) outlines a set of circumstances in which Member States may permit the transfer of personal data to third countries when a data controller introduces 'adequate safeguards'[46] to protect

[41] Regulation (EU) 2016/679, recitals 5, 6, 7 and 13, Article 1.
[42] The EU Charter guarantees the fundamental right to respect for private life in Article 7 and the fundamental right to the protection of personal data in Article 8. The importance of these fundamental rights and freedoms of EU natural persons was confirmed by the CJEU in various cases. See also European Commission, 'Data transfers outside the EU', (2015), http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm (last visited 6 July 2016).
[43] Directive 95/46/EC, Article 25 (1).
[44] Directive 95/46/EC, Article 26 (1) reads that data transfer may take place on condition that '(a) the data subject has given his consent unambiguously to the proposed transfer; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.' See also P. Rees, C. O'Donoghue & J. Nicholson, 'Transferring Personal Data Outside the EEA: The Least Worst Solution', 13 *Computer and Telecommunications Law Review* 66 (2007).
[45] Directive 95/46/EC, Article 26 (1) (a), (b) and (c).
[46] Directive 95/46/EC, Article 26 (2); Two types of 'adequate safeguards' have become recognized over time. Firstly, the 'appropriate contractual clauses' are specified in Art. 26 (2) and are binding contractual commitments between the data exporter and importer. Secondly, 'binding corporate rules' are binding data processing rules to be adopted by a company. While they are not mentioned in the DPD yet, the GDPR codifies them. See C. Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', *BNA Bloomberg Privacy and Security Law Report* (2012), http://www.kuner.com/my-publications-and-writing/untitled/kuner-eu-regulation-article.pdf (last visited 7 July 2016).

the privacy and fundamental rights of data subjects.[47] In light of the focus of this paper, the pursuing analysis refers to the default rule of the DPD only. [48]

The Commission must assess the adequacy of the level of protection afforded by a third country in light of 'all the circumstances surrounding a data transfer operation or set of data transfer operation'.[49] Hence, the adequacy assessment procedure demands a contextual analysis of the protections available in the relevant non-EU country.[50] Pursuant to Article 25 (2) of the Data Protection Directive, particular consideration must be given to

(a) the nature of the data

(b) the purpose and duration of the proposed processing operation(s)

(c) the country of origin and final destination

(d) the rules of law in force in the third country and

(e) the professional rules and security measures in place[51]

Where the Commission finds that a third country does not ensure an adequate level of protection within the meaning of Article 25 (2),[52] Member States must take necessary steps to prevent any transfer of data.[53] Based on Article 25 (6), the Commission may find that an adequate level of protection exists 'by reason of a third state's domestic law and the international commitments it has entered into in order to safeguard the rights of individuals'.[54] In that case, personal data can flow to the third country in question without any additional safeguards being necessary.[55] Member States must take all necessary measures to comply with a Commission decision.[56] Nevertheless, the CJEU found in the 'Schrems' case that both Member States and the Commission may make the finding that a third country does or does not ensure

[47] The Commission issued standard contractual clauses in order to harmonize this exceptional authorization process, which is pursued by EU Member States.
[48] With a focus on the limitations on access by public authorities to data transferred under the Privacy Shield, the discussion of commercial aspects, for which Article 26 of the DPD is relevant, was excluded.
[49] Directive 95/46/EC, Article 25 (2).
[50] P. M. Schwartz, 'The E.U.-U.S. Privacy Collision: A Turn to Institutions and Procedures', 126 *Harvard Law Review* 7 (2013).
[51] Directive 95/46/EC, Article 25 (2).
[52] According to the procedure provided for in Directive 95/46/EC, Article 31 (2).
[53] Directive 95/46/EC, Article 25 (4).
[54] Directive 95/46/EC, Article 25 (6).
[55] Commission Decision 2000/520/EC, recital 2; See European Commission, 'Commission decisions on the adequacy of the protection of personal data in third countries' (n.d.), http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (last visited 6 July 2016).
[56] Directive 95/46/EC, Article 25 (6).

an adequate level of protection.[57] The Commission and the Member States shall inform each other where they consider that a third country does not ensure an adequate level of protection.[58]

Whilst the default rule outlined in Article 25 (1) is a very delicate issue by nature, the DPD does not provide any detailed requirements for a coherent adequacy assessment - except for the above mentioned non-exhaustive list of factors. The President of the European Court of Justice (hereafter 'ECJ')[59] reiterated that the DPD is clear in spelling out the objective of the rule but 'leaves the form and the methods open'.[60] Whereas the independent Article 29 Working Party[61] drafted guidelines with key criteria for a coherent assessment of adequacy,[62] they merely illustrate minimum requirements for an adequate level of protection and are thus limited in facilitating more clarity.[63] In the meantime, ambiguity regarding the assessment procedure of adequacy continues to encompass problems as different EU Member States can make dissimilar judgements on adequacy.[64] Risks of gaps and uncertainties in terms of level of protection remain particularly as activities relating to national security fall outside the scope of EU law.[65]

---

[57] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd,* para. 50; Opinion Advocate General: Opinion of Advocate Bot in Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd* [2015] CJEU, ECLI:EU:C:2015:650, point 86.

[58] Directive 95/46/EC, Article 25 (3).

[59] The ECJ is the highest court in the EU that hears applications from national courts for preliminary rulings, annulment and appeals. In contrast, the CJEU is the collective term for the EU's judicial arm. See Consolidated Version of the Treaty on European Union, 2006 O.J. C 321 E/5 (hereafter 'TEU'), Article 19.

[60] ECJ President Koen Lenaerts in V. Pop, 'ECJ President On EU Integration, Public Opinion, Safe Harbor, Antitrust', *The Wall Street Journal* (2015), http://blogs.wsj.com/brussels/2015/10/14/ecj-president-on-eu-integration-public-opinion-safe-harbor-antitrust/ (last visited 13 August 2016).

[61] The Article 29 Working Party consists of representatives of the 29 national data protection agencies, the European Data Protection Supervisor and the Commission and has advisory status. See Directive 95/ 46/EC, Article 29.

[62] Directive 95/46/EC, Article 30 stipulates that the Article 29 Working Party can give opinions and may suggest codes of conduct.

[63] For instance, it demands that respective frameworks should provide for a core of data protection 'content' principles, including the purpose limitation principle, the data quality and proportionality principle, the transparency principle, the security principle, the right of access, the rectification and opposition principle and restrictions on onwards transfer, as well as 'procedural principles' such as provisions on the support and help to individual data subjects, on appropriate redress mechanisms and the need for a good level of compliance. See Article 29 Working Party, Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (1998), DG XV D/5025/98 WP 12; Hogan Lovells, 'Legal Analysis of the EU-U.S. Privacy Shield: An adequacy assessment by reference to the jurisprudence of the Court of Justice of the European Union', *Authoritative Legal Report* (2016), http://www.hldataprotection.com/2016/03/articles/international-eu-privacy/hogan-lovells-issues-authoritative-legal-analysis-of-the-eu-u-s-privacy-shield/ (last visited 11 August 2016).

[64] L. Bygrave, 'Privacy and Data Protection in an International Perspective', 56 *Scandinavian Studies in Law* (2010).

[65] TEU, Article 4 (2) reads that the EU must respect the EU Member States' exclusive responsibility for national security. Both the DPD and the GDPR exempt matters of national security from their scope. See Directive 95/46/EC, Article 3 (2); Regulation (EU) 2016/679, recital 16.

Whether and to what extent the GDPR, taking into account the 'Schrems' judgment to some extent, will influence the adequacy assessment procedure upon its application in 2018 is outlined in chapter 2.4., following the analysis of the 'Schrems' ruling. Next, the characteristics and problems of the Safe Harbour framework are discussed.

2.2. Safe Harbour: An Unsuccessful First Attempt

Under the Safe Harbour framework, an US-based organization could qualify individually for the presumption of adequacy, allowing for the legal transfer of EU personal data to the US, when it complied with the seven Safe Harbour Privacy Principles[66] (hereafter 'the Principles I') and the related Frequently Asked Questions[67], providing guidance on their implementation.[68] In light of the focus of this paper, they are not further discussed. Whereas the decision to adhere to the Principles I was entirely voluntary,[69] participation was only eligible to those organizations that were subject to the jurisdiction of the Federal Trade Commission (hereafter 'FTC'), which is responsible for enforcing various consumer protection laws in the US.[70] Alternatively, organizations could be subject to any other statutory body that would effectively ensure compliance with the Principles I.[71] Those organizations willing to abide by the scheme were required to publicly disclose their privacy policies,[72] had to self-certify and publicly disclose their unambiguous commitment to comply with the Principles I.[73]

Given that the Principles I were only applicable to self-certified US organizations; US public authorities were not required to comply with them.[74] The issue arising is that

[66] The seven privacy principles had the following titles: Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement. See Commission Decision 2000/520/EC, Annex I.
[67] Commission Decision 2000/520/EC, Annex II.
[68] Ibid, recital 5 and Article 1 (1).
[69] Ibid, Article 1 (3) and Annex I.
[70] Ibid, recital 5; US Federal Trade Commission Act (1914), 15 U.S.C. §§ 41-58, as amended, Section 5 prohibits unfair or deceptive acts or practices in commerce.
[71] Commission Decision 2000/520/EC, recital 5 and Article 1 (2) (b).
[72] Ibid, recital 5.
[73] Ibid, Articles 1 (2) (a) and (3).
[74] The extensive power of US authorities to access personal data was *inter alia* addressed by means of the so-called EU-US Data Protection Umbrella Agreement. This framework on data protection for transatlantic criminal investigations shall ensure the protection of personal data when transferred across the Atlantic for law enforcement purposes and ensure legal certainty for transatlantic data exchange between police and criminal justice authorities. The way for its signature on 2 June 2016 was paved by the Judicial Redress Act, signed by US President Barack Obama on 24 February 2016, to improve the sharing of data in criminal and terrorism investigations. It gives EU citizens access to US courts in order be able to seek redress for alleged data

public authorities could access the personal data guarded by registered organizations under certain circumstances. In other words, the companies' adherence to the Principles I could 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 to create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation could demonstrate that its non-compliance with the Principles I was limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation.[75]

Hence, the derogations to the applicability of the Principles I were permitted *inter alia* based on grounds of national security or where US law imposed conflicting obligations. U.S. organizations, 'whether in the safe harbour or not [had to] comply with the law'.[76] In order to pursue the legitimate objective of national security, US intelligence agencies had legal access to personal data transferred from the EU to the US under the Privacy Shield. Max Schrems, whose case led to the downfall of the Adequacy Decision I, later commented in this context that '[t]he core problem uncovered by Edward Snowden was not only that the US is using massive surveillance programs, but that all of them are in fact *legal* under current US law'.[77] This issue, referred to as legal loophole, is discussed in detail in chapter 2.3.2.

The Safe Harbour had to face much criticism from the beginning onwards. In particular, the national data protection agencies (hereafter 'DPA') challenged its validity as an adequate and effective framework.[78] Additionally, given that the Adequacy Decision I had been negotiated at a time when the Internet was at its infancy, a re-evaluation became necessary soon.[79] In light of the above-mentioned

---

protection violations pursued by the federal government in relation to personal data transferred to the US for law enforcement purposes. The Act extends the protections of the Privacy Act of 1974, which empowers US citizens to challenge the government's use of private data, to the citizens of designated foreign countries. A further discussion of the Judicial Redress Act and the Umbrella Agreement goes beyond the scope of this paper and should be addressed in future research. See Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation and Protection of Criminal Offenses, 2 June 2016; Judicial Redress Act of 2015, H.R. 1428 114th Cong. (2015-2016).

[75] Commission Decision 2000/520/EC, Annex I.

[76] Commission Decision 2000/520/EC, Annex IV (B).

[77] M. Schrems, '"EU-US Privacy Shield": Towards a new Schrems 2.0 Case?', *European Area of Freedom Security &Justice Free Group* (2016), https://free-group.eu/2016/04/06/eu-us-privacy-shield-towards-a-new-schrems-2-0-case/ (last visited 12 August 2016) (emphasis added).

[78] For instance, they communicated dissatisfaction with the lack of annual compliance checks and the self-certification structure. See C. Wolf, 'Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers', 43 *Washington University Journal of Law & Policy* (2014).

[79] V. Reding stated that '[t]he main problem is that our rules predate the digital age and it became increasingly clear in recent years that they needed an update [...]'. In N. Singer, 'Data Protection Laws, an Ocean Apart', *The*

loophole, the validity of the Adequacy Decision I was particularly contested following the Snowden revelations in June 2013. In response to the so-called PRISM surveillance programmes[80] concerning large-scale collection and processing of personal data, the Commission declared that its 'concerns about the level of protection of personal data […] had grown'.[81] As a consequence, the Commission announced in two communications on 27 November 2013 that the fundamental basis of the Safe Harbour framework had to be reviewed.[82] It admitted that 'the personal data of EU citizens sent to the US under Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the EU and the purposes for which it was transferred to the US.'[83] The surveillance programs would go 'beyond what is *strictly necessary and proportionate* to the protection of national security as foreseen under the exception provided in [the Adequacy Decision I]'.[84] Subsequently, in September 2013, the Commission drafted thirteen recommendations to address various weaknesses of Safe Harbour. *Inter alia*, it stressed the need to ensure that the use of the national security exemption provided in the Adequacy Decision I was limited to an extent that was strictly necessary and proportionate.[85] Eventually, the need for an updated adequacy decision became even more apparent when the CJEU declared the Adequacy Decision I invalid on 6 October 2015, as outlined in the following chapter.[86]

2.3. The 'Schrems' Criteria

In order to be able to assess to what extent the Privacy Shield actually differs from its predecessor and whether the Adequacy Decision II meets the criteria under Article

---

New York Times (2013), http://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html?_r=0 (last visited 3 July 2016).

[80] PRISM is not an abbreviation but the full name of a clandestine surveillance program which gives the US National Security Agency the authority to collect Internet communications from major US Internet companies.

[81] Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-U.S. Data Flows, COM (2013) 846 final, p. 4; Ad hoc EU-US Working Group on Data Protection, Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection (2013).

[82] COM (2013) 846 final; 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.

[83] COM (2013) 846 final, p. 12.

[84] COM (2013) 847 final, p. 17 (emphasis added).

[85] European Rapid Press Release, *Viviane Reding Vice-President of the European Commission, EU Commissioner for Justice on Today's Justice Council – A Council of Progress*, 6 June 2014, SPEECH/14/431.

[86] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd.*

25 (6) DPD as interpreted by the CJEU in the 'Schrems' case, it is necessary to analyse the reasons leading to the invalidation of the Adequacy Decision I.

The 'Schrems' case initiated by the Austrian national Maximilian Schrems.[87] He had made a complaint to the Irish Data Protection Commissioner about the fact that Facebook Ireland transferred his personal data to the US, where he did not consider his data to be adequately protected against surveillance activities by US public authorities.[88] Following the Commissioner's refusal to investigate, he appealed before the Irish High Court, which in turn referred the preliminary question whether a national data protection authority could conduct its own investigation regarding the adequacy of the level of data protection provided in a third country or whether it was absolutely bound by the Commission's adequacy decision to the CJEU.[89]

On 6 October 2015, the CJEU delivered its judgement, the outcome of which was two-fold. First, national data protection agencies are allowed to examine if the transfer of personal data to a non-EU country, which is approved by a Commission adequacy decision, is compatible with EU data protection standards.[90] Second and more relevant for this paper, the CJEU declared the Adequacy Decision I invalid.[91] The Court found that the Commission had not duly stated that the US ensured in fact an adequate level of protection based on its domestic law and international commitments.[92] There was no further need for the Commission to establish whether the Safe Harbour framework ensured an equivalent level of protection given that the proof procedure itself was flawed.[93] Consequently, the 'Schrems' judgement is crucial to identify the specific criteria and principles against which the Adequacy Decision II will be legally scrutinised in the future.[94]

In the following, chapter 2.3.1. presents the legal test established by the CJEU to assess the adequacy of the level of protection provided by a third country in line with Art. 25 (6) of the DPD and in the light of the EU Charter. Taking all jurisprudence into

[87] Ibid, para. 26.
[88] Max Schrems referred to the revelations by Edward Snowden as being proof of the surveillance activities of the US intelligence services, in particular those of the US National Security Agency. See ibid, para. 28 and 30.
[89] Ibid, para. 36.
[90] Ibid, para. 107.
[91] Ibid, para. 107.
[92] Ibid, para. 96-97.
[93] Ibid, para. 98.
[94] That is, the Court interpreted the existing criteria set out in Article 25 (2) and (6) of Directive 95/46/EC.

account, the CJEU took issue with two legal loopholes that are relevant for this paper: the US public authorities' excessive and disproportional access to data (chapter 2.3.2.) and missing effective legal protection against such interference (chapter 2.3.3.).

2.3.1. How to Determine Adequacy

In order to determine the validity of Schrems' contention that US law and practices do not ensure an adequate level of protection within the meaning of Article 25 of the DPD,[95] the CJEU first examined whether the Adequacy Decision I complied with the requirements in Article 25 of the DPD read in light of the EU Charter, rather than assessing the content of the Principles I. The CJEU neither made an explicit statement on the adequacy of the Principles I nor on the adequacy of US laws.[96] The CJEU could not engage in fact-finding on its own given that its authority under Article 267 TFEU is restricted to answering questions about the interpretation and validity of EU law in cases presented to the CJEU by EU Member State courts.[97] Therefore, there was neither the need nor the authority to examine the content of the Principles I.[98] Yet, the CJEU clearly condemned the impact of the US intelligence authorities' practices on fundamental rights by referring to the Commission's own assessment, in which it concluded that US authorities were able to access data in a way that violated the EU legal standards of necessity and proportionality and exceeded the purpose limitation.[99]

As pointed out in chapter 2.1., Article 25 of the DPD lacks a clear-cut assessment procedure and specific requirements to assess whether the transfer of personal data to a third country ensures an adequate level of protection. In the 'Schrems' ruling, the CJEU confirmed

> that neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an adequate level of protection. In particular, Article 25(2) does no more than state that the

[95] Ibid, para. 67.
[96] Ibid, para. 90 and 98.
[97] This was further reiterated by CJEU President Koen Lenaerts: We are 'not judging the U.S. system here, we are judging the requirements of EU law in terms of the conditions to transfer data to third countries, whatever they be'. See V. Pop 'ECJ President On EU Integration, Public Opinion, Safe Harbor, Antitrust', *The Wall Street Journal*.
[98] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd,* para. 98.
[99] Ibid, para. 90.

> adequacy of the level of protection afforded by a third country "shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations" and lists, on a non-exhaustive basis, the circumstances to which consideration must be given when carrying out such an assessment.[100]

The Court reiterated that it was merely apparent from Article 25 (6) that an assessment must be based on the 'domestic law and international commitments' of a third country and 'for the protection of the private lives and basic freedoms and rights of individuals'.[101] It concluded that the provision requires a third country to ensure 'a high level of protection'.[102] Moreover, the CJEU determined that a third country 'cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order'.[103] While the level of protection of fundamental rights and freedoms 'may differ', depending on the means a third country has recourse to, it must yet prove 'in practice, effective in order to ensure protection *essentially equivalent* to that guaranteed in the European Union' under the DPD and read in light of the EU Charter.[104] Accordingly, the Commission must assess 'the content of the applicable rules' in the relevant country, resulting from its 'domestic law or international commitments and the practice designed to ensure compliance with those rules'.[105] Since a level of protection is prone to change over time, the Commission is also required to regularly review whether an adequacy finding is 'still factually and legally justified'.[106] Any discretion available to the Commission as to the adequacy of the level of protection must be limited and the review of the requirements in Article 25 must be 'strict'.[107]

In fact, the definition of an adequate level of protection was one of the most controversial issues the Court had to deal with in the judgement.[108] In spite of further specification of the requirements of adequacy, the main issue from a legal point of view remains what standards or criteria should be used to measure 'essential equivalence', as laid down by the Court. First, it seems to imply a legal comparison between the data protection standards of the EU and the third country, that is, the US

[100] Ibid, para. 70.
[101] Ibid, para. 71.
[102] Ibid, para. 72.
[103] Ibid, para. 73.
[104] Ibid, para. 74 (emphasis added).
[105] Ibid, para. 75.
[106] Ibid, para. 76.
[107] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd*, para. 78.
[108] C. Kuner, *BNA Bloomberg Privacy and Security Law Report* (2012).

in the case at hand. Yet, this is a rather difficult task, given that data protection and privacy laws are context-bound and linked to culture.[109] A comparison of legal systems requires the consideration of non-legal and social factors.[110] Henceforth, there is a risk that a decision on whether a third country ensures essentially equivalent protection or not, is based on insufficient knowledge of foreign law or foreign political forces.[111] A discussion on whether and how the different approaches to data protection assumed by the US and the EU can be tackled in the long run follows in chapter four.

After all, it appears that the correct measure to evaluate essential equivalence is provided by the EU Charter alone, given that the Court states various times in the 'Schrems' judgement that the fundamental rights to data protection and private life shall be measured against the EU Charter.[112] It makes regular reference to both the EU Charter and previous CJEU judgements, particularly the *Digital Rights Ireland* case[113]. Thereby, it stresses the need for a 'high'[114] level of protection achieved through a 'strict'[115] assessment under Article 25 of the DPD and in consideration of the EU Charter. The question arises whether it would not have been sufficient to refer to relevant CJEU case law in order to interpret the meaning of adequacy rather than establishing the term *essentially equivalent*. An interpretation by means of case law might have required less linguistic gymnastics than the remaining task of developing a meaningful understanding of the *essential equivalence*. Overall, the standard adopted by the Court can be best understood as a high degree of protection as required by reference to the EU Charter.

[109] Ibid.
[110] Ibid.
[111] Ibid.
[112] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd,* para. 38-39. See also C. Rauchegger, 'The Interplay Between the Charter and National Constitutions after *Åkerberg Fransson and Melloni*', in S. de Vries, U. Bernitz and S. Weatherill (eds.), *The EU Charter of Fundamental Rights as a Binding Instrument* (Hart, 2015).
[113] Ibid, para. 39; In the joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Others* [2014] CJEU, ECLI:EU:C:2014:238*,* the CJEU declared the EU Data Retention Directive for invalid for the reason of violating fundamental rights. The ECJ generally considers the retention of data a suitable measure to fight international terrorism and other serious crimes as long as the criteria developed in the joint cases are complied with. See 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 L 105.
[114] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd*, para. 39, 72 and 73.
[115] Ibid, para. 78.

Having determined how to assess adequacy in light of the 'Schrems' judgement, this paper delineates the two major loopholes of the Adequacy Decision I, which the CJEU took issue with.

2.3.2. Loophole I: Derogations Facilitating Interference with Fundamental Rights

The CJEU strongly affirmed that the rights to data protection and private life illustrate fundamental rights under EU law by making repeated reference to the EU Charter and former data protection judgments[116] and reiterating that the Commission's discretion in making an adequacy decision 'should be strict'[117]. At the same time, the CJEU acknowledged the necessity for certain derogations from the Principles I, stressing that they could be limited 'to the extent necessary to meet the overriding legitimate interests' such as national security, public interest, or law enforcement requirements.[118] Nevertheless, the CJEU identified a conflict between the requirements of the Principles I and US law, as the Adequacy Decision I would clearly stipulate that US law took primacy over the Principles I.[119] Thereby, US organizations would be 'bound to disregard those principles without limitations where they conflict with those requirements'.[120] Consequently, the Court found that the general nature of the derogations to the Principles I facilitated 'interference, founded on national security and public interest requirements or on domestic legislation of the United States' with the fundamental rights to private life and data protection, as guaranteed under the EU Charter.[121] In particular, it criticized a lack of findings in the Adequacy Decision I regarding the existence of rules adopted by the US intended to restrict such interference.[122]

Article 52 of the EU Charter prescribes that interference with the fundamental rights to private life and protection of personal data, guaranteed in Articles 7 and 8 of the EU Charter, must have a legal basis and respect the principles of proportionality and

[116] Case C-131/12 *Google Spain and Google* [2014] CJEU, ECLI:EU:C:2014:317; Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Others.*
[117] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd*, para. 78.
[118] Ibid, para. 84.
[119] Ibid, para. 85.
[120] Ibid, para. 86.
[121] Ibid, para. 87.
[122] Ibid, para. 88.

necessity while meeting objectives of general interest.[123] Accordingly, EU law involving interference with these fundamental rights must 'lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards', so that the persons whose personal data is affected have 'sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data'.[124] Such rules are of particular importance where there is a high risk of unlawful accesses. In this regard, the CJEU went on to highlight that, as demonstrated by the Commission's own assessment of the *status quo* following the implementation of the Adequacy Decision I, the US authorities were able to access 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'.[125] With reference to the *Digital Rights Ireland* case, the CJEU underlined that derogations to the protection of the fundamental right to privacy at EU level had to be 'strictly necessary'.[126] The CJEU clarified that 'legislation'[127] (whether EU or non-EU) is not limited to what is strictly necessary where it authorizes

> on a generalised basis, storage of all the personal data of all the persons whose data was transferred from the European Union 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 by which to determine the limits of the access of the public authorities to the data, and of its subsequent use.[128]

On this basis, the CJEU concluded that legislation permitting the US public authorities access to the content of electronic communication 'on a generalised basis', as was the case under the Safe Harbour framework that was approved by Adequacy Decision I, had to be interpreted as 'compromising the essence of the fundamental right to respect for private life'[129] in light of the EU Charter.

---

[123] Charter of Fundamental Rights of the European Union, Article 52 (1) reads: 'Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principles 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.'.
[124] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd*, para. 91; Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Others*, para. 54-55.
[125] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd*, para. 90.
[126] Ibid, para. 92.
[127] The CJEU did not further specify the meaning of the term 'legislation'. See ibid, para. 93.
[128] Ibid, para. 93.
[129] Ibid, para. 94.

2.3.3. Loophole II: Insufficient Legal Protection

The CJEU was also concerned with insufficient accountability mechanisms provided by the Safe Harbour. The Court referred to the Commission's own assessment, which found that data subjects did not have access to sufficient administrative and judicial means of redress, empowering them individuals to access and possibly rectify or erase the data relating to them.[130] It found fault with missing findings in the Adequacy Decision I regarding the existence of effective legal protection against the interference with fundamental rights founded on national security.[131] Procedures before the FTC and private dispute resolution mechanisms for commercial disputes could not be applied to disputes relating to the legality of interference with fundamental rights resulting from measures exercised by the US state.[132] Consequently, the CJEU concluded that 'legislation' not providing for any possibility for an individual to pursue legal remedies 'does not respect the essence of the fundamental right to effective judicial protection', as enshrined in Article 47 of the EU Charter.[133] The very existence of effective judicial review would be inherent in the existence of the rule of law.[134]

In sum, based on the above mentioned considerations, the CJEU reasoned that the Adequacy Decision I, approving the Safe Harbour framework, did not state that the US in fact ensured an adequate level of protection essentially equivalent to that guaranteed in the EU legal order by reason of its domestic or its international commitments. Hence, it annulled the Adequacy Decision I.[135] However, it is important to stress that the CJEU neither reached its own conclusions regarding the US legal order nor to the extent to which it lacks rules limiting any interference with data protection rights.[136]

In the following, this paper examines the recently adopted GDPR and analyses the impact of the 'Schrems' ruling on the adequacy assessment procedure therein.

[130] Ibid, para. 90.
[131] Ibid, para. 89.
[132] Ibid, para. 89.
[133] Ibid, para. 95.
[134] Ibid, para. 95.
[135] Ibid, para. 107.
[136] Ibid, para. 88.

2.4. Post - 'Schrems' Era: Adequacy Assessment under the GDPR

The DPD will be replaced by the GDPR upon entering into application on 25 May 2018.[137] The GDPR maintains the twofold objective: to facilitate the transfer of personal data to third countries while ensuring a high level of protection of data.[138] It uses 'the same toolkit' as its predecessor.[139] The general principles guiding the transfer of personal data to third countries and the notion of adequacy are upheld but described in more detail than in the DPD.[140] The GDPR maintains the three major grounds permitting data transfers under the DPD, that is, by means of adequacy decisions, derogations and appropriate safeguards. First, Article 45 (1) of the GDPR permits data transfer to third countries whose data protection regime is considered to provide an adequate level of protection following an adequacy decision by the Commission.[141] Article 45 (3) requires the Commission to assess the level of protection in a third country according to a list of elements outlined in Article 45 (2). Thereby, the GDPR effectively follows the procedure under Article 25 (6) of the DPD. At the same time, a formal departure from the DPD's adequacy-focused approach can be noted. That is to say, the GDPR introduces a shift from a general prohibition of transferring data to third countries, as outlined in the DPD,[142] to the principle that transfers take place when enumerated conditions, set out in Article 45 (2) of the GDPR, are met.[143] Such circumstances include but are not limited to the issuance of

[137] Regulation (EU) 2016/679.
[138] Regulation (EU) 2016/679, recital 6, Article 1.
[139] Allen & Overy, 'The EU General Data Protection Regulation', *Authoritative Legal Report* (2016), http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf (last visited 13 August 2016), p. 7.
[140] Regulation (EU) 2016/679, recital 48, Chapter V (Articles 44-49) governs cross-border transfers of personal data.
[141] Ibid, Article 45 (1) reads: 'A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, or a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation'.
[142] Directive 95/46/EC, Article 25 (1).
[143] Regulation (EU) 2016/679, Article 45 (2) states that the following elements must be considered: 'a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

a Commission adequacy decision. In absence of an adequacy decision pursuant to Article 45 (3), data transfer can take place according to Articles 46-49.[144] Consequently, it is evident that the GDPR provides more legal grounds authorizing the transfer of data outside of the EU.

Other differences regarding the assessment of adequacy can be identified. For instance adequacy decisions are subject to periodic review, in which the Commission must consult with the relevant entity[145] and, unlike the DPD, violations of the GDPR's international data transfer provisions may result in hefty fines.[146] Furthermore, the GDPR allows the Commission to determine the adequacy of a larger amount of entities, including territories, or specified sectors within third countries and international organizations.[147] To this adds that the territorial scope of the GDPR is extended 'to the processing of personal data of data subjects who reside in the EU by a controller or processor not established in the Union', where the processing activities regard a) the offering of goods or services and b) the monitoring of their behaviour.[148]

It is particularly noticeable that the 'Schrems' ruling, which raised the bar for a level of protection of a third country from adequate to essentially equivalent, was taken into account.[149] That is, recital 104 of the GDPR confirms that a third state must ensure an 'adequate level of protection *essentially equivalent* to that ensured within the Union'.[150] Moreover, it requires a third country to provide effective and enforceable rights as well as effective administrative and judicial redress.[151] The 'Schrems' judgment also surfaces in the numerous elements in Article 45 (2) of the GDPR that must be considered in determining adequacy. *Inter alia*, they require the respect for the rule of law and fundamental freedoms, the consideration of general and sectorial

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.'.

[144] Regulation (EU) 2016/679, Article 46 sets out the conditions for transfers subject to appropriate safeguards; Article 47 sets forth the conditions for transfers through binding corporate rules, which were not codified in the Data Protection Directive yet; Article 48 addresses situations where a tribunal of a third country has ordered a transfer not permitted by the GDPR; Article 49 lists the conditions for derogations for specific situations in the absence of an adequacy decision or appropriate safeguards, including binding corporate rules.

[145] Regulation (EU) 2016/679, recitals 106-107, Article 45 (3).

[146] Ibid, Article 83 (5) (c).

[147] Ibid, Article 45 (1) and (2).

[148] Ibid, Article 3 (2).

[149] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd,* para. 73 and 96.

[150] Regulation (EU) 2016/679, recital 104 (emphasis added).

[151] Ibid, recital 104.

legislation of a country concerning public security, defence, national security and criminal law as well as the attention to the access of public authorities to personal data, effective and enforceable data subject rights and judicial redress for data subjects whose personal data are being transferred.[152]

Thus, in comparison to the DPD, the GDPR has a more detailed definition of what constitutes 'adequacy' and how it can be assessed, incorporating the standards adopted by the CJEU to a large extent. Nevertheless, it may be argued that the wording of the adequacy rule is still not sufficiently detailed and rigorous in order to provide a clear-cut assessment procedure. Furthermore, the adequacy assessment procedure continues to lack guidelines for coherent logistics that facilitate the actual issuance of adequacy decisions and their practical implementation. Altogether, the adequacy assessment procedure in the GDPR appears more bureaucratic than in the DPD.[153] In order to advance the credibility of the process, in which the Commission remains both judge and jury, it would also be valuable to include additional checks and balances in the future.[154] In sum, it must be noted that the adequacy assessment process brings about various positive changes. Nevertheless, the procedure will probably remain a contentious issue upon the entry into application of the GDPR in May 2018.

In light of the formal adoption of the GDPR, the question arises what effect it will have on data transfers to third countries under the Privacy Shield, which does not yet reflect the future situation under the GDPR. Although the GDPR already incorporates the standards of the 'Schrems' judgment to a great extent, a review of the Privacy Shield should take place upon application of the GDPR in May 2018 – less than a year after the full implementation of the Privacy Shield by controllers – in order to maintain a high level of protection. The Adequacy Decision II stipulates that the decision will be suspended by the Commission, justified on grounds of urgency, for a maximum period of six months in order to adapt the Privacy Shield to the new

[152] Ibid, Article 45 (2) (a).
[153] P. M. Schwartz, 'The E.U.-U.S. Privacy Collision: A Turn to Institutions and Procedures', 126 *Harvard Law Review* 7 (2013).
[154] Review, veto or appeal options might be given to the national DPA or the European Data Protection Supervisor. See European Digital Rights, 'Transfer of Data to Third Countries', (n.d.), https://protectmydata.eu/topics/transfers-to-third-countries/ (last visited 11 August 2016).

situation under the GDPR.[155] This is particularly necessary in light of the fact that the GDPR will tighten obligations on controllers, arguably exceeding the Principles II of the Privacy Shield to some extent.[156] A detailed analysis of potential consequences of the adoption of the GDPR for the Privacy Shield goes beyond the scope of this paper and should be addressed in future research.

2.5. Impact Beyond Borders: The Extraterritoriality of Adequacy

The Adequacy Decision I approving the Safe Harbour framework was not the only adequacy decision issued by the Commission. Until today, the Commission has issued adequacy decisions for Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.[157] Additionally, various other countries have applied or are about to apply for an adequacy finding.[158]

In fact, the EU adequacy assessment procedure in the DPD has strongly influenced the development of data protection standards outside the EU.[159] Given that the EU's 'border control' approach gives EU Member States the power to block data transfer to third countries – including but not only to the US – the EU's global authority has considerably increased over time.[160] This development can be traced back to, first, the aspiration of non-EU countries to have their laws acknowledged as adequate and, second, their desire to have laws considered 'the highest international standard of privacy protection'.[161] Arguably, *adequacy* can therefore no longer be considered an exclusively European concept.[162]

[155] Commission Implementing Decision C (2016) 4176 final, footnote 208.
[156] Additional obligations on data controllers such as the obligations to pursue data protection impact assessments have not been considered by the Privacy Shield framework yet.
[157] An overview of all Commission decisions on the adequacy of the protection of personal data in third countries is available at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.
[158] G. Greenleaf, 'Do not dismiss "adequacy": European data privacy standards are entrenched', *Privacy Laws & Business International Report* 114 (2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2001825 (last visited 22 August 2016).
[159] P. M. Schwartz, 126 *Harvard Law Review* 7 (2013).
[160] G. Greenleaf, *Privacy Laws & Business International Report* 114 (2011), p. 17.
[161] Ibid, p. 17.
[162] Ibid.

In spite of a slow pace in respect to the making of adequacy assessments, the EU has developed into a major actor in the global data protection debate throughout the past 25 years. Its significant influence on the development of data protection laws outside the EU has been reiterated by various studies. *Inter alia*, privacy expert Greenleaf demonstrated in 2011 that out of the then 29 jurisdictions with data protection laws from Africa, Latin America, Asia and Australia, all jurisdictions except for four had incorporated at least forty percent of the most distinctive European elements.[163] Moreover, while only seven data protection laws existed globally in 1970, today more than 100 countries from nearly all parts of the world have data protection laws.[164] Most of these countries adopted comprehensive principles for both the private and public sector, created a data protection authority and usually also provide for data export limitations similar to the EU approach.[165] Consequently, Greenleaf concludes that the DPD, together with the mandatory adequacy assessment therein, 'is the most significant overall influence on the content of data privacy laws outside of Europe, and that its influence is gradually strengthening'.[166] Today, the EU exercises global regulatory supremacy and is being used as model for many regulatory systems in the world.[167] Greenleaf considers the US, next to China, to represent a major exception to this global development of comprehensive data protection laws given that it insists on sectorial laws, as further described in chapter four.[168]

Some authors argue that the EU data protection rules have brought about the so-called 'Brussels effect',[169] being a consequence of the adequacy-based framework established by the DPD. As the EU regime has grown in influence organically, it has developed supremacy by default rather than by design.[170] That is to say that the extraterritorial impact of the EU's regime can be interpreted as a result of the EU

[163] G. Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108', 2 *International Data Privacy Law* 2 (2012).
[164] G. Greenleaf, *Privacy Laws & Business International Report* 114 (2011); Not included in these figures are the US as the country does not provide for any comprehensive data protection laws. This is further explained in chapter four. An updated overview of all data protection laws of the world is available at https://www.dlapiperdataprotection.com/#handbook/world-map-section and G. Greenleaf, 'Global Tables of Data Privacy Laws and Bills', *133 Privacy Laws & Business International Report* (2015), *UNSW Law Research Paper No. 2015-28*, http://ssrn.com/abstract=2603502 (last visited on 13 August 2016).
[165] G. Greenleaf, *Privacy Laws & Business International Report* 114 (2011).
[166] G. Greenleaf, *Privacy Laws & Business International Report* 114 (2011), p. 17.
[167] P. M. Schwartz, 126 *Harvard Law Review* 7 (2013).
[168] G. Greenleaf, *Privacy Laws & Business International Report* 114 (2011).
[169] A. Bradford, 'The Brussels Effect', 107 *Northwestern University Law Review* 1 (2012).
[170] O. Lynskey, *The Foundations of EU Data Protection Law*.

rules on data transfer to third countries. Given that third countries seek to fulfil the requirement of adequacy, they often replicate EU rules in practice. Arguably, the EU never imposed its views but rather assumed the role of a 'privacy cop'.[171] However, the introduction of an extended territorial scope of the GDPR, as depicted in the preceding sub-chapter, could be interpreted as the EU's willing exercise of supremacy over the regulatory regimes of third countries. It can be considered a bold and intentional move of the EU legislature and might suggest a slow movement from supremacy of default to supremacy of design.[172] Consequently, a question arising in this context is whether the global impact of EU rules is a reflection of simple endorsement or a by-product of the EU's commitment to high-level protection of personal data.

In sum, this chapter provides an overview of the EU data protection regime in place before and after the 'Schrems' judgement by the CJEU. It demonstrates that the DPD comprises provisions to ensure that the transfer of personal data to third countries only takes place where the Commission has found that the country in question provides an adequate level of protection of personal data. However, the adequacy requirements in Article 25 DPD are not very clear, bringing about risks of uncertainty and gaps in protection. Moreover, the chapter draws attention to the voluntary nature of the Safe Harbour framework, under which companies can self-certify their commitment to the Principles I. In light of a general lack of limitations on the derogations to the adherence to the Principles I, US public authorities could legally access personal data transferred from the EU to US organizations under the Safe Harbour. The justified criticism rocketed in the course of the Snowden revelations, which were followed by the invalidation of the Adequacy Decision I by the CJEU in the 'Schrems' ruling. Therein, the CJEU took issue with two loopholes. First, it found fault with the US public authorities' unlimited access to data transferred under the Safe Harbour and second, with insufficient legal remedies against such interference. The CJEU found that interference founded on *inter alia* national security or domestic legislation of the US must be strictly necessary and proportional while meeting objectives of general interest. It determined that adequate data protection provided by a third country must be effective in practice and essentially equivalent to that

[171] S. Simitis, 'Privacy-An Endless Debate', 89 *California Law Review* 6 (2010), p. 1993.
[172] O. Lynskey, *The Foundations of EU Data Protection Law*.

guaranteed in the EU legal order. Nevertheless, the meaning of the term *essentially equivalent* remains controversial. The standard adopted can best be interpreted as a high degree of protection in line with the EU Charter. Next, the GDPR reforms the DPD and the adequacy assessment procedure to some extent. While it incorporates the 'Schrems' ruling by prescribing enumerated conditions for the assessment of adequacy, it does not offer a final solution for a clear-cut assessment procedure yet. In any event, the Privacy Shield will have to be reviewed to ensure its validity upon the coming into force of the GDPR in 2018. Lastly, this chapter shows that many more Commission adequacy decisions are in place, approving the level of protection provided by various countries around the world. Thereby, the DPD has had and continues to have a strong influence on the development of data protection standards outside the EU.

Following this introductory chapter, the succeeding chapter comprises the main analysis providing for an answer to the research question of this paper.

3. Assessing the Adequacy of the Privacy Shield

On 12 July 2016, the Commission adopted the Adequacy Decision II, stating that the US ensured an adequate level of protection for personal data transferred from the EU to self-certified organizations in the US under the EU-US Privacy Shield.[173] In the following, I examine whether the Privacy Shield passes the 'essentially equivalent' test created by the CJEU in the 'Schrems' judgement and thereby in fact ensures adequate protection of the fundamental rights to privacy and data protection. The research question guiding the analysis is:

To what extent does the Privacy Shield meet the criteria for adequacy under Article 25 (6) of the Data Protection Directive as interpreted by the CJEU in the 'Schrems' judgement?

[173] Commission Implementing Decision C (2016) 4176 final, Article 1 (1).

To be precise, I explore whether US law provides for sufficient limitations on the access and use of personal data transferred under the Privacy Shield for national security purposes and I assess whether the US thereby ensures effective legal protection against any interference by its intelligence authorities with the fundamental rights of the persons whose data are transferred from the EU to the US. Additionally, I investigate whether oversight and redress mechanisms guarantee sufficient safeguards to ensure effective protection against unlawful interference.

To be clear, I do not assess the commercial aspects of the Privacy Shield, including the content of the Principles II. My analysis is restricted to the access and use of personal data transferred under the Privacy Shield by US public authorities. Consequently, the current legal framework and practices of the US Intelligence Community as described in the Adequacy Decision II and the Privacy Shield as well as the conditions under which it allows any unjustified interference to the fundamental rights to respect for private life and data protection, as enshrined in the EU Charter, are examined. Given that US law provides the legal bases for the US authorities' access and use of personal data, US law and practices must be discussed in detail, although the research question of this paper as such involves an assessment pursuant to the EU legal order.

The assessment of the Adequacy Shield and relevant US law is intricate in nature, particularly in light of the heightened awareness of data protection authorities and the public towards US surveillance programs in the aftermath of the Snowden revelations. While I desire to provide an impartial assessment, I cannot deny that my point of view is that of a EU lawyer. Whereas a black and white approach must be circumvented by all means, US lawyers, who may assume an inherently different approach to data protection due to distinctive ideological and constitutional standpoints, different conclusions are possible.[174]

In order to structure the pursuing analysis, chapter 3.1. describes the structural framework to be followed in this chapter. While chapter 3.2. discusses whether the Privacy Shield and the US surveillance laws are sufficiently clear and specific, chapter 3.3. carefully examines whether limitations on interference for national

[174] The different approaches to data protection regulation are juxtaposed in chapter four.

security purposes have in fact a limited scope subject to the criteria of necessity and proportionality. Chapter 3.4. scrutinizes whether the Privacy Shield provides for an independent oversight mechanism and effective redress possibilities for affected data subjects before chapter 3.6. summarizes the main findings.

3.1. Structural Framework: The 'Essentially Equivalent' Test

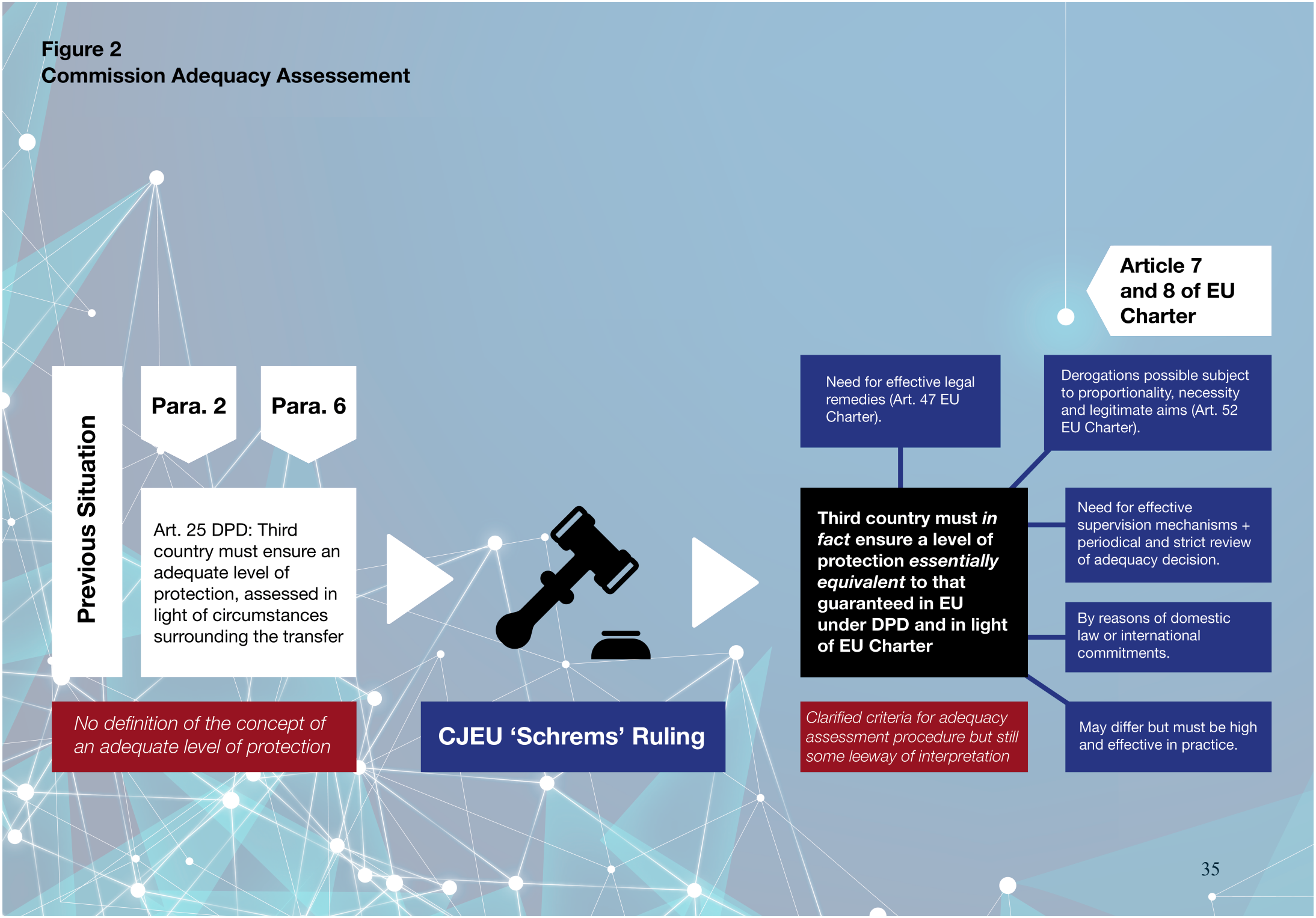
As revealed in the preceding chapter, the CJEU clarified in the 'Schrems' judgment the criteria that are relevant for an adequacy assessment under Article 25 (6) of the DPD. Firstly, the Commission must find, duly stating reasons, that the third country in question ensures in fact a level of protection of fundamental rights 'by reasons of its domestic law or its international commitments'[175] that is 'essentially equivalent'[176] to that guaranteed within the EU legal order under the DPD and read in light of the EU Charter. The Commission's discretion must be 'strict'.[177] The word *adequate* does not require a third country to provide an 'identical'[178] level of protection; whereas it may differ, it must be 'high'[179] and 'in practice, effective'[180]. Effective supervision mechanisms must exist.[181] Moreover, legitimate exceptions permitting the interference with the fundamental rights guaranteed by Articles 7 and 8 of the EU Charter must be in line with Article 52 of the EU Charter and settled case law.[182] The scope and application of respective measures must be governed by 'clear and precise rules'[183] and be limited to what is 'strictly necessary' and 'proportionate'[184] to pursue legitimate objectives of general interest such as national security.[185] Legislation is not strictly necessary, where authorities access and store personal data on 'a generalised basis'[186]. Possibilities for EU data subjects to pursue legal remedies must exist.[187]

[175] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd,* para. 71.
[176] Ibid, para. 73 and 96.
[177] Ibid, para.78
[178] Ibid, para. 73.
[179] Ibid, para. 72.
[180] Ibid, para. 73.
[181] Ibid, para. 81.
[182] Ibid, para. 91.
[183] Ibid, para. 91.
[184] Ibid, para. 90 and 92.
[185] Ibid, para. 88.
[186] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd*, para. 92 and 93.
[187] Ibid, para. 95.

These requirements illustrate the new benchmark for the level of protection of privacy and data in protection in the EU legal order, which the US legal order, as presented in the Privacy Shield framework, is scrutinized against in the following. It must be stressed that while the CJEU offers more and clearer criteria than those set out in Article 25 (2) and (6) of the DPD, they do not go beyond stating limitations and standards to comply with.[188] As such, they continue to give some leeway in assessing adequacy, particularly as it is not entirely clear how 'essential equivalence' should be measured. As clarified in chapter 2.3.1., it appears that the CJEU does not require a context-bound comparison of legal systems but rather a strict measurement against the EU Charter. Figure 2 on the following page visualizes the 'essentially equivalent' test. Additionally, an exhaustive list of the criteria stipulated by the CJEU to pursue the 'essentially equivalent' test is provided in Annex II.

[188] The CJEU did not address the exact margin of discretion granted to Member States in pursuing the difficult exercise of balancing the right of free movement of data with the fundamental right to privacy. Nor does the ruling provide advice on how to balance these fundamental rights with measures taken to fight terrorism.

Figure 2
Commission Adequacy Assessement



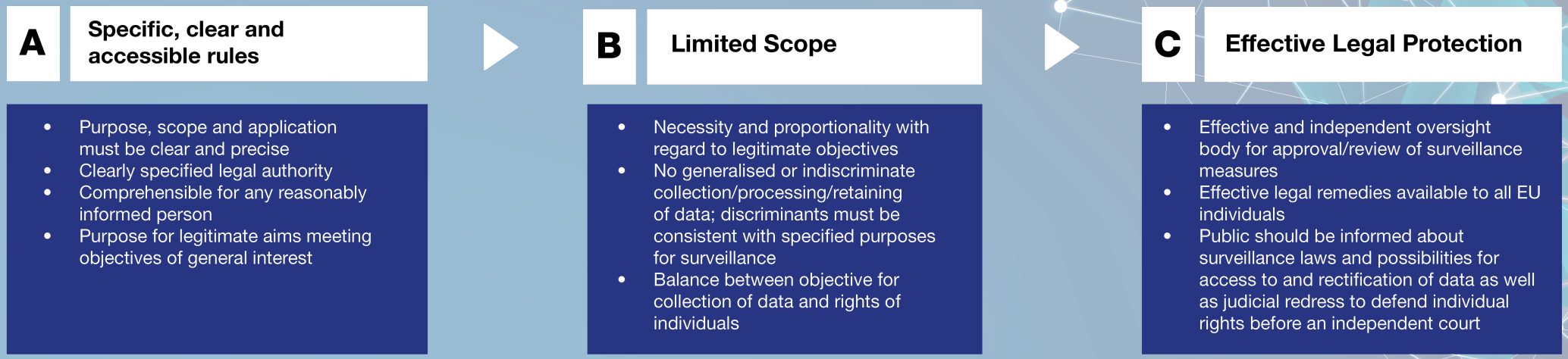
The high standards resulting from the CJEU's strict interpretation of the EU Charter can be condensed into a three-part test, laying down the basic structure for the analysis in this chapter. In line with the suggestions by the Article 29 Working Party,[189] the ensuing Figure 3 summarizes the specific legal criteria determined by the CJEU to assess whether the Privacy Shield is adequate in accordance with Article 25 (6) of the DPD and in light of the European jurisprudence on fundamental rights. More specifically, these three essential guarantees help to examine whether US surveillance activities interfere with the fundamental rights to respect for private life and data protection for national security purposes in a way that they conform with the standards set out by the CJEU in the 'Schrems' judgement.

In the following, first, chapter 3.2. discusses whether the Privacy Shield and the US legal framework described therein are sufficiently clear and specific. Then, chapter 3.3. analyses whether limitations on the access and use of personal data transferred under the Privacy Shield for national security purposes are limited in scope. Chapter 3.4. examines whether effective legal protection against such interference exists before chapter 3.5. summarizes the main findings of this analysis.

[189] Article 29 Working Party, WP 12 Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (2016), 16/EN WP 238.

Figure 3
Condensed Three-Part Test

Based on the principles in the 'Schrems' ruling and in light of European jurisprudence on fundamental rights, legislation involving interference with the fundamental rights to privacy and data protection should satisfy the following essential adequacy criteria:



3.2. A: Specific, Clear and Accessible Rules

Whereas the Commission did not explicitly mention any specific limitations on access by US authorities to data transferred under the Safe Harbour in the Adequacy Decision I,[190] the Adequacy Decision II describes in considerable detail restrictions existing under current US law in an entire section titled 'Access and use of personal data transferred under the EU-US Privacy Shield by US public authorities'.[191] Similar to the Safe Harbour scheme, the adherence to the Principles II can be limited to the extent necessary to meet national security, public interest, or law enforcement requirements. However, other than this familiar statement in the derogation provision,[192] the restrictions on access are not expressly stated in the Principles II as such. The reason is that, just at the Principles I, the Principles II are only applicable to self-certified US organizations while the US government and its agencies are not subject to the Privacy Shield framework.[193] Consequently, the Principles II, information on their enforcement as well as safeguards and limitations applicable to US national security authorities are provided in the seven Annexes to the Adequacy Decision II. This package of Privacy Shield materials consists of written assurances from diverse US government officials[194] who reiterate that the US government takes its commitments to an effective operation of the Privacy Shield 'seriously'[195].

While this subchapter further analyses the specificity and clarity of the form of the Privacy Shield containing the relevant limitations and safeguards applicable to US national security authorities, chapters 3.3. and 3.4. focus on the content of the limitations. I deliberately chose to analyse the clarity and specificity of the Privacy

[190] Except for the non-exhaustive list of limitations in the derogation provision of Commission Decision 2000/520/EC, Annex I.
[191] Commission Implementing Decision C (2016) 4176 final, recitals 67-124.
[192] Ibid, Annex II, Section I. 5.
[193] Ibid, recitals 14-19, Annex II.
[194] The Annexes include the following assurances from the US: Annex I: a letter from the International Trade Administration of the Department of Commerce, which administers the programme, describing the commitments that it has made to ensure that the Privacy Shield operates effectively; Annex II: the EU-US Privacy Shield Principles; Annex III: a letter from the US Department of State and accompanying memorandum describing the State Department's commitment to establish a Privacy Shield Ombudsperson for submission of inquiries regarding the US intelligence practices; Annex IV: a letter from the Federal Trade Commission describing its enforcement of the Privacy Shield; Annex V, a letter from the Department of Transportation describing its enforcement of the Privacy Shield; Annex VI: a letter prepared by the Office of the Director of National Intelligence regarding safeguards and limitations applicable to US national security authorities; and Annex VII: a letter prepared by the US Department of Justice regarding safeguards and limitations on US Government access for law enforcement and public interest purposes. See Commission Implementing Decision C (2016) 4176 final, Annexes I-VII.
[195] Commission Implementing Decision C (2016) 4176 final, Annex I, p. 3.

Shield framework as such, rather than the US surveillance laws only, as the latter cannot be understood if the former are unclear in the first place. In the following, chapter 3.2.1. assesses the form ad presentation of the Privacy Shield and relevant US laws, before chapter 3.2.2. examines their legal validity. Chapter 3.2.3. draws attention to linguistic issues.

3.2.1. Lack of Clarity and Specificity

Taking into account the sheer length of the Annexes to the Adequacy Decision II, delineating the safeguards and limitations applicable to US authorities, it is clear that considerable efforts were made to bring about more clarity about the circumstances in which personal data can be accessed under the Privacy Shield framework.[196] Nevertheless, it must be noted that a more exhaustive depiction of existing limitations and safeguards does not necessarily mean that the restrictions actually differ from those in place under the Safe Harbour. The detailed description is rather a necessary consequence of the 'Schrems' ruling, in which the CJEU determined that the Commission must clearly state reasons for an adequacy decision based on domestic law and international commitments.[197] In fact, the Adequacy Decision II is mostly founded on a more detailed description of existing laws rather than providing for essential changes of relevant limitations and safeguards.[198]

A problematic point resulting from these lengthy descriptions is that the Privacy Shield is a rather opaque framework with about 150 pages. It consists of the Annexes to the Adequacy Decision II, comprising the Principles II and written assurances by different US government officials as well as Annexes to the Annexes. The principles and guarantees provided by the Privacy Shield are stipulated in both the Adequacy Decision II and the Annexes, making information difficult to find and partially inconsistent. Thereby, the documents lack clarity and precision, making the accessibility of information for data subjects, organizations and data protection authorities difficult.[199] The complex structure makes it challenging to assess what limitations and safeguards are provided and whether they are effective in practice. It

[196] Hogan Lovells, *Authoritative Legal Report* (2016).
[197] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd,* para. 97.
[198] This argument is further developed in chapter 3.3.
[199] Article 29 Working Party WP 12 Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (2016), p.1.

is hence difficult for a reasonably informed person to foresee what could happen to his or her data.

Next to the information provided in the Adequacy Decision II,[200] General Counsel Robert Litt of the Office of the Director of National Intelligence (hereafter 'ODNI') presents in a letter in Annex VI the safeguards and limitations that are applicable to US national security authorities under US law.[201] He depicts the operation of 'US Intelligence Community signals intelligence collection activity'[202] by reference to the multi-layered US legal framework, including the legal bases that are relevant for providing adequate limitations and safeguards: the Foreign Intelligence Surveillance Act, the USA Freedom Act, the Executive Order 12333 and the Presidential Policy Directive 28.[203] In doing so, the ODNI offers information regarding collection limitations, retention and dissemination limitations, transparency safeguards as well as compliance and redress mechanisms.

On a positive note, it must be acknowledged that the complex information on the multi-layered legal framework is depicted in relative detail, spread over 18 pages. Nevertheless, it is still difficult for a reasonably informed person to comprehend the provided information all at once. In my opinion, the ODNI merely delivers minimum background information on both the content and functioning of the laws, impeding a quick assessment of the practical application of the depicted laws. Instead, further consultation of the original texts of the depicted laws is necessary to fully understand their scope. It must be recognized in this regard that all the original texts relating to US intelligence activities are available to the public online. They are also accessible outside the US.[204] Various policies, decisions and other declassified documents have been published particularly since the Snowden revelations in 2013, underlining efforts towards transparency taken by the US authorities.[205] Yet, the additional value

[200] Commission Implementing Decision C (2016) 4176 final, recitals 64-124.
[201] Commission Implementing Decision C (2016) 4176 final, Annex VI, p. 77-94.
[202] Ibid, Annex VI, p. 77.
[203] Their purpose, scope and application are analysed in detail in chapters 3.3. and 3.4.
[204] This conclusion is based on my own investigation. I was able to access the websites of all laws mentioned in this analysis.
[205] See report by Article 29 Working Party, WP 12 Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (2016).

and insight provided by those declassified texts in regards to intelligence activities is often limited.[206]

Consequently, given the complexity of information at hand, it is difficult to conclude that the US legal framework for surveillance activities is described clearly enough and with sufficient detail in the Privacy Shield. In sum, both the Privacy Shield and relevant US laws lack specificity and clarity. Hence, it is difficult for a reasonably informed person to foresee the situations and conditions under which public authorities can access the data relating to them.

3.2.2. The Softy: A Questionable Legal Authority

The Commission presents the written commitments and explanatory notes by various US government officials as binding commitments ensuring meaningful and effective limitations on the access to data transferred under the Privacy Shield.[207] However, it must be questioned whether these written representations would be looked upon favourably by the CJEU and would survive its legal scrutiny. In my opinion, it is not clear whether the written declarations can be considered as providing an adequate level of protection in the eyes of the Court, which requires actual findings that adequate measures are in place,[208] based on hard law with legally binding force.

On the one hand, I acknowledge the authority of the authors, as well as the fact that, following the publication of the Adequacy Decision II and its Annexes in the Official Journal of the European Union, these commitments are considered legally valid assurances.[209] On the other hand, I am of the opinion that, given the importance of these written assurances, they would deserve a higher legal value, established by hard law with a clearly specified legal authority. In an era of hyper connectivity and distributed networks, representations and commitments by public officials can play a meaningful role in the short term indeed. However, in the long run, they should not be sufficient to safeguard the rights of individuals and satisfy the needs of a globalized

[206] Ibid.
[207] Commission Implementing Decision C (2016) 4176 final, recital 140. See also Hogan Lovells, *Authoritative Legal Report* (2016).
[208] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd*, para. 83, 96 and 97.
[209] TFEU, Article 297.

digital world where various countries already provide for data protection rules.[210] This conclusion is reinforced by Max Schrems[211] and Johannes Caspar, the Commissioner for Data Protection and Freedom of Information of the German state of Hamburg. To the latter 'there are basically no law-based guarantees that are based on sufficiently justified rules. Instead, the [Commission] decision depends on trust in administrative confirmations'.[212]

3.2.3. Inconsistent Terminology

A third issue undermining the Privacy Shield's clarity and validity is the inconsistent usage of terminology in the documents at hand. The language used therein should be consistent with the EU data protection legal framework, given that the US legal framework is scrutinized against the level of protection in the EU legal order. In fact, language is neither consistent with the terminology commonly used in the EU nor with that usually employed in the US. This would not be a problem if the Privacy Shield clearly communicated the corresponding terminology under EU law and US law, respectively. However, this is not the case. Accordingly, this inconsistency necessarily leads to different understandings of the Privacy Shield and the US laws depicted therein on both sides of the Atlantic. A simple juxtaposition of essential terms generally used in the data protection debate in the EU and the US, respectively, illustrated in Table 1[213], demonstrates the potential for misunderstandings.

EU	**US**
Data Subject	Individual Concerned
Data Controller/Processor	Data User

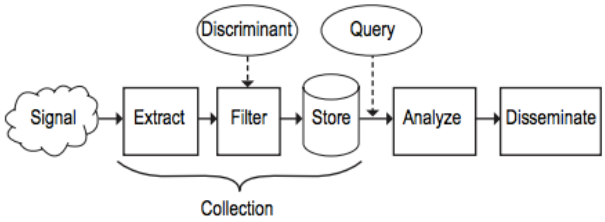
[210] European Data Protection Supervisor, Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision (2016).
[211] M. Schrems argues that 'a couple of letters […] is by no means a legal basis to guarantee the fundamental rights of 500 million European users in the long run, when there is explicit U.S. law allowing mass surveillance.' See BBC News, 'EU and US clinch data-transfer deal to replace Safe Harbour' (2016), http://www.bbc.com/news/technology-35471851 (last visited 22 August 2016).
[212] Own translation from: 'Aber bei der Problematik, auf die es am Ende auch dem EuGH ankam, nämlich die Frage, wie ein umfassender Zugriff der US-Administration auf die Daten von EU-Bürgern rechtstaatlich eingehegt wird, gibt es an sich keine rechtstaatlichen Garantien, die eben auf hinlänglich begründeten Regelungen fußen, sondern letztlich setzt die Entscheidung auf Vertrauen in Verwaltungszusagen. Und das dürfte möglicherweise vor einer erneuten Prüfung des EuGHs schwierig werden, hier den Test der Angemessenheit zu bestehen'. See Interview with Johannes Caspar on the Privacy Shield, NDR Kultur, 'Johannes Casper zum "Privacy Shield"' (2016), http://www.ndr.de/kultur/Johannes-Caspar-zum-Privacy-Shield,journal440.html (last retrieved 19 August 2016).
[213] The table is based on my own conclusion following the examination of the Privacy Shield and extensive research on comparative privacy law.

Personal Data	Personally Identifiable Information
Data Protection laws/principles	(Information) privacy laws/principles

Table 1

When searching for these legal terms in the Adequacy Decision II, drafted by the Commission, and its Annexes, drafted by US officials, one soon realizes that the terms *data subject* and *individual concerned* as well as *personal data* and *personal information* are used interchangeably. While the terms *data user* and *information privacy laws* are not mentioned at all by neither of both, US officials also employs the European terms *processor* and *data protection*. Moreover, in the Adequacy Decision II and its Annexes, words like *targeting*, *collection*, *use* or *search* are often used contrary to the meaning one would subscribe to in the EU. For instance, the Commission uses the word *access* in chapter three of the Adequacy Decision II[214] in a way that suggests the collection of personal data, rather than the process of allowing an individual to see its data after it was collected by authorities. Yet, the word *collection,* as used in the Annexes by US officials, appears to illustrate the actual search operation rather than the initial taking from a service provider, which is the understanding under EU law,[215] as illustrated in Figure 4.[216]

Figure 4



For rules to be specific and clear in line with the jurisprudence of the CJEU, the collection of data by companies and an individual's right to access his or her data must not be confused with each other. Relevant terminology must be used consistently throughout all documents for a reasonably informed person to be able to understand their content. Dissimilar terms and concepts in the Adequacy Decision II and the Annexes might be a consequence of lacking consent between the US and

[214] Commission Implementing Decision C (2016) 4176 final, chapter three on the 'Access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities', recitals 64-135.
[215] Directive 95/46/EC, Art. 2 (b) states, in light of Article 8 of the EU Charter, that processing of data includes various activities such as collection, recording, organization, storage, use, disclosure etc.
[216] The figure is taken from National Research Council, *Bulk Collection of Signals Intelligence – Technical Options* (2015), p. 28.

the EU on uniform definitions. In this case, there should at least be sufficient guidance on the meaning of the different key terms regarding their usage in the EU and the US, respectively.[217]

It must be noted that definitions are provided for the terms *personal data* and *personal information*, as well as for *processing* and *controller*.[218] All of these terms are well defined and in line with the respective definitions in the DPD.[219] However, various other important terms such as *agent*, *processor*, *signals intelligence* or *EU individual* lack a clear definition, which is necessary for a coherent understanding of the rules and principles by data controllers and processors, the general public and national supervisory authorities. In particular, a lack of clarity regarding those who benefit from protection under the Privacy Shield is prevalent. It is not clear who can be considered a *EU individual* or *EU data subject*[220] – all EU citizens or all individuals residing in the EU? The answer to this question is of crucial importance, not at least to determine who has a right to redress. For the sake of consistency, this paper further refers to *EU individuals*, without being able to provide a definition.

Particularly problematic in this context is that US law will apply 'to questions of interpretation and compliance with the Principles and relevant privacy policies […] except where such organizations have committed to cooperation with [EU DPAs]'.[221] The question arising is how US law can apply to questions of interpretation when various underlying terms derive from EU law, including essential terms such as *personal data*, *processing* or *controller*, whose definitions are provided by the DPD.[222] The EU definition of *personal data*, in particular, is much broader in scope than the US concept of *personally identifiable information*.[223] Consequently, it is uncertain how the Principles II, being dominated by EU legal terms, can be interpreted coherently in line with US law.[224] This uncertainty further contributes to

[217] For instance, definitions for key terms could be added in an appendix to the Privacy Shield.
[218] Commission Implementing Decision C (2016) 4176 final, Annex II, Section I. 8. (a)-(c).
[219] Directive 95/46/EC, Art. 2 (a), (b) and (d).
[220] The terms *data subject* and *EU individual* are used interchangeably in the Adequacy Decision II and the Annexes.
[221] Commission Implementing Decision C (2016) 4176 final, Annex II, Section I. 1. (7), p. 18.
[222] Op. cit.: 202 and 203.
[223] P. M. Schwartz and D. J. Solove, 'Reconciling Personal Information in the United States and the European Union', 102 *California Law Review* 4 (2014).
[224] G. Voss, 'The Future of Transatlantic Data Flows, Privacy Shield or Bust?', 19 *Journal of Internet Law* 11 (2016).

the overall inconsistency of the Privacy Shield and to an incoherent understanding of the limitations applicable to the activities of US national security authorities.

In essence, it can be concluded that the Privacy Shield suffers from a general complexity of documents while lacking clarity and specificity in regards to structure and terminology. It is questionable whether the written commitments by US officials can be considered hard law with legally binding force that would stand up to legal scrutiny by the CJEU. The Privacy Shield is not able to convey to a reasonably informed person what can happen with her or his data when transferred to the US, to what extent interference by US intelligence authorities can be limited and what legal avenues of redress are available for EU individuals. In sum, criterion A is not met.

3.3. B: Limited Scope

Annex II, Sections I. 5. (a) to the Adequacy Decision II states that adherence to the Principles II may be limited to the extent necessary to meet national security, public interest or law enforcement requirements. Annex II, Section I. 5. (b) further authorizes restricted adherence by statute, government regulation, or case law that creates conflicting obligations, provided that, in exercising any such authorization, an organization can show that its non-compliance with the Principles II is limited to the extent necessary to satisfy the overriding legitimate interests. It is noticeable that these derogations are the same as those stipulated in the Safe Harbour framework. The requirements for their legal basis as well as the purpose remain broad in both sections.

Accordingly, the crucial question arising in light of the ‘Schrems’ ruling is whether the current US legal framework and practices of US intelligence authorities provide sufficient limitations for the circumstances under which the interference with the fundamental rights to respect for private life and data protection is permitted. In fact, the Commission concludes in the Adequacy Decision II that

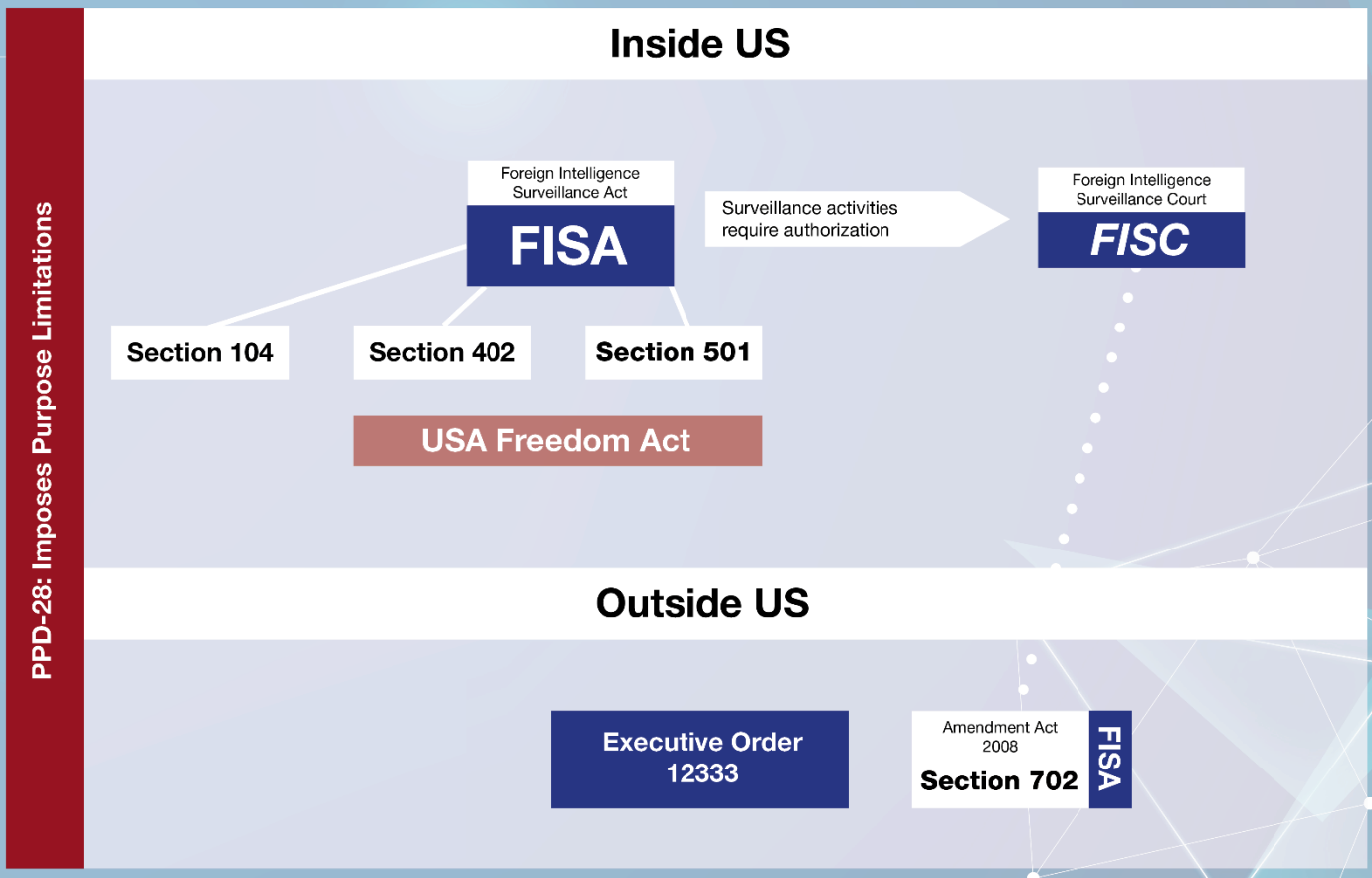
> there are rules in place in the United States designed to limit any interference for national security purposes with the fundamental rights of the persons whose personal data are transferred from the Union to the US

> to what is *strictly necessary* to achieve the *legitimate objective* in question.[225]

Accordingly, this subchapter examines whether the Commission's conclusion is correct that the US legal framework includes sufficient rules that intend to limit the access and use of personal data transferred under the Privacy Shield for national security purposes, in line with the criteria outlined in chapter 3.1. In order to determine whether the Privacy Shield is capable of providing truly adequate protection that is essentially equivalent to that afforded in the EU legal order, the US legal framework is discussed in detail. Given that 'U.S. Intelligence Community signals intelligence collection'[226] is governed by a mosaic of laws and policies, each legal instrument authorizing signals intelligence activities is analysed separately. First, chapter 3.3.1. reviews Section 702, being the most relevant legal basis established by the Foreign Intelligence Surveillance Act, as well as the US Freedom Act. Chapter 3.3.2. considers the Executive Order 12333. Lastly, chapter 3.3.3. examines the Presidential Policy Directive 28. Given the complexity of the US legal framework, the subsequent analysis is guided by the illustration in Figure 5. The analysis mostly relies on the information regarding US signals intelligence collection activities provided by the Commission in the Adequacy Decision II as well as by US officials in the letters in Annex III[227] and VI[228] to the Adequacy Decision II. While these documents mentioned and shortly summarized all laws, the original texts of the discussed laws were consulted as well for a complete understanding.

[225] Commission Implementing Decision C (2016) 4176 final, recital 88.
[226] For the matter of simplicity, this paper adopts the term *signals intelligence collection*, which the Privacy Shield refers to regularly without providing any definition.
[227] Letter from US Secretary of State John Kerry on the commitment to establish an Ombudsperson.
[228] Letter from General Counsel Robert Litt, Office of the Director of National Intelligence, on the operation of US Intelligence Community signals intelligence collection activity.

Figure 5
US Legal Framework for Surveillance on non-US persons for National Security Purposes



3.3.1. Section 702 FISA and USA Freedom Act

Broadly speaking, US intelligence authorities may only[229] collect personal data transferred under the Privacy Shield from the EU to the US where their request conforms with the Foreign Intelligence Surveillance Act (hereafter 'FISA').[230] Since its enactment in 1978, FISA governs the conduct of electronic surveillance in the US to acquire foreign intelligence information in order to protect against potential terrorists or spies of foreign powers against the US.[231] FISA includes several legal bases that can be used to collect and subsequently process the personal data of EU individuals transferred under the Privacy Shield.[232] Next to Section 104 FISA,[233] covering traditional individualised electronic surveillance, and Section 402 FISA,[234] covering the installation of pen registers or trap and trace devices, the two principal instruments are Section 501 FISA,[235] covering the collection of tangible things, and Section 702 FISA[236], which this paper focuses upon.

The US government passed Section 702 as part of the FISA Amendment Act in 2008, expanding the scope of FISA to activities conducted outside the US.[237] As legal basis for the intelligence programs PRISM and UPSTREAM,[238] Section 702 came under scrutiny in the course of the Snowden revelations. It authorizes the acquisition of foreign intelligence information, both the content of Internet and telephone communications, of non-US persons outside the US, targeted with the assistance of communications service providers.[239] Thus, Section 702 FISA may be used to collect and process the personal data of EU individuals, which is transferred under the Privacy Shield. [240]

---

[229] Additionally, the Federal Bureau of Investigation (hereafter 'FBI') can collect data based on law enforcement authorization. See Commission Implementing Decision C (2016) 4176 final, recitals 125-137.
[230] 50 U.S.C. Chapter 36 §§ 1801-1885c; Alternatively, the request can be made by the FBI based on the so-called National Security Letter, a form of statutorily authorized administrative order. See Commission Implementing Decision C (2016) 4176 final, recital 78 and Annex VI, Section III, p. 89-90.
[231] However, over time, US Congress expanded the scope of FISA to apply to physical searches in the US as well 50. See U.S.C. Chapter 36 §§ 1801-1885c.
[232] Commission Implementing Decision C (2016) 4176 final, recital 78.
[233] 50 U.S.C. § 1804.
[234] 50 U.S.C. § 1842.
[235] Formerly known as Section 215 of the U.S. Patriot Act, it authorizes the FBI to request a court order in order to produce tangible things such as telephone metadata or business records for foreign intelligence purposes. See Commission Implementing Decision C (2016) 4176 final, footnote 83.
[236] It permits the US Intelligence Community to access information such as the content of Internet communications from within the US of targeted non-US persons located outside the US. See Commission Implementing Decision C (2016) 4176 final, footnote 83.
[237] FISA Amendments Act of 2008, Public Law No. 110-261, 122 Stat. 2438 (codified at 50 U.S.C. § 1881(a)).
[238] Commission Implementing Decision C (2016) 4176 final, recital 81.
[239] Ibid, Annex VI, Section II, p. 86.
[240] Commission Implementing Decision C (2016) 4176 final, recital 78.

Section 702 requires the Attorney General and the Director of National Intelligence[241] to submit annual certifications to the so-called Foreign Intelligence Surveillance Court (hereafter 'FISC').[242] These written certifications must identify specific categories of foreign intelligence to be collected that fall into the categories of foreign intelligence provided by the FISA statute.[243] The letter of the ODNI in Annex VI to the Adequacy Decision II refers to a report by the supervisory Privacy and Civil Liberties Board[244], which noted that '[t]hese limitations do *not* permit unrestricted collection of information about foreigners'.[245]

Furthermore, the General and the Director must certify under oath before the FISC that 'a *significant purpose* of the acquisition [of the foreign intelligence information] is to obtain foreign intelligence'.[246] In fact, there is neither the need to prove a probable cause, relevance or a reasonable articulable suspicion, nor the existence of any foreign power or agent. Thus, the significant purpose is exceedingly wide and it must be questioned whether the principles of necessity and proportionality are fulfilled in the pursuance of a truly legitimate objective, as required by the CJEU in the 'Schrems' ruling.

The written certifications must also refer to 'targeting' and 'minimization' procedures, to be reviewed and approved by the FISC.[247] While the targeting procedures shall generally ensure that the collection is only pursued as authorized by statute, the minimization procedures are intended to restrict the acquisition, dissemination and retention of information about *US persons*. According to the ODNI, the minimization procedures 'provide substantial protection to information about *non-U.S. persons* as well'.[248] Yet, it is not very specific as regards the circumstances in which Section 702 provides protection to non-US persons. In fact, it is unclear which minimization procedures under Section 702 apply to non-US persons. This is particularly worrying in light of the fact that prior to the adoption of the Presidential Policy Directive 28,

[241] That is, two Cabinet-level officials appointed by the President and confirmed by the Senate.
[242] 50 U.S.C. §§ 1881a (a) and (b).
[243] 50 U.S.C. §1801 (e).
[244] The function of the Privacy and Civil Liberties Board is further depicted in chapter 3.4.1.
[245] Commission Implementing Decision C (2016) 4176 final, Annex VI, Section II, p. 86. The report is available at https://www.pclob.gov/library/702-Report.pdf (last visited 26 August 2016).
[246] 50 U.S.C. § 1881a (g) (2) (A) (v) (emphasis added).
[247] 50 U.S.C. §§ 1881a (f) and (e).
[248] Commission Implementing Decision C (2016) 4176 final, Annex VI, Section II, p. 86 (emphasis added).

analysed in chapter 3.3.3., none of the minimization procedures under Section 702 FISA applied to non-US persons.[249] Hence, it appears that the scope of application of the minimization procedures has not expanded very much since then.
Whereas the FISC reviews the compliance of the written certifications as well as the targeting and minimization procedures with the statutory requirements,[250] there is no need to provide a factual basis justifying the procedures of such kind. Upon issuance of the order approving the certification and the procedures, collection of data under Section 702 is, according to the ODNI, no longer 'bulk or indiscriminate'[251]. Instead, it would entirely target specific persons about whom an individualized determination had been made by means of individual selectors.[252] The basis or the selection of the target must be documented and reviewed by the Department of Justice.[253] However, it must be questioned whether the usage of selectors automatically means that data collection can be considered discriminate and limited in scope.

Overall, the ODNI ensures in Annex VI to the Adequacy Decision II that Section 702 does not entail 'mass and indiscriminate' but only 'narrowly focused' collection of foreign intelligence.[254] The Commission reiterates in the Adequacy Decision II that collection is 'carried out in a targeted manner through the use of individual selectors'.[255] Its conclusion is based on the US Intelligence Community's explicit assurance' that it will 'not engage in indiscriminate surveillance of anyone, including ordinary European citizens'.[256]

On the one hand, Section 702 of FISA is unique among US intelligence programs as it provides at least nominal judicial review for non-US persons.[257] The legal authorization and review process for surveillance under Section 702 FISA is

[249] D. Severson, 'American Surveillance of Non-U.S. Persons: Why New Privacy Protection Offer Only Cosmetic Change', 56 *Harvard International Law Journal* 2; Nat'l Sec. Agency, Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended § 3(b)(1) (hereinafter 'minimization procedures'), available at https://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf, §7 reads: 'Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy'.
[250] 50 U.S.C. §§ 1881a (d)-(e).
[251] Commission Implementing Decision C (2016) 4176 final, Annex VI, Section II, p. 86.
[252] Ibid.
[253] 50 U.S.C. § 1881a (l).
[254] Commission Implementing Decision C (2016) 4176 final, Annex VI, Section II, p. 85-86.
[255] Ibid, recital 81.
[256] Ibid, recital 82.
[257] D. Severson, 'American Surveillance of Non-U.S. Persons: Why New Privacy Protection Offer Only Cosmetic Change', 56 *Harvard International Law Journal* 2.

theoretically a valuable means to ensure that the collection of foreign intelligence information has a limited scope while pursuing legitimate objectives – particularly in light of the on-going fight against terrorism.[258] On the other hand, the FISC has a very limited authority to review the certifications as well as the targeting and minimization procedures in practice. It can merely conclude that the government's certifications are sufficient and that the minimization and targeting procedures meet statutory requirements.[259] Hence, FISC does not review individual targeting decisions and has only little influence on whether the principles of proportionality and necessity are fully complied with.[260] To this adds that the FISC only rejected 12 out of 38,270 FISA surveillance orders between 1979 and 2013.[261] These striking numbers strongly suggest that the FISC does not engage in a very strict authorization and review process. However, given that Section 702 provides an extremely broad surveillance authority,[262] a very strict and precise authorization process is crucial to continuously maintain a balance between the objective of data collection and the fundamental rights of individuals. In particular, there should be more clarity and transparency on the minimization and targeting procedures.

It must be acknowledged that, generally spoken, the targeting and minimization procedures illustrate a useful feature of the authorization process under Section 702 FISA, as they can assist in restricting the collection and processing of the personal data of EU individuals that is transferred under the Privacy Shield. However, it remains unclear how the targeting and minimization procedures of the Intelligence Community operate in fact and how the discriminants and individual selectors for collection are chosen. In the letter in Annex VI, the ODNI stipulates that about 90,000 individuals where targeted under Section 702 in 2014, being 'a miniscule fraction of the over 3 billion Internet users throughout the world'.[263] Comparing the amount of individuals targeted under Section 702 with the amount of worldwide Internet users

[258] Particularly since the terrorist attack on 11 September 2001, the US engages in more extensive bulk collection and monitoring, which requires legal authorization through *inter alia* the US Patriot Act of 2001, Public Law No. 107-56, 115 Stat. 272.
[259] 50 U.S.C. § 1881a (i).
[260] D. Severson, 56 *Harvard International Law Journal* 2.
[261] Numbers are retrievable at the website of the FISC, http://www.fisc.uscourts.gov/.
[262] The majority of data stored with American cloud services and telecommunication services is associated with foreign users or businesses. Consequently, according to General Counsel Robert Litt, collection under Section 702 is 'one of the most valuable sources of intelligence protecting both the United States and our European partners'. See Commission Implementing Decision C (2016) 4176 final, Annex VI, Section II, p. 86.
[263] Commission Implementing Decision C (2016) 4176 final, Annex II, p. 87.

might aim at relativize the number but is neither a logic nor adequate justification for extensive US surveillance activities.

Overall, given the lack of information about the assessment and content of the targeting and minimization procedures, it is difficult to preclude that the interference with the fundamental rights to privacy and data protection under Section 702 FISA is sufficiently limited in accordance with the principles of necessity and proportionality. It is also difficult to assess whether the discriminants used for the targeting and minimization procedure are in line with the specified purposes for the surveillance activities in question. At the same time, the purpose for the acquisition of foreign intelligence information can be very broad as long as it is significant, which is very vague criterion. In sum, in spite of assurances by the ODNI, it cannot be ruled out that surveillance activities pursuant to Section 702 FISA involve generalised and indiscriminate collection.

As mentioned, other legal bases are available for the collection of personal data of EU individuals transferred under the Privacy Shield, including Section 402 FISA[264] and Section 501 FISA[265]. Enacted on 2 June 2015, the USA Freedom Act[266] prohibits bulk collection of any records of US and non-US persons under Section 402 FISA, authorizing the installation of pen registers or trap and trace, and Section 501 FISA, authorizing the collection of tangible things.[267] Both the US authorities and the Commission refer to the USA Freedom Act as a positive development since the Snowden revelations by modifying US surveillance laws to the extent that indiscriminate surveillance is limited and transparency under FISA enhanced.[268]

While acknowledging the introduction of the USA Freedom Act as a welcome development and a step into the right direction, its actual impact on the collection of personal data of EU individuals under the Privacy Shield is limited. That is, collection

[264] This legal authority does not regard the content of communications but information about customers or subscribers using a service, such as name, address, length of service received, means of payment etc. See 50 U.S.C. § 1842.
[265] Formerly known as Section 215 of the USA Patriot Act, it authorizes the FBI to request a court order in order to produce tangible things such as telephone metadata or business records for foreign intelligence purposes. See Commission Implementing Decision C (2016) 4176 final, footnote 83.
[266] USA Freedom Act of 2015, Public Law No. 114-23.
[267] Commission Implementing Decision C (2016) 4176 final, recital 79 and Annex VI, Section III, p. 88-90.
[268] For instance, Section 501 FISA was transformed from Section 215 USA Patriot Act; Commission Implementing Decision C (2016) 4176 final, recital 79 and Annex VI, Section III, p. 89.

continues to be possible where based on a 'specific selection term'[269] – a term identifying a person, his or her address, account or personal device. Thereby, the scope of the information retrieved by US authorities shall be limited 'to the greatest extent reasonably practicable'.[270] Consequently, the supposed prohibition rather implies a restriction, which facilitates a more focused and targeted collection procedure of information for intelligence purposes.

Moreover, the application of the USA Freedom Act is limited to two very specific legal bases under FISA, excluding the important Section 702 FISA. Consequently, the protection provided under the USA Freedom Act is largely 'irrelevant' for data transferred under the Privacy Shield.[271] Although the US government highlights the improvements for EU individuals achieved through the USA Freedom Act, it is not primarily focusing on data coming from the EU and it must hence be assumed that the USA Freedom Act was not only introduced to sooth European concerns. In sum, in can be concluded that the USA Freedom Act is most probably not able to impede the generalized and indiscriminate collection of records based on Section 402 and 501 FISA given that the selection terms can only focus but not prevent respective national intelligence activities.

Overall, neither Section 702 FISA nor the USA Freedom Act is designed in a way that interference with the fundamental rights to privacy and data protection is limited to what is strictly necessary and proportionate given that both laws authorize the collection of personal data transferred to the US under the Privacy Shield on a generalized basis, although targeted and narrowly focused. Given that there is not sufficient transparency of on the minimization procedure and the specific selection terms, respectively, as absolute prohibition of bulk collection must be questioned. Thus, Section 702 FISA and the USA Freedom Act do not meet the standards set out by the CJEU in the 'Schrems' ruling.

3.3.2. Executive Order 12333

[269] Commission Implementing Decision C (2016) 4176 final, Annex VI, Section III, p. 89.
[270] Ibid.
[271] M. Schrems, '"EU-US Privacy Shield": Towards a new Schrems 2.0 Case?', *European Area of Freedom Security &Justice Free Group* (2016).

FISA governs surveillance programs targeting non-US persons that are conducted inside the US (and since the passing of Section 702, as part of the 2008 Amendment Act, also outside the US) through authorization by the US Congress. In contrast, most surveillance activities regarding non-US persons occurring outside the US are pursued at the discretion of the US President.[272] US Presidents direct the acquisition of foreign intelligence in line with their constitutional responsibility as Commander in Chief, Chief Executive and their constitutional authority to conduct US foreign relations.[273] They direct the conduct of intelligence activities of the US Intelligence Community particularly by means of issuing Executive Orders and Presidential Directives or by executing law enacted by the Congress, which may provide guidance or impose limitations.[274] Two central legal instruments exist that are directly relevant when the privacy interests held by non-US persons are at stance, including those of EU individuals under the Privacy Shield: the Presidential Policy Directive 28 (hereafter 'PPD-28'), further analysed in chapter 3.3.3., and Executive Order 12333 (hereafter 'EO 12333').

In 1981, President Reason issued Executive Order 12333.[275] The executive order lays down rules for the exercise of intelligence activities outside FISA's scope. Thus, covering almost all surveillance that is not dealt with by FISA, EO 12333 is the primary basis for surveillance activities outside of the US.[276] The executive order authorizes foreign intelligence investigations, including bulk and targeted intelligence programs, regarding the content of both communications and metadata.[277] Restrictions on collection, retention and dissemination exist but apply only to US persons. [278] Thus, restrictions do not apply to EU individuals whose data is transferred under the Privacy Shield. Moreover, due to its legal position as executive orders, EO 12333 is not subject to oversight from Congress. Hence, it acts in a zone of twilight, lacking any meaningful form of oversight, judicial review possibilities or redress mechanisms.[279]

[272] US Constitution, Article II.
[273] Ibid.
[274] Commission Implementing Decision C (2016) 4176 final, recital 68.
[275] Executive Order 12333, United States Intelligence Activities, Federal Register Vol. 40, No. 235 (1981).
[276] D. Severson, 56 *Harvard International Law Journal* 2.
[277] Ibid.
[278] Executive Order 12333, United States Intelligence Activities, § 2.4. does not refer to non-US persons.
[279] The Commission acknowledges in the Adequacy Decision II that it is 'clear that at least some legal bases that U.S. intelligence authorities may use (*e.g. E.O. 12333*) are not covered' and thus not available under US law to EU individuals. This is worrying in light of the executive order's broad legal authority; there is an urgent need for

Although Executive Order 12333 governs most intelligence operations,[280] neither the Commission nor the ODNI provide sufficient information on its actual scope. In fact, they hardly mention it at all. Both the Adequacy Decision II and the Privacy Shield lack information on the geographical scope, on the extent to which data can be collected, retained and disseminated as well as on the specific offences that permit surveillance.[281] In comparison to other legal bases for surveillance mentioned in the Adequacy Decision II and the Annexes, the Commission refrains from making an explicit statement, in which it reiterates its confidence in EO 12333 to ensure an adequate level of protection of fundamental rights essentially equivalent to that assured in the EU legal order. The question arises why such a limited amount of information is provided on one of the most commonly used surveillance authorities, suggesting that existing procedures are non-transparent. Consequently, as the scope and application of EO 12333 are not sufficiently clear and precise it is difficult if not impossible to assess whether the scope of the collection in question is sufficiently limited, meeting the principles of necessity and proportionality, as determined by the jurisprudence of the CJEU. In sum, in light of non-transparency and the lack of information regarding the scope of EO 12333, it must be questioned whether the access to data transferred under the Privacy Shield to the US is sufficiently limited by Executive Order 12333 in light of the 'Schrems' ruling.

3.3.3. Presidential Policy Directive 28

In order to reform and streamline the procedures for surveillance programs,[282] US President Barack Obama issued on 17 January 2014 Presidential Policy Directive 28 (hereafter 'PPD-28').[283] It sets out consistency principles and requirements with which US signals intelligence operations, no matter which program and irrespective of the nationality and location of the person of whom the data be related to, shall be authorized and executed. Hence, PPD-28 also applies to the collection and

---

wide-ranging judicial and congressional oversight and transparency instruments. Commission Decision 2000/520/EC, recital 115 (emphasis added).

[280] D. Severson, 56 *Harvard International Law Journal* 2.

[281] This is reiterated by the Commission by stating that EO 12333 defines the goals, directions, duties and responsibilities of US intelligence efforts '[t]o the extent that the Executive Order is publicly accessible'. See Commission Implementing Decision C (2016) 4176 final, footnote 59.

[282] As explained, the US Constitution stipulates that national security is under the authority of the President as Commander in Chief, as Chief Executive and as regards foreign intelligence. The President can direct the activities of the US Intelligence Community, in particular through executive orders or presidential directives. See US Constitution, Article II.

[283] Commission Implementing Decision C (2016) 4176 final, recital 69.

processing of personal data for surveillance purposes when transferred under the Privacy Shield, including collection under Section 702 FISA.[284]

While PPD-28 is not a legal basis for the collection of data such as Section 702 FISA and the Executive Order 12333, it introduces purpose limitations for the use of personal data and conditions according to which they can be disseminated. First, it stresses that signals intelligence may only be collected where authorized by statute or executive order and for 'legitimate and authorized national security purposes'[285]. In this regard it should be acknowledged that PPD-28 is very clear in determining that signals intelligence can only be collected with a well-defined legal authority. Any interference must be scrutinized against a valid enacted and enforceable law. However, in comparison to Section 702 FISA, there is no need for a *significant* purpose but simply *a* foreign intelligence purpose. Hence, the requirements are comparably watered down. Second, PPD-28 states that signals intelligence activities must always be 'as tailored as feasible'.[286] While recognizing these limitations, it appears rather difficult to determine the precise meaning of this restriction. Accordingly, it is unclear whether the assessment of a limited scope based on the principles of necessity and proportionality is required. Are the discriminants in line with specified purposes for surveillance or does surveillance continue to occur on a generalized basis, while being roughly limited by broad filters?

Moreover, PPD-28 permits the Intelligence Community to engage in bulk collection 'in order to identify new or emerging threats and other vital national security information that is often hidden within the large and complex system of modern global communications'.[287] According to PPD-28, bulk collection is defined as the collection of signals intelligence that 'due to technical or operational considerations, is acquired without the use of discriminants (such as specific identifies or selection terms)'.[288] In this regard, the US appears to engage in a debate on semantics to justify the supposedly limited scope of PPD-28, arguing that the filters and technical tools could not be considered 'mass' or 'indiscriminate'.[289] Hence, what counts as

[284] Implementing Decision C (2016) 4176 final, Annex II, p. 85.
[285] Implementing Decision C (2016) 4176 final, Annex VI, Section I. (a), p. 78.
[286] Ibid, Annex VI, Section I. (a) and (b), p. 78-79.
[287] Ibid, Annex VI, Section I. (b), p. 79.
[288] Ibid, Annex VI, Section I. (b), p. 79.
[289] Implementing Decision C (2016) 4176 final, Annex VI, p. 95.

bulk collection is not obvious.[290] Where the US considers it necessary be treated with dignity comprising measures to counter threats coming from 'espionage, terrorism, weapons of mass destructions, threats to cyber security, to the Armed Forces or military personnel, as well as transitional criminal threats related to the other five purposes'.[291]

While applauding the introduction of the above mentioned purpose limitations, I perceive them as being very wide and possibly too wide to be considered sufficiently clear and precise as required by the CJEU. They lack instructions on what each exception means and how they should be balanced with EU fundamental rights.[292] This is particularly worrying in light of the fact that the act of balancing privacy and civil liberties of EU citizens with the practical necessities of intelligence activities is at the discretion of the Intelligence Community, which cannot be scrutinized. In the Adequacy Decision II, the Commission concludes that

> [a]lthough *not phrased in those legal terms*, [the PPD-28 principles] capture the essence of the principles of necessity and proportionality. Targeted collection is clearly prioritised, while bulk collection is limited to (exceptional) situations where targeted collection is not possible for technical or operational reasons. Even where bulk collection cannot be avoided, further "use" of such data through access is strictly limited to specific, legitimate national security purposes.[293]

Consequently, there is a need for explicit reassurances that the principles of necessity and proportionality are met. A limited scope satisfying the standards of the EU jurisprudence cannot be demonstrated by legitimising the routine of targeted collection by US public authorities pursued according to unclear criteria and founded on a legal basis under US law. While PPD-28 appears to trigger a trend to move from indiscriminate surveillance activities on a general basis to more targeted and selected operations, the actual scale of signals intelligence as well as the amount of data transferred from the EU, potentially subject to the collection and use by US authorities from the moment of transfer onwards, is potentially still very high and must thus be questioned.[294] Consequently, while PPD-28 explicitly continues to

[290] D. Severson, 56 *Harvard International Law Journal* 2.
[291] Ibid, Annex VI, Section I. (b), p. 80.
[292] To this adds that the concept of 'reasonableness' shall be used in balancing efforts to protect legitimate privacy and civil liberties with 'the practical necessities' of signals intelligence operations. See ibid, Annex VI, Section I. (b), p. 80.
[293] Implementing Decision C (2016) 4176 final, recital 76 (emphasis added).
[294] See for example clarifications in Implementing Decision C (2016) 4176 final, Annex VI, Section I. (a) that the PPD-28 would apply to data collected from transatlantic cables by the US Intelligence Community. The ODNI states that if the Intelligence Community collected data from transatlantic cables in the course of being transmitted

enable the collection of personal data in bulk; the scale of such collection option remains unclear. In fact, it is potentially broad given that the ODNI refuses to provide EU individuals with a precise number regarding the amount of bulk collection activities: 'any bulk collection activities regarding Internet communications that the U.S. Intelligence Community performs through signals intelligence operate on a *small proportion* of the Internet'[295].

Lastly, perhaps the greatest modification introduced by PPD-28 is a public acknowledgement that non-US persons, and hence, EU individuals, have a legitimate privacy interest by stating that the US government 'must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information'.[296] Although even this pronouncement is restricted to the extent that it only applies to the *handling* rather than the *collection* of personal data, the statement opens the door for future reform. It alters the debate from *whether* non-US persons should receive privacy protection to *how many* they should have.[297]

In sum, PPD-28 has the potential to transform US intelligence programs in the long run, given the historic acknowledgement that non-US persons must be treated with dignity. However, PPD-28 has not changed US surveillance law to the extent necessary that it would pass the 'essentially equivalent' test at this point in time, as it continues to authorize the indiscriminate collection of personal data in bulk. If the US seeks to uphold the six national security purposes that authorize the data collection in bulk in the future, further guidelines, describing neatly and in debt what each exceptions means and how it meets the criteria of proportionality and necessity, should be created. Such guidelines should also elucidate how the purpose of each exception is to be balanced with the fundamental rights to privacy and data protection.

---

to the US, 'it would do so subject to the limitations and safeguards set out herein, including the requirements of PPD-28'. It neither denies nor confirms whether it uses cables interception as a means to collect intelligence data. This is worrisome in absence of established jurisprudence establishing the legality of cables interception.

[295] Ibid, Annex VI, Section I. (b), p. 80.

[296] Presidential Policy Directive, Signals Intelligence Activities (2014); Prior to PDD-28, the US government made no effort to protect the privacy of non-US persons. For instance, for electronic surveillance none of the minimization procedures under Section 702 FISA applied to non-U.S. persons. Op. cit.: 246.

[297] D. Severson, 56 *Harvard International Law Journal* 2.

Overall, summarizing this chapter, the limitations to the Principles II provided in the Privacy Shield are exactly the same as the limitations to the Principles I in the Safe Harbour. The adherence to the Principles II can be limited to the extent necessary to meet objectives of general interest such as national security or law enforcement requirements as well as statues, government regulations or case law that create conflicting obligations. Consequently, US law continues to take primacy over the privacy principles, which was one essential criterion the CJEU found fault with in the 'Schrems' judgement. Hence, it is all the more important that the Privacy Shield demonstrates the existence of effective US rules that can ensure the adequate protection of fundamental rights in line with the 'Schrems' criteria in case of interference by national authorities. Nevertheless, the representations of the ODNI in the Annexes to the Adequacy Decision II do not offer sufficient information proving that massive and indiscriminate collection of personal data transferred under the Privacy Shield can be excluded now and in the future. There are indications that the US continues to engage in generalized and indiscriminate collection of data given that introduced discriminants and selection terms are not sufficiently precise. It is not clear if the applied discriminants are all consistent with the purpose of obtaining foreign intelligence information, which is as such a legitimate policy objective.[298] Thus it must be doubted whether the scope of all the depicted intelligence activities is strictly necessary and proportionate.

It is important to realize that, in evaluating the existing restrictions on US surveillance activities, the Commission refers to legal bases and mechanisms that were in place before the Snowden revelations and the invalidation of the Adequacy Decision I, except for PPD-28 and the USA Freedom Act. The major legal bases for foreign intelligence collection activities, Section 702 FISA and Executive Order 12333, existed before already. Despite the welcome purpose limitations introduced by PPD-28, concerns about the proportionality and necessity of data collection persist. The six purposes for which data can be collected in bulk need urgent clarification to ensure that the purposes and the scope of collection are sufficiently limited to was is necessary and proportionate. It must be noted that the USA Freedom Act prohibits bulk collection of records under Sections 402 and 501 FISA. Nonetheless, collection of data remains an option as long as it is targeted to the greatest extent possible. The

[298] The CJEU declared national security as a legitimate policy objective. See Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd*, para. 88.

remaining question is whether the strict EU principles of proportionality and necessity, in respect to legitimate interference with someone's privacy, should be dismissed by reference to filters and other technical tools to focus the collection of personal data. In my opinion, such selection terms do not provide any concrete indication on the actual scope of collection. Bulk collection remains an impermissible interference with the right to privacy due to its indiscriminate nature.[299] In sum, criterion B is not met.

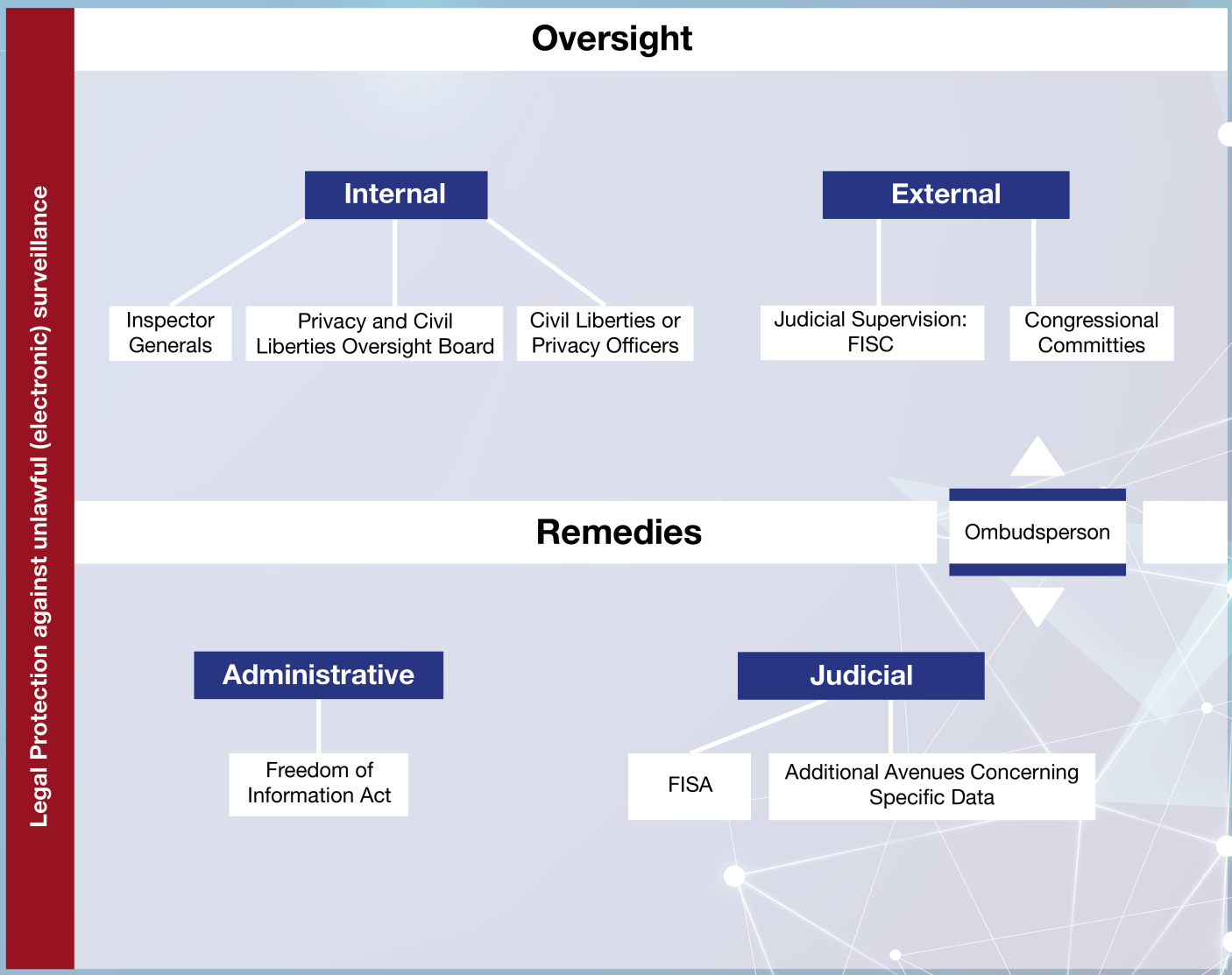
3.4. C: Effective Legal Protection

In the 'Schrems' ruling, the CJEU found that the Adequacy Decision I did not refer to the existence of effective legal protection against the interference with the fundamental rights of the persons whose data is transferred under the Privacy Shield by US national authorities when pursuing legitimate objectives including national security. The Commission's own assessment demonstrated that the US did not afford sufficient administrative and judicial means of redress for EU individuals to access and rectify the data relating to them. As a natural consequence, in the Adequacy Decision II and the Annexes, the Commission and the various US officials discuss and assess oversight mechanisms that exist in the US and are relevant for the interference by US intelligence authorities with personal data transferred from the EU. They are examined in chapter 3.4.1. They also assessed the avenues of individual redress available to EU data subjects as well as the new Ombudsperson, portrayed in chapter 3.4.2. and 3.4.3., respectively.

[299] The European Court of Human Rights confirmed this in *Zakharov v Russia*, finding that the use of surveillance powers and the level of specificity had to safeguard that interception powers were not used arbitrarily. It further reiterated that the principles of necessity and proportionality had to be complied with properly by the interception authorization by clearly identifying 'a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information'. See ECtHR *Zakharov* 47143/06 of 4 December 2015, para. 264.

Figure 6
Oversight and Legal Remedies

The Privacy Shield framework outlines oversight mechanisms in the US with regard to interference by US intelligence authorities with personal data transferred under the Privacy Shield and avenues of redress available for EU individuals.



3.4.1. Internal vs. External Oversight

The US does not have a single oversight body at federal level that oversees the activities of the US Intelligence Community in regard to privacy and data protection. Instead, the US foreign intelligence activities are subject to a multi-layer review and oversight process falling within the three branches of the State, including oversight from within the executive branch and from various Congressional Committees as well as judicial supervision by the FISC.[300]

First, intelligence activities are subject to internal oversight mechanisms within the executive branch.[301] Each Intelligence Community element has its own Inspector General, which oversees foreign intelligence activities and their compliance with the respective laws.[302] Appointed by the President, Inspector Generals are statutorily independent.[303] Moreover, they can issue reports and non-binding recommendations, which are partially made public, and have the authority to carry out audits and inspections.[304] However, Inspector Generals can withhold reports and can be required to withhold classified information from the public by Intelligence Community departments or agencies.[305] However, given that Inspector Generals are subject to oversight by Congress, essential safeguards are in place.[306] Second, various US departments and agencies with intelligence responsibilities have civil liberties or privacy officers at their disposal. Whereas their specific tasks vary, they shall generally assist with the implementation and supervision of procedures in order to ensure that affected individuals can address their concerns regarding privacy and civil liberties. The officers report to Congress periodically.[307] They receive all information from the head of their department or agency. Overall, the Commission considers the depicted internal oversight mechanisms as 'fairly robust' and sufficient.[308]

[300] Commission Decision 2000/520/EC recital 92; Annex VI, Section I, p. 77.
[301] According to Presidential Policy Directive, Signals Intelligence Activities (2014), Section 4 (a) (i) (v) policies and practices of the Intelligence Community must include 'appropriate measures to facilitate oversight over the implementation of safeguards protecting personal information', that require periodic auditing.
[302] Commission Decision 2000/520/EC, recital 97, Annex VI, Section I. (d), p. 83.
[303] Ibid.
[304] Ibid.
[305] Article 29 Working Party, WP 12 Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (2016).
[306] Commission Decision 2000/520/EC, recital 97, Annex VI, Section I. (d), p. 83.
[307] Commission Decision 2000/520/EC, recital 96, Annex VI, Section I. (d), p. 83.
[308] Commission Decision 2000/520/EC, recital 96.

Indeed, it must be acknowledged that the oversight bodies and practices are fairly detailed and are made public to a great extent.[309] Based on the provided information, the Inspector-Generals appear to be able to carry out the necessary checks effectively and are hence likely to meet the criteria for organizational independence as defined by the CJEU. The performance of the Civil Liberties and Privacy Officers is noted as well. Yet, the required level of independence, necessary to justify an interference with the fundamental rights to privacy and data protection, raises some concerns.[310]

Third, the Privacy and Civil Liberties Oversight Board (hereafter 'PCLOB') is an independent agency within the executive branch of the US government.[311] It shall ensure that counterterrorism policies are developed and implemented with a view to privacy and civil liberties. It has the power to monitor the efficacy of surveillance programs in this regard and to access classified information.[312] In fact, this supervision mechanism has proven its independent authority by disagreeing with the President on various legal issues and publishing various findings criticising the unnecessary withholding of classified documents.[313]

Fourth, next to these internal oversight mechanisms from within the executive branch, the US Congress has oversight obligations with respect to US foreign intelligence activities.[314] Based on the National Security Act, the President must ensure that the congressional intelligence committees are continuously fully informed of the intelligence activities of the US.[315] Members of these committees have access to classified information and intelligence programs.[316] Relevant Inspector Generals and Attorney Generals must inform these committees every six months about FISA electronic surveillance.[317] Yet, it is not clear whether and to what extent the committees can debate the processing of personal data of EU individuals under FISA. Moreover, the USA Freedom Act requires the US government to disclose to

[309] Article 29 Working Party, WP 12 Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (2016).
[310] Article 29 Working Party, WP 12 Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (2016).
[311] Commission Decision 2000/520/EC, recital 98, Annex VI, Section I. (d), p. 83-84.
[312] Ibid.
[313] PCLOB, Report on the Surveillance program operated pursuant of Section 702 FISA (2014).
[314] Commission Decision 2000/520/EC, recital 102.
[315] 50 U.S.C. § 3091 (a) (1).
[316] 50 U.S.C. § 3091 (d).
[317] 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

Congress and to the public the number of FISA orders and directives sought and received on an annual basis as well as the estimated number of targeted (non-) US persons by surveillance. It makes the review of every decision issued by FISC mandatory.[318] It is evident that the mandatory disclosure of the FISA orders is a necessary step into the right direction and could lead to positive developments in the long run.

Lastly, the FISA court FISC conducts external supervision, the functioning of which under Section 702 FISA was revealed and assessed in the preceding chapter.[319] A panel of five individuals supports the FISC, one of whom is appointed as *amici curiae*. The *amici curiae* shall give technical advice on legal questions and ensure that privacy considerations are mirrored in the court's assessment.[320] While his function must be acknowledged, *the amici* curiae's impact is limited as he is only consulted in important cases, which is at the discretion of the FISC.[321]

In sum, the Adequacy Decision II and Annex VI depict in detail various internal and external oversight mechanisms available under US law with regard to interference by US intelligence authorities with personal data transferred under the Privacy Shield to US organizations. On the one hand, the internal oversight mechanisms in place appear to be sufficient and effective in conducting their review; the reporting practices seem to be very detailed and usually carried out in public. Accordingly, they are relatively independent and effective in reviewing surveillance laws, as required by the CJEU in the 'Schrems' ruling. On the other hand, the external oversight schemes have some room for improvement, particularly as regards the FISC operations. As outlined in chapter 3.3, there are concerns regarding the ability of the FISC to effectively review the targeting and minimization procedures.[322] It is not clear how congressional intelligence committees can actually influence the processing of

[318] USA Freedom Act of 2015, § 602.
[319] Judicial supervision by FISC differs depending on the legal authorizations for surveillance under FISA. The legal authorizations that are most important for data transfers under the Privacy Shield are Section 501 FISA and Section 702 FISA. Surveillance authorization under the former is different from the outlined procedure under Section 702 FISA to the extent that the application to the FISC has to comprise a statement of facts demonstrating that reasonable grounds exist to believe that the tangible things sought to collect are relevant to an authorized investigation that is carried out to receive foreign intelligence information regarding non-US person or to protect against international terrorism. See. 50 U.S.C. § 1861 (b); Commission Decision 2000/520/EC, recital 108.
[320] Translated as 'friend of the court', he is not a party to a case but assists the court. Acting independently, he does not defend specific individuals involved in the case. See 50 U.S.C. § 1803 (i) and Commission Decision 2000/520/EC, recital 106.
[321] Commission Decision 2000/520/EC, recital 106.
[322] See also PCLOB, Report on the Surveillance program operated pursuant of Section 702 FISA (2014), p. 11

personal data under FISA. As a consequence, the external oversight mechanisms do not seem to be sufficiently independent and effective in reviewing surveillance laws.

3.4.2. Individual Redress with Practical Impossibility

As stressed by the CJEU, the Adequacy Decision I approving the Safe Harbour did not contain any findings regarding the existence of effective legal protection against any interference with the fundamental rights to privacy and data protection by US public authorities. Consequently, the Privacy Shield and Adequacy Decision II present in detail three avenues available under US law for EU individuals, who are concerned that their personal data was processed by the US Intelligence Community and if so, whether the limitations applicable in US law were complied with. Summarized, they relate to three areas, depending on the claim raised: a) access to information under the Freedom of Information Act (hereafter 'FOIA'), b) interference under FISA and c) unlawful, intentional access to personal data by US government officials, outlined in the following. The introduction of the Ombudsman, which provides for both oversight and individual redress by means of its composite structure, is depicted in detail in the pursuing chapter.

First, administrative remedies are available to all persons under the FOIA.[323] It shall facilitate the access to any existing federal agency records on any topic, including the personal data related to the individual in question.[324] FOIA seems to aim at addressing paragraph 95 of the 'Schrems' ruling, where the CJEU requires legal remedies to be offered to EU individuals in order for them to access their personal data. However, the Commission acknowledges in the Adequacy Decision II that FOIA

> does not provide an avenue for individual recourse against interference with personal data as such, even though it could in principle enable individuals to get access to relevant information held by national intelligence agencies. Even in this respect the possibilities appear to be limited as agencies may withhold information that falls within certain enumerated exceptions, including access to classified national security information and information concerning law enforcement investigations.[325]

Given that agencies are not required to give EU individuals access to classified information, including information on the individual, it is highly unlikely that FOIA requests are successful. However, to pass the 'essentially equivalent' test as

[323] Commission Decision 2000/520/EC, recital 114, Annex VI, Section V, p. 93.
[324] 5 U.S.C. §522; Commission Decision 2000/520/EC, recital 114, Annex VI, Section V, p. 93.
[325] Commission Decision 2000/520/EC, recital 114, p. 32.

established by the CJEU in the 'Schrems' ruling, individuals must have opportunities for access and rectification of the data relating to them.

Second, under FISA, judicial remedies are available to non-US persons; allowing EU individuals to challenge unlawful electronic surveillance in case they can establish standing.[326] FISA states that 'an aggrieved person, other than a foreign power […] who has been subject to an electronic surveillance […] shall have a cause of action against any person who committed such violation'.[327] That is, US government officials can be sued in their personal capacity for money damages.[328] EU individuals can also bring a civil cause of actions for money damages against the US government when information about them was unlawfully and wilfully used in electronic surveillance under FISA.[329] They can also challenge the legality of surveillance where the US government intends to use or disclose any obtained information from electronic surveillance in judicial or administrative proceedings.[330]

Third, EU individuals have a number of additional avenues at their disposal to seek legal recourse against US government officials for unlawful collection or use of data, including for claimed national security purposes.[331] Yet, all of these causes of action concern very specific data, types of accesses and targets and are therefore only available under specific conditions.[332]

Consequently, it must be acknowledged that various legal remedies are available for EU individuals. Nevertheless, they have a significant limit: According to the US Constitution, an individual must demonstrate that he or she has standing, which is highly difficult to prove.[333] In practice, chances of winning a claim (on personal data breach) against the US government in an US court are extremely low.[334] To be clear,

[326] However, this is highly difficult in practice, as is demonstrated below. Commission Decision 2000/520/EC, recital 112, Annex VI, Section V, p. 92.
[327] 50 U.S.C. §1810.
[328] 50 U.S.C. §1810 and Commission Decision 2000/520/EC, recital 112, Annex VI, Section V, p. 92.
[329] 18 U.S.C. §2712 and Commission Decision 2000/520/EC, recital 112, Annex VI, Section V, p. 92.
[330] 18 U.S.C. §1030 and Commission Decision 2000/520/EC, recital 112, Annex VI, Section V, p. 92.
[331] See Computer Fraud and Abuse Act (18 U.S.C. § 1030); The Electronic Communications Privacy Act (18 U.S.C. §§ 2701-2712) and The Right to Financial Privacy Act (12 U.S.C. § 3417).
[332] Such as wilful or intentional conduct, harm suffered, etc.; A more general redress possibility offers the Administrative Procedure Act (5 U.S.C. § 702), which states that 'any person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action' has the right to seek judicial review.
[333] This criterion stems from the 'case or controversy' requirement of the US Constitution. See US Constitution, Article III, Section 2, Clause 1.
[334] The available causes of action require the existence of damage (18 U.S.C. § 2712; 50 U.S.C. § 1810) or the intention of the government to use or disclose information against that person in judicial or administrative

even US persons usually have hardly any chance to invoke their rights of judicial redress due to the high standing requirements. To win, a plaintiff must prove that the US government pursued a 'wilful' and 'intentional' violation.[335]

It is particularly problematic to tie a breach to a specific government official or entity. In actual fact, given the lack of notification to individuals that are subject to surveillance, ascribing a breach to a specific government department or employee is close to impossible. The Commission acknowledges this by stating that

> even where judicial redress possibilities in principle do exist for non-U.S. persons, such as for surveillance under FISA, the available causes of action are limited and claims brought by individuals (including U.S. persons) will be declared inadmissible where they cannot show "standing", which restricts access to ordinary courts.[336]

In other words, the Commission confirms that US law, as described in the Privacy Shield, does not provide sufficient effective judicial remedies for affected EU individuals. This is contrary to the requirements by the CJEU and the European Court of Human Rights (hereafter 'ECtHR').[337] To meet the criteria under Article 25 (6) as interpreted in the 'Schrems' judgement, administrative and judicial remedies under US law must not only be available for all EU individuals but must also be effective. While various avenues exist indeed, a normally informed person would probably not know which one to pursue to invoke his or her rights. Additionally, in light of the high standing requirement, remedies available to EU individuals are not effective. A future update of the Privacy Shield should thus lower the standing requirements, which seems an impossible endeavour in practice, though.

Although this paper focuses on the interference with personal data transferred under the Privacy Shield based on national security reasons; limitations and safeguards for interference for law enforcement purposes shall be pointed out shortly. In this respect, the US Department of Justice refers in Annex VII to the Adequacy Decision II to the US Constitution, which ensures that the US government 'does not have limitless, or arbitrary power to seize private information'.[338] The fourth Amendment

---

proceedings in the US (50 U.S.C. § 1806). See *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1144 (2013); M. Gilles, 'Representational Standing: U.S. ex rel. Stevens and the Future of Public Law Litigation', 89 *California Law Review* (2001).

[335] The Privacy Act of 1974, Public Law No. 93-579, 88 Stat. 1896; 5 U.S.C. §§ 552a (g) (1) (D), (g) (4).

[336] Commission Decision 2000/520/EC, recitals 115-116.

[337] ECtHR *Zakharov* 47143/06 of 4 December 2015, §171 states that anyone who has a legitimate reason to suspect an interference of fundamental rights can go to court.

[338] Commission Decision 2000/520/EC, Annex VII, p. 101.

provides 'the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures', with the basic purpose 'to safeguard the privacy and security of individuals against arbitrary invasion by government officials'.[339] However, non-US persons located outside the US are excluded from this constitutional protection under the fourth Amendment.[340] Consequently, as reiterated by the Commission,[341] affected EU individuals are precluded from effective remedies since they would not be able to challenge warrants in courts by invoking the fourth Amendment.[342] Henceforward, it is difficult to argue that US rules limit interference with the fundamental rights of the individuals whose personal data is transferred under the Privacy Shield for law enforcement purposes and thereby ensure effective legal protection against such interference.

Overall, several judicial remedies exist under the US legal framework. However, taking note of the CJEU's judgement in the 'Schrems' case, they are not effective given that it is close to impossible to enforce rights of judicial redress available under FISA and other more specific avenues due to the high standing requirements. It is also highly difficult for EU individuals to access or rectify data relating to an individual under FOIA, given that agencies are not required to give access to classified information Since all of the listed options already existed under the Safe Harbour, the Privacy Shield's more detailed depiction does not bring about any actual change in terms of legal protection for EU individuals whose data is transferred under the Privacy Shield. Nevertheless, the Ombudsperson, described in the following chapter, illustrates an entirely new oversight and redress mechanism.

3.4.3. The Powerless Ombudsperson

Annex III to the Adequacy Decision presents a letter from Secretary of State John Kerry, which describes the commitment of the Department of State to create a new Privacy Shield Ombudsperson for submissions of inquiries about inappropriate data collection or processing by the US government.[343] This Ombudsperson shall facilitate the processing of requests from EU individuals in regard to US signals intelligence

[339] *Berger v State of New York* 388 U.S. 41 (1967) (emphasis added).
[340] Commission Decision 2000/520/EC, recital 127.
[341] Commission Implementing Decision C (2016) 4176 final, recital 127.
[342] They could only benefit indirectly from the protection of the fourth Amendment, as law enforcement authorities must seek judicial authorization to access the personal data held by US companies in some cases. See Commission Implementing Decision C (2016) 4176 final, recitals 127-128.
[343] Commission Implementing Decision C (2016) 4176 final, Annex III, p. 51-59.

activities.[344] The Secretary of State designates a Senior Coordinator as Ombudsperson[345] to 'serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States'.[346] In carrying out his investigations, the Ombudsperson will 'coordinate closely' with the ODNI, the Department of Justice and other departments involved in the US national security as well as appropriate Inspector Generals, FOIA Officers and Civil Liberties and Privacy Officers.[347] The Ombudsperson shall be independent from the Intelligence Community and must report directly to the US Secretary of State, who shall ensure that his function is executed objectively.[348]

On the one hand, the establishment of an Ombudsperson with the Privacy Shield is a very welcome introduction of an alternative oversight and redress mechanism. If executed well, the Ombudsperson has the potential to encompass a meaningful improvement for EU citizens' rights in respect to data transfer under the Privacy Shield. The Ombudsperson can be considered 'a novelty in international relations regarding signals intelligence or national security'.[349] Hence, the efforts made by the Commission and the US government to improve the legal protection of EU individuals must be acknowledged.

On the other hand, several limitations on the functioning of the Ombudsperson exist. a first concern regards the alleged independence of the Ombudsperson from national security operations. The Ombudsperson will be located in the Department of State; he will both be appointed by and report to the Secretary of State, who interacts with the national security agencies in relation to various issues on a regular basis. Given that the Department of State, the Federal Bureau of Investigation (hereafter 'FBI'), the Central Intelligence Agency (hereafter 'CIA') and the National Security Agency

[344] The Ombudsperson will also process data transferred pursuant to standard contractual clauses, binding corporate rules, respective derogations or 'possible future derogations'. See Commission Implementing Decision C (2016) 4176 final, recital 116, Annex III, Annex A, p. 52.
[345] The position will be filled by Under Secretary Catherine A. Novelli. In addition to serving in that function, she will keep her role as Senior Coordinator for International Information Technology Diplomacy, established in Presidential Policy Directive 28, Signals Intelligence Activities (2014), Section 4 (d). See Commission Implementing Decision C (2016) 4176 final, Annex III, Annex A, p. 52.
[346] Commission Implementing Decision C (2016) 4176 final, Annex III, Annex A, p. 52.
[347] Commission Implementing Decision C (2016) 4176 final, Annex III Annex A. 2. (a).
[348] Commission Implementing Decision C (2016) 4176 final, Annex III Annex A. 1.
[349] Article 29 Working Party, WP 12 Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (2016), p. 46.

(hereafter 'NSA') all belong to the same system of government,[350] potential investigations led by the Ombudsperson are likely to be pursued or strongly supported by all of them in practice. Yet, without sufficient distance from the Intelligence Community, a real independence appears highly questionable. While the Commission's adequacy assessment determined that the Ombudsperson is impartial and independent, the Ombudsperson seems to be part of the US administration in fact. This finding contradicts with Article 8 (3) of the EU Charter, which requires 'control by an independent authority' as well as with Article 47 of the same Charter, which the CJEU referred to in the 'Schrems' ruling,[351] demanding 'an effective remedy before […] an independent and impartial tribunal previously established by law'.[352]

Nevertheless, it must be acknowledged that some expertise of the US Intelligence Community is necessary for the Ombudsperson to executive his role effectively. The remaining problem that neither the Adequacy Decision II nor the Annex III address is to what extent the Ombudsperson has access to individuals' data himself and how much he relies on information provided by government officials. It is not obvious either whether he can execute investigations on his own or if he has the competence to assess if a data processing operation by the security services occurred in line with the law. Consequently, one must question whether the Ombudsperson can exercise his duties effectively. In fact, it appears that the Ombudsperson does not have any power to determine or enforce matters himself at all given that he must refer alleged violations of law to the relevant US government bodies.[353] As a consequence, his powers of redress seem to be very limited and hence, insufficient under CJEU jurisprudence.

[350] Former US President Ronald Reagan established the Intelligence Community consisting of 16 members, including but not limited to the FBI, CIA and NSA. See Executive Order 12333, United States Intelligence Activities, on 4 December 1981.
[351] C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd,* para. 95.
[352] Article 13 of the ECHR obliges Member States to ensure that 'everyone whose rights and freedoms […] are violated shall have an effective remedy before a national authority'. The ECtHR clarified in *Klass,* §56 and 67 that this does not necessarily have to be a judicial authority. Rather, the Court developed under Article 8 that redress before other authorities can be in order as a necessary safeguard to surveillance activities. Yet, the ECtHR has high expectations of other authorities to provide an effective remedy, stating that such an authority must be 'independent of the authorities carrying out the surveillance, and be vested with sufficient powers and competences to exercise an effective and continuous control'. See *Case of Klass and Others v Federal Republic of Germany,* 2 EHRR 214, September 1978, § 56 and 67.
[353] Commission Implementing Decision C (2016) 4176 final, Annex III, Annex A. 6.

Regarding the procedure, EU individuals submit their requests to the supervisory authority responsible for the oversight of national security in the relevant Member State.[354] The supervisory authorities must ensure that an individual's complaint is complete before being forwarded to the Ombudsperson.[355] There is no need to prove that the US government collected an individual's data. Once passed on, the Ombudsperson must acknowledge the receipt of a complaint and must update the national supervisory authority about the status of the request.[356] Thus, contacting the Ombudsperson is quite cumbersome as individuals as national bodies mediate the communication.

Upon completion of the request, the Ombudsperson must send an appropriate response in a timely manner, a) confirming that the complaint was properly investigated, b) that US laws, statutes, executive orders, presidential directives and agency policies have either been complied with or, in case of non-compliance, that such non-compliance has been remedied. Nevertheless, c) the Ombudsperson will neither confirm nor deny whether the individual has been the target of surveillance activities nor endorse the specific remedy that was applied.[357] Arguably, the information provided by the Ombudsperson in response to requests by EU individuals does not go beyond a standard letter. It is unspecific regardless of the facts of the case. Accordingly, the Ombudsperson neither promises a meaningful scrutiny or review nor a satisfactory remedy.

Lastly, the Ombudsperson has a very limited scope of application, as his commitments do not apply to general claims regarding the consistency of the Privacy Shield with the EU data protection requirements but only to requests relating to the compatibility of surveillance with US laws. [358] As they are not mentioned, requests related to access by law enforcement agencies appear to be excluded.

Overall, the Ombudsperson is a positive step forward. Yet, the outlined shortcomings suggest that the Ombudsperson is not capable of offering effective and essentially equivalent oversight and redress possibilities comparable to those guaranteed in the

[354] Ibid, Annex III, Annex A. 3. (a).
[355] Ibid, Annex III, Annex A. 3. (b).
[356] Ibid, Annex III, Annex A. 4. (a) and (d).
[357] Ibid, Annex III, Annex A. 4. (e).
[358] Commission Implementing Decision C (2016) 4176 final, Annex III, Annex A. (4) (g).

EU legal order.[359] He is neither sufficiently independent nor vested with adequate powers to provide impartial oversight in line with the requirements set out by the CJEU in the 'Schrems' case. In sum, criterion C is not met.

3.5. Not Yet There

This analysis has shown that the Adequacy Decision II and the Privacy Shield, consisting of the Principles II as well as commitments and representations by US officials, differ to some extent from their predecessors and thereby suggests that the Privacy Shield has potential for limited change. While the Privacy Shield offers some improvements, they are not revolutionary in nature. Only few changes in US law were made to limit the access of US authorities to data transferred under the Privacy Shield. As demonstrated, existing rules cannot limit interference for national security purposes to the extent that provided protection is essentially equivalent to that guaranteed in the EU legal order. Hence, it is rather unlikely that the Privacy Shield would be able to stand up to future legal challenges before the CJEU.

First, the CJEU determined in the 'Schrems' ruling that US law, allowing US authorities to collect and process data transferred under the Privacy Shield, must be specific, clear and accessible. As demonstrated, the Privacy Shield does not provide for clearly specified and user-friendly rules. Whereas the Adequacy Decision II and the Privacy Shield outline in much more detail the limitations on US authorities than their predecessor, the information is offered in an essentially formless way, lacking clarity and structure. Thereby, it is difficult for a reasonably informed person to anticipate what can happen to her or his data when transferred to the US. Moreover, the validity of the described legal protection mechanisms is only confirmed through commitments in various letters in the Annexes to the Adequacy Decision II. In my opinion, the legal validity of the written assurances is questionable, suggesting that hard law should replace them in order for the Privacy Shield to provide adequate and legally binding protection. Arguably, the Privacy Shield is unable to endure potential legal scrutiny under the CJEU in this form. Besides, concerns arise at the conceptual level as well. The framework lacks uniform definitions of relevant legal core terms,

[359] Council of Europe and Commissioner for Human Rights, 'Democratic and effective oversight of national security services' (2015), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770 (last visited 24 August 2016).

encompassing differing understandings of basic principles between the EU and the US so that complications down the line are to be expected. It is crucial for an effective functioning of the framework that all affected parties have a common and unambiguous understanding of obligations and rights stipulated in the Privacy Shield. Overall, various cross-references and unrelated formulations next to the general complexity of the relevant documents bring about a lack of consistency, clarity and intelligibility. There is an urgent need for harmony in structure to avoid speculation about the details of the US surveillance program in the future. Consequently, criterion A is not met.

Second, the CJEU ruled in the 'Schrems' judgement that US law permitting the US Intelligence Community to collect foreign intelligence transferred under the Privacy Shield must have a limited scope that satisfies the requirements of necessity and proportionality in regards to a legitimate objective. This analysis has demonstrated that rules in place do not sufficiently, that is, in line with the principles of necessity and proportionality, limit interferences for national security purposes with the fundamental rights to privacy and personal data. Both legal bases for signals intelligence collection, Section 702 FISA and Executive Order 12333 as well as the US Freedom Act fall short of affording adequate protection to preclude generalized and indiscriminate collection. While assuming good intentions, their targeting procedures are simply too broad to truly be effective in practice; providing a high level of protection. Using selectors to pursue individual searches is not different from typing a chosen word into the Google search engine. That is, it still searches in the entire web and provides you with hundreds of millions of results within a few seconds. Unless there is more transparency on the discriminants used in the relevant collection processes, the depicted US laws fail to prove efficient safeguards and limitations in place that are applicable to US signals intelligence activities. To this adds that the US surveillance laws and safeguards, as referred to in the written assurances, have been in place before the Snowden revelations. The only changes introduced afterwards were the Presidential Policy Directive 288 in January 2014 and the USA Freedom Act in June 2015. It can be well assumed that the CJEU was aware of these developments when delivering its judgment in the 'Schrems' case. Yet, the PPD-28 continues to explicitly permit mass collection of data as long as one of the six broad exceptions are applicable. Overall, the Privacy Shield framework

does not introduce any new mechanism that essentially limit the interference with the fundamental rights of those EU individuals whose personal data is transferred from the EU to the US. In sum, criterion B is not met.

Third, the CJEU found in the 'Schrems' ruling that US law authorizing the US Intelligence Community to obtain foreign signals intelligence transferred under the Safe Harbour lacked effective legal remedies before an independent court available for EU individuals. The legal framework also missed effective detection and supervision mechanisms. In contrast, the Privacy Shield presents a variety of internal and external oversight mechanisms that monitor the activities of the US Intelligence Community authorized under US law. The former, including Inspector Generals, civil liberties and privacy officers as well as the Privacy and Civil Liberties Oversight Board, seem efficient in executing their responsibilities. The latter, comprising the Congressional Committees and the FISC have potential for improvement and are not fully complying with the 'Schrems' criteria yet. Moreover, various individual redress avenues under US law exist, which EU individuals can use when they are concerned that US Intelligence processed their personal data. Although administrative remedies exist under FOIA, individuals have hardly any opportunities for access and rectification of their data in practice. Additionally, several judicial remedies are available under FISA, which, given the practical impossibility to prove standing, do not meet the criteria of effectiveness. In respect to surveillance pursued with a law enforcement purpose, EU individuals are deprived from Fourth Amendment Rights. Lastly, all of these mechanisms were already in place under the Safe Harbour framework already, except for the Ombudsperson, and hence, continue to fall short of meeting the CJEU criteria. While the introduction of the latter oversight mechanism is a great step forward, it must be noted that its powers and independence are too limited to ensure effective and independent oversight. Initiating a truly neutral third party supervisor would have been necessary and easy to implement.[360] Overall, as criterion C is not met.

Accordingly, none of the criteria to assess adequacy under Article 25 (6) of the DPD as interpreted by the CJEU in the 'Schrems' ruling are met.

[360] Different options exist. For instance, the EU and the US could position the Ombudsman in a different body that is not affiliated with any of the two parties. Alternatively, one could appoint an entirely different and external mediator, to be hosted in a neutral international body.

4. Moving Forward

As shown, the Privacy Shield has made slight progress in comparison with its predecessor the Safe Harbour but continues to operate with fundamental flaws that could impair European data protection and privacy standards in the long run. The foregoing analysis suggests a need to find new ways for a better coordination of transatlantic data flows in order to overcome prevalent differences between the legal frameworks at hand. In fact, the contrasting legal approaches between the EU and the US are recognized in the Privacy Shield, which seeks to 'bridg[e] the differences in [their] legal approaches, while furthering trade and economic objectives of both Europe and the United States.[361] Following this analysis, I question whether the Privacy Shield in fact bridges existing differences. Instead, I argue that the 'Schrems' judgement has shed light on the inherent contradictions of data protection regulation between the EU and the US. They are discussed shortly in order to understand whether and how future convergence can occur.

The aetiology of existing transatlantic differences is complex and is deeply rooted in fundamentally different ideological, constitutional and legislative approaches towards the notion of privacy.[362] For the sake of clarity it must be stressed that in many parts of the world the term *data protection* is usually used to designate what American professionals refer to as *privacy*[363] *protection*, implying rules and practices for the handling of personal information. While there is thus a tendency to deal with the right to data protection as an expression of the right to privacy, the distinction between the two rights in the EU Charter has more than symbolic meaning.[364] First, within the EU,

[361] Commission Implementing Decision C (2016) 4176 final, Annex I, Annex 1, p. 4.
[362] G. Greenleaf, *Privacy Laws & Business International Report* 114 (2011); I. Tourkochoriti, 36 *University of Arkansas at Little Rock Law Review* (2014).
[363] The term privacy has a variety of complex meanings and connotations, depending on distinct cultural norms. In the US, it usually refers to a citizen's 'right to be let alone' and a 'right to freedom from intrusions by the state, especially in one's own home'. In the late nineteenth century Warren & Brandeis published an article with the title 'right to be let alone', generally considered to be the most influential article in facilitating the development of a common law right to privacy. It is manifested in several privacy torts in the US today. As Justice of the US Supreme Court, Brandeis later added the right to the American jurisprudence surrounding the US fourth Amendment. Thereby, US citizens received the right to claim protection of their privacy rights against intrusions by the state. This understanding is linked to the general constitutional perception centring upon limited government power in order to allow an individual's pursuit of liberty and happiness. In contrast, the protection of privacy in much of Europe is associated with the protection of dignity and honour of individuals and a society as a whole. Thereby, pluralism, democracy and civility shall be maintained. See S. Warren, and L. Brandeis, 'The Right to Privacy', 4 *Harvard Law Review* 5 (1890); E. J. Eberle, *Dignity and Liberty. Constitutional Visions in Germany and the United States,* (Westport, Conn., London: Praeger, 2002), p. 257; J. Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty', 113 *Yale Law Journal* 6, p. 1161.
[364] Nevertheless, given that this paper drew inspiration from both American and European authors, the right to privacy and the right to data protection are used interchangeably in the following. See also J. Kokott and C.

the right to privacy is perceived as a fundamental right both at national and international level since the taking effect of the Lisbon Treaty.[365] The right to respect for privacy and family life is laid down in Article 7 of the EU Charter and in Article 8 of the ECHR. Additionally, personal data is protected as a separate right in Article 8 of the EU Charter and Article 16 TFEU and is further reinforced through case law by the CJEU.[366] These fundamental rights must be balanced in line with Article 52 (1) of the EU Charter, which provides that any limitations on the exercise of these rights may only be imposed subject to the principle of proportionality and necessity in regards to the general interests recognized by EU law.[367] In contrast, the US Constitution does not make any express reference to a right to respect for privacy.[368] To this adds that US privacy rights are often weighed against free-speech rights,[369] which are enshrined in the first Amendment to the US Constitution.[370] While the protection of freedom of expression can theoretically bolster privacy, it often restricts it in practice.[371] That is, statutes that limit information sharing due to privacy reasons are under constitutional scrutiny regarding their impact on the speech of the data processor.[372]

In light of this stark contrast between the American notion of citizen privacy and its European counterpart, different legislative approaches in developing data protection laws have developed over time. Firstly, continental Europe has embraced omnibus information privacy laws for a long time. As a single overarching framework, the DPD has encouraged the development of comprehensive and robust regulatory standards

---

Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', 3 *International Data Privacy Law* 4 (2013).

[365] The EU Charter is binding on the EU Member States since the taking effect of the Treaty of Lisbon amending the Treaty of the European Union and the Treaty Establishing the European Communities on 13 December 2007. See M. C. James, 29 *Connecticut Journal of International Law* 2 (2014).

[366] *Inter alia,* Case C-553/07, *Rijkeboer* [2009] ECR I-3889, para. 47; Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Others*, para. 53; Case C-131/12, *Google Spain and Google*, para. 53, 66 and 74.

[367] This highly critical view on data protection, requiring strict data protection controls in the EU, can be traced to the fascist and totalitarian past of Europe. See M. Weiss & K. Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield', *CRS Report* (2016).

[368] However, an assertable and substantive right to privacy is provided by different constitutional amendments (first, third, fourth, fifth, ninth, and fourteenth). See also *Griswold v. Connecticut*, 381 U.S. 479 (1965) and *Roe v. Wade*, 410 U.S. 113 (1973); In the US, the Constitution is the legal basis for all laws and is considered to be legally sacrosanct. See M. C. James, 29 *Connecticut Journal of International Law* 2 (2014).

[369] Depending on how a society defines the right to privacy and what legal meaning it ascribes the term, it can conflict with other rights like the freedom of expression or law enforcement and national security requirements. See M. C. James, 29 *Connecticut Journal of International Law* 2 (2014).

[370] US Constitution, Amendment I reads: 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances'.

[371] P. M. Schwartz, 126 *Harvard Law Review* 7 (2013).

[372] *Sorrell v. IMS Health Inc*. No. 10-779 131 S. Ct. 2653 (2011) reaffirms that Amendment I of the US Constitution can prevent certain privacy protection measures.

with a very broad scope and application.[373] Sectorial laws are merely used to enhance the specificity of regulatory norms that developed from statutory frameworks.[374] By contrast, the US regime does not have a single law addressing privacy protection but a body of laws consisting of various statutory protections at federal and state level.[375] Over time, it has narrowly regulated specific privacy issues in sensitive areas such as medical and financial records for both public and private sectors.[376] In case information neither fits into a specific category nor is it covered by any substantive information privacy regime it may not be protected at all.[377] Consequently, the transatlantic dialogue on data protection is pervaded by controversy and inherent regulatory divergence,[378] for which there is a need to identify new solutions.

The in April 2016 adopted GDPR, coming into effect in May 2018, vividly illustrates that the collision in the EU-US privacy debate about contentious areas of information policy is on-going and is unlikely to stop with the recent adoption of the Privacy Shield. In fact, existing inconsistencies in data protection regulations between the EU and the US are likely to deepen given that the GDPR is more detailed and stringent than its predecessor in many regards.[379] It comprises various elements that are not reflected in current or proposed US privacy laws. For instance, the revolutionary 'right to be forgotten'[380], allowing individuals to enforce the deletion of their personal data, is likely to conflict with the first Amendment to the US Constitution.[381] The direct expansion of the jurisdictional reach of data protection rules to companies outside the EU that seek to process EU personal data[382] also runs afoul with US privacy law, which only governs companies located in the US. Instead, US law makes companies that export personal data from the US accountable for the behaviour of their third

[373] P. M. Schwartz, 126 *Harvard Law Review* 7 (2013).
[374] For instance, Directive 95/46/EC was complemented by the e-Privacy Directive for the communications sector in 1995. See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201.
[375] M. C. James, 29 *Connecticut Journal of International Law* 2 (2014).
[376] Ibid.
[377] P. M. Schwartz, 126 *Harvard Law Review* 7 (2013).
[378] L. A. Bygrave, *Transworld Working Paper* 19 (2013).
[379] For a detailed analysis see for instance I. Tourkochoriti, 36 *University of Arkansas at Little Rock Law Review* (2014).
[380] Regulation (EU) 2016/679, Article 17.
[381] The US has to balance its privacy laws against strong constitutional protection for free expression. Op. cit.: 370-372.
[382] Regulation (EU) 2016/679, Article 3 (2).

parties functioning abroad.[383] Complicating matters, the GDPR appears to have the potential to create even deeper trenches between the US and EU data protection regimes in the long run. An US diplomat was cited as warning of a new trade war if certain rights such as the right to be forgotten would be followed through.[384] Finding a comprehensive agreement with mutual recognition of data privacy based on the GDPR will be an 'uphill struggle' and is likely to lead to a clash that could possibly delay the EU-US trade negotiations.[385] Accordingly, in the following, I elaborate on three options according to which these long-standing differences could be dealt with in the future. First, the EU should be more confident in promoting its standards; second, the US should rebuild trust by acknowledging existing gaps in its laws and thirdly, both the US and the EU should make more efforts for further rapprochement by focusing on common grounds.

4.1. Option 1: Promoting and Insisting on EU Standards

As has been outlined, the adequacy assessment procedure in the DPD has strongly influenced the development of data protection standards outside the EU,[386] so that '[s]omething reasonably described as "European standard"'[387] is developing in most parts of the world. As a consequence of stronger limitations on data exports and efficient enforcement requirements, EU standards have globally been recognized 'as the strongest standard for data privacy in an international instrument'[388]; they are the 'most ambitious, comprehensive and complex in the field'[389]. Regardless of the expected changes through the GDPR, the ideals of adequacy will continue to be at the heart of data transfer to third countries. Accordingly, it can be anticipated that relevant third countries will remain connected to the EU data protection regime so that the EU rules will continue to have influence beyond borders by default. Consequently, rather than compromising standards for the sake of compromise with

[383] C. Wolf, 43 *Washington University Journal of Law & Policy* (2014).
[384] Pinsent Masons, 'US diplomat warns of "trade war" if "right to be forgotten" proposals are followed through', *Out-Law*.com (2013), http://www.out-law.com/en/articles/2013/february/us-diplomat-warns-of-trade-war-if-right-to-be-forgotten-proposals-are-followed-through/ (last visited 14 August 2016).
[385] Andreas Geiger, 'EU Will Ramp Up Data Protection in Wake of Snowden', *The Hill' Congress Blog* (2014), http://thehill.com/blogs/congress-blog/foreign-policy/317061-eu-will-ramp-up-data-protection-in-wake-of-snowden- (last visited 26 August 2016).
[386] Ibid; P. M. Schwartz, 126 *Harvard Law Review* 7 (2013).
[387] L. A. Bygrave, 'Transatlantic Tensions on Data Privacy', *Transworld Working Paper* 19 (2013), http://pubblicazioni.iai.it/content.php?langid=2&contentid=893 (last visited 26 August 2016), p. 11.
[388] G. Greenleaf, 2 *International Data Privacy Law* 1 (2012), p. 3.
[389] L. A. Bygrave, *Transworld Working Paper* 19 (2013), p. 5.

the US,[390] I argue that the Commission should rely on its bargaining power, which it assumes thanks to the predominance of its standards in the world. I encourage the Commission to give a stronger signal by upholding its standards firmly and by relying on its bargaining power.

The strong influence of EU data protection initiatives is particularly contentious for American business interests.[391] US American scholar Bradford reiterates that global operations have adjusted to the strict EU standards, as companies find difficulties in isolating their databases.[392] Already in 2003, the US American Wall Street Journal stated that 'Europe is plowed ahead with the world's toughest set of rules [that] are increasingly shaping the way businesses operate around the globe'.[393] In fact, US federal government officials estimated that respective restrictions could annually jeopardize up to 120 billion US dollars in trade.[394] Hence, it is possible that in case the EU, one of the biggest markets in the world, blocked the US market effectively because of unrestricted surveillance laws, US companies would see their international business at detriment and hence exert pressure on the US government in order to demand a true commitments to comprehensive and high standards.[395] Consequently, in my opinion, the Commission should demonstrate to be a true and convinced promoter of its standards by insisting on the full expansion in respect to the collection and use of data from the EU. Privacy expert Greenleaf reiterates in this respect that

> Europe has no reason to retreat from its privacy standards developed over forty years. The rest of the world is moving its way, and it should not compromise fundamental standards for the sake of compromise with powerful outliers, particularly the USA and China. Respect for their domestic prerogatives should not be confused with any need to reduce fundamental aspects of global data privacy standards.[396]

---

[390] G. Greenleaf argues that the Commission accepted in the Adequacy Decision I a weaker and more fragmented standard of data protection as 'adequate' in order to maintain good trade relations between the EU and the US. Given that the Adequacy Decision I was the first decision on adequacy on a non-European country, it could be considered as setting a low benchmark for 'adequacy'. See G. Greenleaf, 'Safe Harbor's low benchmark for 'adequacy': EU sells out privacy for US$', 7(3) *Privacy Law and Policy Reporter* 45 (2000).
[391] L. A. Bygrave, *Transworld Working Paper* 19 (2013).
[392] A. Bradford, 107 *Northwestern University Law Review* 1 (2012).
[393] D. Scheer, 'Europe's New High-Tech Role: Playing Privacy Cop to the World', *Wall Street Journal* (2003), http://www.wsj.com/articles/SB106574949477122300 (last visited 13 August 2016).
[394] D. Heisenberg, *Negotiating Privacy: The European Union, The United States, and Personal Data Protection*, (Lynne Rienner Publishers, 2005).
[395] M. Schrems elaborated on this option in the European Parliament. See M. Schrems, 'Privacy Shield: Safe Harbour with teeny tiny changes' (2016), https://www.youtube.com/watch?v=EdCmpmL1UJk (last visited on 13 August 2016).
[396] G. Greenleaf, *Privacy Laws & Business International Report* 114 (2011), p. 16.

Instead, the Commission stressed in February 2016 that trust had to be restored, being the reasonable and necessary basis for working with the US in the future. It stressed that 'trust is a must [for] our digital future'.[397] Whether trust should be the sole basis for the future transatlantic relationship regarding data transfer is questionable, though. In spite of assurances by the US government that it will no longer engage in indiscriminate mass data collection,[398] one must be doubtful – from a realpolitik point of view – whether it will refrain from doing so in light of on-going terrorism in the world.[399] In fact, the Working Party 29 took note of the US government's 'tendency to collect ever more data on a massive and indiscriminate scale in light of the fight against terrorism' in April 2016.[400] Trust, which was significantly undermined in the course of the Snowden revelation,[401] implies the important willingness to cooperate and compromise – two generally very positive features. Yet, if compromise signifies a weakening of standards one might find fault with it given that the EU's fundamental rights are non-divisible and should therefore not be put on the negotiating table with trade partners.[402] As reiterated by ECJ President Lenaerts, 'it is not about judging the U.S. system' but about upholding fundamental rights that 'Europe should not be ashamed of', stressing that the rules of law were not 'not up for sale'.[403] In this respect, he raised the question: '[W]hy should Europe not be proud to contribute its requiring standards of respect of fundamental rights to the world in general? [T]he world will see what it does with it. But for us, it's essential here'.[404] Arguably, a proud Commission should exert pressure and insist on efficient restrictions and limitations on US surveillance laws in accordance with EU fundamental rights. My argument can be summarized with Vladimir Lenin's illustrious words 'Trust is a good but control is better'.[405]

---

[397] European Commission Press Release, *European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows'*, 12 July 2016, IP-16-2461.
[398] Commission Implementing Decision C (2016) 4176 final, Annexes I-VII.
[399] Since 2001, US surveillance activities have often been pursued in the name of counter-terrorism. See Commission Implementing Decision C (2016) 4176 final, Annexes VI; N.M. Richards, 'The Dangers of Surveillance', *Harvard Law Review* (2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239412 (last retrieved 23 August 2016).
[400] Article 29 Working Party, 'Statement of the Article 29 Working Party on the Opinion on the EU-U.S. Privacy Shield' (2016), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf (last visited 23 August 2016).
[401] See for instance P. Singer and I. Wallace, 'Big Bets and Black Swans 2014: Secure the Future of the Internet', *Brookings Institution Press* (2014).
[402] See European Rapid Press Release, *PRISM scandal: The data protection rights of EU citizens are non-negotiable* 14 June 2014, SPEECH-13-536.
[403] ECJ President Koen Lenaerts in V. Pop 'ECJ President On EU Integration, Public Opinion, Safe Harbor, Antitrust', *The Wall Street Journal*.
[404] Ibid.
[405] B.J. Blodgett, *Lives Entrusted: An Ethic of Trust for Ministry* (Fortress Press, Minneapoils, 2008), p. 27.

At the same time, the Commission should work on the promotion of its standards by improving its adequacy assessment procedure. In light of on-going problems to conduct coherent and harmonious adequacy assessments for all countries interested, the Commission should establish a more transparent and pro-active process for adequacy findings outside of Europe.[406] In order to benefit from the continuous desire from third countries to fulfil the adequacy requirements, the EU should speed up the pace in making and publicising adequacy assessments. It should provide more information about what constitutes adequacy and publish reasons in case access was denied so that countries are not discouraged and turn their back on the EU. This also applies to the Privacy Shield, which was negotiated in secret and then adopted quickly without a proper public debate.[407] The EU must introduce modern and structured schemes that allow the public to make comments while draft adequacy decisions are being reviewed. Likewise, it is important that adequacy decisions and related frameworks demonstrate more structural and language clarity and make the accessibility of information for data subjects easier.[408] The Privacy Shield, consisting of a complex package of documents and annexes while mixing European and American terminology and legal definitions, is a good example of how it should not be.

4.2. Option 2: Need for Reform to Regain Trust

Several US privacy advocates claim that the result of the US sectorial approach is a patchwork of laws with significant gaps, demanding the US Congress to enact comprehensive legislation for data protection.[409] Moreover, the authors of a comparative study on different approaches to privacy challenges describe the US privacy laws as historically 'incoherent', providing for legislative protection that is 'largely reactive, driven by outrage at particular, narrow practices', requesting that the right to privacy be fully entrenched into domestic American law.[410] On the contrary,

[406] G. Greenleaf, *Privacy Laws & Business International Report* 114 (2011).
[407] C. Kuner, *BNA Bloomberg Privacy and Security Law Report* (2012).
[408] Article 29 Working Party, 'Statement of the Article 29 Working Party on the Opinion on the EU-U.S. Privacy Shield' (2016).
[409] P. M. Schwartz and D. J. Solove, *102 California Law Review* 4 (2014); L. A. Bygrave, *Transworld Working Paper* 19 (2013); P.M. Schwartz and J.R. Reidenberg, *Data Privacy Law. A Study of United States Data Protection* (1996).
[410] C. Hoofnagle, 'Country Studies B.1 – United States of America' in D. Korff, (Ed.) Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments' European

some US officials claim that the sectorial US law is 'more nimble than […] the EU's "one-size-fits-all" approach' and therefore more apt to promote technological innovation.[411] To the General Counsel of the US Commerce Department, Cameron Kerry, '[t]he sum of the parts of the U.S. privacy protection is equal to or greater than the single whole of Europe'.[412] Furthermore, US scholar Wolf perceives the advantage that US privacy laws can be tailored across sectors and are thus able to provide different levels of protection according to the sensitivity and use of personal information. This flexibility would permit faster changes and responses to new threats.[413] Nevertheless, these advantages would be 'underappreciated in Europe'.[414]

While these opposing opinions will always co-exist, studies demonstrate that the world gradually embraces omnibus laws with comprehensive data protection principles similar to the European approach.[415] In his comprehensive analysis, privacy expert Greenleaf suggests that the rest of the world has embraced the EU omnibus approach rather than the sectorial US approach.[416] In fact, even countries that originally took an approach similar to the US would change course. Accordingly, he concludes that the sectorial nature of the US privacy regime would only have limited chances to shape global standards in the future.[417] According to the Center for Democracy & Technology, the US is currently one of only two developed nations next to Turkey without comprehensive privacy protection for all personal data.[418] As a consequence of this development, the question arises whether the US will continue to act as 'a solitary outlier in the field' or whether it will adapt to the rest of the world earlier or later.[419]

Thus, is it possible to identify a victor in the on-going struggle over data protection? In one sense it is. If the criterion for victory is based on which party is most successful in influencing and setting global standards in the field of data protection,

---

Commission D-G Justice, Freedom and Security (2010), p.1http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf
(last visited 2 August 2016), p. 1.
411 N. Singer, 'Data Protection Laws, an Ocean Apart', *The New York Times* (2013).
412 Ibid.
413 C. Wolf, *43 Washington University Journal of Law & Policy* (2014).
414 Ibid, p. 252.
415 See G. Greenleaf, 2 *International Data Privacy Law* 1 (2012).
416 G. Greenleaf, 2 *International Data Privacy Law* 1 (2012).
417 G. Greenleaf, 2 *International Data Privacy Law* 1 (2012).
418 Center for Democracy & Technology, 'Analysis of the Consumer Privacy Bill of Rights Act' (2015), https://cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act/ (last visited 25 August 2016).
419 L. A. Bygrave, *Transworld Working Paper* 19 (2013), p. 12.

the EU is the winner. Compared to the influence of the European model, the US has been rather passive.[420] Nevertheless, one has to acknowledge that the EU has not unilaterally imposed its regulatory vision on the world.[421] Naturally, various elements of the transatlantic data protection equation are a product of cross-fertilization of regulatory traditions, of which the Safe Harbour and the Privacy Shield, respectively, is a blatant example.[422] Political, economic and academic influence on the transatlantic dialogue has also given rise to regulatory convergence and consensus to some extent.[423]

In the meantime, the US should regain trust by taking high-level engagement, which will enable responsible data collection in the long run. The most effective response to the Snowden disclosures is more disclosure and engagement to increase the transparency about surveillance activities. In this regard, the increased transparency efforts demonstrated by US authorities must be noted.[424] The US should also strengthen its own privacy protection. Part of being transparent and forthright is to acknowledge that US privacy protection has gaps such as the selectivity of US privacy protection. For instance, the Consumer Privacy Bill of Rights unveiled by Obama in February 2015 illustrates a promising avenue to gradually build bridges by suggesting a more comprehensive privacy legislation.[425] The draft bill intends to govern the collection and dissemination of consumer data by calling for the adoption of codes of conduct that shall be legally enforceable by the FTC. By creating a set of broad principles for businesses and consumers the bill could build a foundation for trust for big data aggregators and the US Intelligence Community and improve their public perception.[426] Such developments should be estimated by Europeans, who should 'not sit like rabbits in the face of scandals' but be 'mature about data' by

[420] L. A. Bygrave, *Transworld Working Paper* 19 (2013).
[421] P. M. Schwartz, 126 *Harvard Law Review* 7 (2013).
[422] For instance, the Data Security and Breach Notification Act of 2015 was inspired by EU security breach notification rules, while the EU's new interest in BCRs was influenced by the US Sarbanes-Oxley Act. See P. M. Schwartz, 126 *Harvard Law Review* 7 (2013).
[423] L. A. Bygrave, *Transworld Working Paper* 19 (2013).
[424] See report European Data Protection Supervisor, Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision (2016), p. 2.
[425] S.1158-Consumer Privacy Protection Act of 2015 was introduced to the US Senate on 30 April 2015. The current status can be tracked at https://www.congress.gov/bill/114th-congress/senate-bill/1158.
[426] The Privacy Bill of Rights illustrates a revival of draft legislation first introduced by Obama in 2012. Then Commissioner Brill noted that 'there is always room for improvement'. Thus, he supported such *comprehensive* privacy legislation while recognizing the strength of the existing US framework. See J. Brill 'Remarks to the Mentor Group for EU-U.S., *Legal Economic Affairs 1* (2013), https://www.ftc.gov/public-statements/2013/04/remarks-mentor-group-forum-eu-us-legal-economic-affairs-brussels-belgium (last visited 25 August 2016).

recognizing positive changes.[427] Overall, long-term solutions for the transatlantic dialogue are very welcome but require the US to enact essential rights, containing the substance of the EU data protection principles, into binding federal law. Just as other non-EU countries have been assessed strictly in regards to their level of protection, the US should not be treated differently.

4.3. Option 3: Let's do this!

Transatlantic data flows between the US and the EU are the highest in the world.[428] Moreover, the US and the EU are the two largest net exporters of digital goods and services to the rest of the world.[429] Looking at these facts, one soon comprehends the practical necessity for the transatlantic data transfer to agree on a mutually satisfactory framework. The high value of a legal framework representing the biggest trading partnership in the world, particularly in an era of global and unpredictable data flows, must be recognized.[430] Thus, former Commission Vice-President Viviane Reding and former US Secretary of Commerce John Bryson stressed in a joint statement that '[b]oth parties are committed […] to create mutual recognition frameworks that protect privacy [and] the common principles at the heart of both systems'.[431] They stressed that a transatlantic data protection framework should fully reflect the shared democratic and individual rights-based values, which are expressed both in the Lisbon Treaty and the EU Charter as well as in the US Constitution.

Accordingly, next to debating the regulatory differences, the substantial common ground between EU and US data protection standards deserve some consideration. Although less comprehensive than in the EU, US legislation is 'far from being a legislative laggard in the field'.[432] In fact, the US was one of the first countries in the

[427] K. Neelie, 'Europe Needs Data Protection, Not Data Protectionism', *World Economic Forum Blog* (2014), http://forumblog.org/2013/12/europe-needs-data-protection-not-data-protectionism/ (last visited 11 August 2016).
[428] J. P. Melther, 'The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment', *Report Brookings Institute* (2014), https://www.brookings.edu/research/the-importance-of-the-internet-and-transatlantic-data-flows-for-u-s-and-eu-trade-and-investment/ (last visited 12 August 2016).
[429] J. R. Nicholson and R. Noonan, 'Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services', *Economics and Statistics Administration* (2014), http://www.esa.doc.gov/sites/default/files/digitaleconomyandcross-bordertrade.pdf (last visited 13 August 2016).
[430] European Data Protection Supervisor, Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision (2016).
[431] European Rapid Press Release, *EU-U.S. joint statement on data protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson*, 19 March 2012, MEMO-12-192.
[432] L. A. Bygrave, *Transworld Working Paper* 19 (2013), p. 3.

world to enact data protection laws.[433] Moreover, both the EU and the US adhere to a core set of broadly similar principles for the protection of personal data.[434] This early cross-jurisdictional exchange of viewpoints is also exemplified by the work of the Council of Europe (hereafter 'CoE') and the Organisation for Economic Cooperation and Development (hereafter 'OECD') whose chief data protection codes mirror each other considerably.[435]

It would also be too easy to cast transatlantic divergence along clear-cut lines, in which US privacy protection is uniformly weaker than data protection rules in Europe and to treat Europe and the US as homogeneous entities. That is to say that data protection regimes do not only differ from state to state within the US but are far from being uniform in the EU Member States either.[436] Looking back, the DPD had a long and troublesome gestation due to differing rules on data protection between EU Member States. However, as those differences threatened the realization of the internal market, the unevenness of these national regimes could be overcome to a large extent.[437] The fact that the new GDPR was adopted in March 2016 demonstrates that convergence is possible where there is the necessity of trade – and modern trade invariably involves the transfer of personal data.

If the EU and the US really seek to develop a durable trade discipline facilitating the free flow of data while upholding their data protection standards, there is a need for earnest discussion about how US law compares to EU standards. The on-going negotiations on the Transatlantic Trade and Investment Partnership[438] (hereafter

[433] Then, only Sweden and the German state of Hessen had similar laws in place (Sweden's Data Act 1973; Data Protection Act 1970). Moreover, the US legal system acknowledges a broader right to privacy both in common law (tort) and under the US Constitution. See Credit Reporting Act 1970, Public Law No. 91-508, 84 Stat. 1127 and Federal Privacy Act 1974, 5 U.S.C. § 552a; P. M. Schwartz, 126 *Harvard Law Review* 7 (2013).
[434] The famous Warren and Brandeis article on the Right to Privacy of 1974 Fair Information Practice Principles is the origin of privacy protection in US and elsewhere. Op. cit.: 287.
[435] The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980) illustrate an international consensus on the basic rules governing the protection of personal data and privacy, whereas the CoE Convention 108 was a first binding agreement that applied to all data processors applicable to members of the CoE, including the EU Member States. See Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Eur. T.S. No. 108, 28 January, 1981; L. A. Bygrave, *Transworld Working Paper* 19 (2013).
[436] For example, various Nordic EU countries such as Sweden make data on personal income publicly available through tax agencies, which can be considered unthinkable in many other EU countries. See Swedish Tax Agency, 'Taxes in Sweden', Tax Statistical Yearbook of Sweden (2015), https://www.skatteverket.se/download/18.3810a01c150939e893f29d0f/1455280476021/taxes-in-sweden-skv104-utgava16.pdf.
[437] See Directive 95/46/EC, recitals 7 and 8; Regulation (EU) 2016/679, recitals 9 and 10.
[438] TTIP aims at enhancing trade in goods and services and investment between the US and the EU. If concluded, the scale and breadth of the free trade agreement would be unprecedented, given that the economic relationship between the US and the EU is the largest in the world, accounting for ca. 40 % of world GDP and

'TTIP') could illustrate one opportunity to pour oil on troubled water.[439] The EU and the US should seek interoperability and mutual respect, taking into account the political, cultural and constitutional differences between their legal systems. In the end, the biggest risk, which can be circumvented by means of negotiation, involve unsatisfactory decisions that are based on insufficient knowledge of foreign law or political forces.[440]

At the same time, although exceptional in volume, the transatlantic dialogue on data protection will not continue to be the only important driver of standards in the field on the global scale. Other countries such as China increasingly voice their opinion and want to be heard in order to influence international standards in the field as well.[441] If China's messages runs counter the Western 'privacy paradigm', it is all the more important to find new means of coordination and convergence of EU and US regulatory policies.[442]

Eventually, the Privacy Shield is a special arrangement between the EU and the US – rather than a gift from the EU to the US or vice versa. It should be an arrangement with mutual benefits between two trading partners in the world's largest trading relationship. Neither the EU nor the US can afford a 'transatlantic data war'.[443] Unless both demonstrate genuine disposition to pursue mutual rapprochement in order to identify solutions for existing concerns, a second 'Schrems' case can be expected earlier or later.

30% of world trade. See Memorandum, European Commission, Ensuring transparency in EU-US trade talks: EU publishes negotiating positions in five more areas (2014), http://trade.ec.europa.eu/doclib/presslindex.cfm?id=1076 (last visited 24 August 2016); W. H. Cooper, 'EU-US. Economic Ties: Framework, Scope and Magnitude', *Congressional Research Service* (2013), http://www.hsdl.org/?view&did=735058 (last visited 12 August 2016).

[439] Former Commissioner for External Trade, Karel de Gucht, excluded data protection from the TTIP negotiations. While, the final scope is not yet set, on-going negotiations are likely to touch upon the facilitation of international data flows. Yet, they will exclude privacy and data protection as such. See European Commission Press Release Database, *"Stepping up a gear": Press Statement by EU Trade Commissioner Karel De Gucht following the stocktaking meeting with USTR Michael Froman on the Transatlantic Trade and Investment Partnership (TTIP),* 18 February 2014, Statement-12-12; European Parliament, 'Parliamentary questions on the Protection of personal data in the context of the TTIP negotiations' (2016), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2016-003858+0+DOC+XML+V0//EN&language=it (last visited 14 August 2016).

[440] W. H. Cooper, *Congressional Research Service* (2013).

[441] L. A. Bygrave, *Transworld Working Paper* 19 (2013).

[442] Ibid, p. 13.

[443] C. Kerry, 'Missed Connections: Talking With Europe About Data, Privacy, And Surveillance', *Center for Technology Innovation at Brookings* (2014), https://www.brookings.edu/wp-content/uploads/2016/06/Kerry_EuropeFreeTradePrivacy.pdf (last visited 25 August 2016), p. 17.

5. Conclusion

Following the invalidation of the Adequacy Decision I, approving the adequacy of the level of protection guaranteed under the EU-US Safe Harbour framework, in the 'Schrems' judgement in October 2015, the EU and the US agreed on a new framework, the EU-US Privacy Shield, which the Commission approved with the Adequacy Decision II in July 2016. This paper examines if it was right of the Commission to approve the Privacy Shield by adopting the Adequacy Decision II and whether the framework has the potential to survive a legal challenge in the future. The research question guiding this paper is 'To what extent does the Privacy Shield framework meet the criteria for adequacy under Article 25 (6) of the Data Protection Directive as interpreted by the CJEU in the 'Schrems' judgement?'. Thereby, the paper analyses the US legal order, examining whether it conforms with the standards set out by the CJEU in the 'Schrems' ruling. In other words, this paper investigates whether US law provides a level of protection that is *essentially equivalent* to that ensured in the EU legal order under the DPD and read in light of the EU Charter. This paper assesses whether effective restrictions on the access and use of personal data transferred under the Privacy Shield by US authorities are in place and whether effective oversight and redress possibilities against such interference are available for EU individuals.

Chapter two of this paper sheds light on the EU data protection rules under the DPD. Article 25 (1) therein prohibits Member States to transfer personal data from the EU to third countries that do not offer an adequate level of data protection. The Commission conducts such adequacy assessments according to a non-exhaustive list of factors in Article 25 (2) and (6) of the DPD. While the directive requires equivalence of data protection standards of third countries with the EU system, it is not very explicit about the conditions and criteria for appraising such equivalence. Yet, in the 'Schrems' judgement, the CJEU brought some clarity by interpreting the requirements stipulated in Article 25 to the extent that they require a third country to provide essentially equivalent data protection to that guaranteed in the EU legal order. However, some leeway of interpretation remains as regards the exact meaning of essential equivalence. Overall, the standard adopted by the Court can be best understood as a high degree of protection as determined by reference to the EU Charter. Next, the GDPR, entering into application in May 2018, introduces many

substantive changes to the EU data protection regime but maintains the basic structure of the adequacy assessment process. The Privacy Shield will have to be adapted accordingly. Lastly, the second chapter also reveals that EU data protection rules have been used as a blueprint for regulatory regimes across the world. The influence of European standards outside the EU can be traced back to the adequacy assessment procedure established with the DPD.

Chapter three assesses the current legal framework and the practices of the US Intelligence Community and the circumstances under which US law permits any unjustified interference to the fundamental rights to respect for private life and to data protection. In order to analyse whether such interference is justifiable in a democratic society, chapter three conducts an assessment in light of three essential guarantees based on the jurisprudence of the CJEU. This paper shows that the Privacy Shield framework differs from its predecessor to a limited extent and can hence be considered a soft update of the Safe Harbour framework. While it is a step into the right direction, the Privacy Shield does not provide sufficient limitations on access to data by US public authorities and effective safeguards to protect the rights of EU individuals in this regard. At the same time it must be acknowledged that the US and the EU have made an effort to clarify the protection of EU individuals whose data is transferred under the Privacy Shield by outlining and assessing existing US laws in more detail in both the Adequacy Decision II and the Annexes, that is, the Privacy Shield framework. However, concerns remain, particularly regarding the clarity and scope of US laws as well as remedies available for EU individuals thereunder.

First, criterion A concerning specific, clear and accessible rules, is not met. Although required by the CJEU in the ‘Schrems’ ruling, the Privacy Shield and the outlined US law lack consistency. This paper displays that the Privacy Shield is generally more detailed, particularly as regards existing limitations on access of data from the EU by US authorities. Yet, the provided information is shapeless and incoherent, lacking clarity and structure. To this adds that the legal validity of the written assurances by various US officials in the Annexes to the Adequacy Decision II is questionable. Definitions of core terms, varying essentially between the EU and the US, are used interchangeably and are likely to encompass misunderstandings, which in turn impedes an effective functioning of the Privacy Shield in practice. The complexity and

inharmonious structure of the framework and the related adequacy decision make it difficult for a reasonably informed person to anticipate what happens to her or his data when transferred under the Privacy Shield.

Second, criterion B regarding the required limited scope of US laws authorizing data collection is not met. Since the Snowden revelations on extensive US surveillance practices in June 2013, few changes in US domestic law have taken place to strengthen the privacy protection of EU individuals whose data is transferred under the Privacy Shield. While the PPD-28 and the Freedom Act have brought about some additional limitations, they fall short of precluding mass data collection one and for all, focusing on targeted and tailored access by US authorities to data instead. As evidenced in this paper, the US continues to engage in bulk collection of EU citizen data by means of the legal avenues of Section 702 FISA, Executive Order 12333 or the exceptions under PPD 28. The latter requires that collection in bulk is limited to six specific national security purposes. However, they can be interpreted in a very broad manner. Consequently, these limited changes suggest that the interferences with the fundamental rights to data protection and privacy are not necessary and proportionate in respect to the legitimate objective of national security. Accordingly, the risk of unrestrained infringements with fundamental rights continues to exist where US agencies access the personal data of EU individuals in line with the derogation provisions to the Principles II.

Third, criterion C on effective legal protection and oversight is not met either. While the CJEU determined the need for US law to provide effective legal remedies and supervision mechanisms, the schemes in place fall short of satisfying the standard of essential equivalence. Although the Privacy Shield refers to diverse internal and external oversight mechanisms for US surveillance measures, they are, in sum, not fully compliant with the ‘Schrems’ criteria. US law also offers numerous individual redress avenues available for EU data subjects who have concerns that the data related to them was processed and whether limitations applicable in US law were complied with. Unfortunately, neither the judicial nor the administrative remedies are meaningful and effective in practice, *inter alia* due to high standing requirements, restricting the access to ordinary courts. The introduction of the Ombudsperson as a composite structure of oversight and redress is a great step forward. Yet, in light of

his limited powers to ensure effective and independent oversight, he does not meet the 'Schrems' criteria either.

In sum, the answer to the research question of this paper is that the Privacy Shield does not fully meet the criteria under Article 25 (6) DPD as interpreted in the 'Schrems' ruling and hence, the Privacy Shield does not provide an 'essentially equivalent' level of protection for personal data transferred from the EU to the US under the Privacy Shield. Accordingly, it may be argued that it was wrong of the Commission to approve the Privacy Shield by adopting the Adequacy Decision II. It also appears highly unlikely that the Privacy Shield would survive a legal challenge in the future. Accordingly, the EU and the US have a long way to go and have more steps to take before the transatlantic data transfer will be adequate in practice. Just as Max Schrems argued: 'We need a system that provides real protection and not just some wording that doesn't work in practice'.[444] Otherwise, to tie in with the title of this paper, the future of transatlantic data flows will be dependent on a privacy sieve rather than a privacy shield.

Regarding the future of transatlantic data flows, chapter four unpacks the contradictions of data protection regulation between the US and the EU, shedding light on their fundamentally different approaches to privacy and data protection. Consequently, the outlined long-standing tensions are unlikely to disappear in the near future, particularly with new conflicts looming ahead for the US and the EU because of the GDPR, which adds significant new regulatory requirements. Hence, there is an urgent need to find new solutions to build bridges between both sides of the Atlantic eventually. This paper identifies three solutions to address the issue at hand. First, given the predominance of EU data protection policies in the world, it argues that the Commission should be more assertive in promoting its standards and their full expansion rather than compromising at an early stage of negotiations. Secondly, the US has to regain trust by strengthening its data privacy laws. Being trustworthy means to acknowledge its own gaps in protection. Lastly, both legislators acknowledge a need for transatlantic regulation for the processing of personal data. Hence, the EU and the US should focus on existing common grounds rather than

[444] European Parliament News, 'Sending data to the US: how to safeguard your privacy' (2016), http://www.europarl.europa.eu/news/en/news-room/20160314STO19279/Sending-data-to-the-US-how-to-safeguard-your-privacy (last visited 29 August 2016).

regulatory differences in order to foster growing convergence. Ultimately, the level of protection of the Privacy Shield will prove in its day-to-day operation. What is important is that it proves effective in practice.

Given the complexity of the Privacy Shield, this paper focuses on the limitations on the access and the use of personal data transferred under the Privacy Shield by US authorities for national security purposes only. It needs to be acknowledged that various improvements were made in respect to the content of the Principles II and the commercial aspects such as redress and monitoring mechanisms. Future research should be devoted to this part of the Privacy Shield. Moreover, a detailed analysis of potential consequences of the adoption of the GDPR for the Commission adequacy assessment and the Privacy Shield, shortly touched upon in this paper, should be discussed.

The future will show whether we are heading towards a ‘Schrems’ case 2.0. If a new lawsuit was initiated, then the CJEU should use the opportunity to fully clarify what essential equivalence means so that neither American businesses nor EU individuals have to live in uncertainty any longer.

Bibliography

1. Case Law

- *Berger v State of New York 388 U.S. 41 (1967).*
- Case C-131/12 *Google Spain and Google* [2014] CJEU, ECLI:EU:C:2014:317.
- Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd.* [2015] CJEU, ECLI:EU:C:2015:650.
- Case C-553/07, *Rijkeboer* [2009] ECR I-3889.
- *Case of Klass and Others v Federal Republic of Germany,* 2 EHRR 214, September 1978
- ECtHR *Zakharov* 47143/06 of 4 December 2015.
- *Griswold v. Connecticut*, 381 U.S. 479 (1965).
- Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Others* [2014] CJEU, ECLI:EU:C:2014:238.
- *Roe v. Wade*, 410 U.S. 113 (1973).
- *Sorrell v. IMS Health Inc*. No. 10-779 131 S. Ct. 2653 (2011).

2. Legislation

2.1. Treaties

- Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation and Protection of Criminal Offenses, 2 June 2016 ('Umbrella Agreement').
- Agreement on the European Economic Area, 1994, OJ No L 1.
- APEC Privacy Framework, December 2005, APEC#205-SO-01.2.

- Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.
- Convention for the Protection of Individuals with Regard to Automatic Processing of
  Personal Data, Eur. T.S. No. 108, 28 January 1981.
- Consolidated Version of the Treaty on European Union, 2006, O.J. C 321 E/5.
- Consolidated Version of the Treaty on the Functioning of the European Union, 2008, O.J.
  C 115/47.
- EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement [2000] OJ L296/41.
- European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

2.2. Other Official Documents

- 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.
- Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-U.S. Data Flows, COM (2013) 846 final.
- 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 (2000) OJ L 215.
- Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C (2016) 4176 final.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2002) OJ L 201.
- 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 L 281/32.
- 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 L 105.
- Executive Order 12333, United States Intelligence Activities (1981).
- Federal Trade Commission Act (1914), 15 U.S.C. §§ 41-58, as amended.
- FISA Amendments Act of 2008, Public Law No. 110–261, 122 Stat. 2438.
- See Judicial Redress Act of 2015, H.R. 1428 114th Cong. (2015-2016).

- Nat'l Sec. Agency, Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended § 3(b)(1) [hereinafter Minimization Procedures].
- National Security Act of 1947, Public Law No. 235, 61 Stat. 496.
- OECD Guidelines on the Protection of Privacy & Transborder Flows of Personal Data (1980).
- Opinion Advocate General: Opinion of Advocate Bot in Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd.* [2015] CJEU, ECLI:EU:C:2015:650.
- Presidential Policy Directive, Signals Intelligence Activities (2014).
- The Privacy Act of 1974, Public Law No. 93-579, 88 Stat. 1896.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (2016) OJ L 119.
- S.1158-Consumer Privacy Protection Act of 2015.
- United States Code (Code of Laws of the United States of America).
- US Federal Privacy Act (1974), 5 U.S.C. § 552a.
- USA Freedom Act of 2015, Public Law No. 114-23.
- USA Patriot Act of 2001, Public Law No. 107-56, 115 Stat.272.
- US Credit Reporting Act (1970), Public Law No. 91-508, 84 Stat. 1127.
- US Constitution.

3. Secondary Sources

3.1. Books

- B. J. Blodgett, *Lives Entrusted: An Ethic of Trust for Ministry* (Fortress Press, Minneapolis, 2008).
- C. Rauchegger, 'The Interplay Between the Charter and National Constitutions after *Åkerberg Fransson and Melloni*', in S. de Vries, U. Bernitz and S. Weatherill (eds.), *The EU Charter of Fundamental Rights as a Binding Instrument* (Hart 2015).
- D. Heisenberg, *Negotiating Privacy: The European Union, The United States, and Personal Data Protection* (Lynne Rienner Publishers, 2005).
- E. J. Eberle, *Dignity and Liberty. Constitutional Visions in Germany and the United State,* (Westport, Conn., Praeger, London, 2002).
- J.S. Mill, *On Liberty* (6th edition, London: Longmans, Green, Reader & Dyer, 1869).
- National Research Council, *Bulk Collection of Signals Intelligence – Technical Options* (2015).
- O. Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, Oxford, 2015).

- P.M. Schwartz and J.R. Reidenberg, *Data Privacy Law. A Study of United States Data Protection* (Michie Law, Charlottesville, 1996).

3.2. Journals

- A. Bradford, 'The Brussels Effect', 107 *Northwestern University Law Review* 1 (2012), p. 1-68.
- C. Wolf, 'Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers', 43 *Washington University Journal of Law & Policy* (2014), p. 227-257.
- D. Severson, 'American Surveillance of Non-U.S. Persons: Why New Privacy Protection Offer Only Cosmetic Change', 56 *Harvard International Law Journal* 2, p. 465-514.
- G. Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108', 2 *International Data Privacy Law* 2 (2012), p. 68-92.
- G. Greenleaf, 'Safe Harbor's low benchmark for "adequacy": EU sells out privacy for US$', 7 *Privacy Law and Policy Reporter* 3 (2000). P. 45-47.
- G. Voss, 'The Future of Transatlantic Data Flows, Privacy Shield or Bust?', 19 *Journal of Internet Law* 11 (2016), p. 9-18.
- I. Tourkochoriti, 'The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide between U.S.-E.U. in Data Privacy Protection', 36 *University of Arkansas at Little Rock Law Review* (2014), p. 161-176.
- J. Kokott and C. Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, 3 *International Data Privacy Law* 4 (2013), p. 222-228.
- J. Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty', 113 *Yale Law Journal* 6 (2004), p. 1151-1221.
- L. Bygrave, 'Privacy and Data Protection in an International Perspective', 56 *Scandinavian Studies in Law* (2010), p. 166-194.
- M. C. James, 'A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe', 29 *Connecticut Journal of International Law 2* (2014), p. 257-300.
- M. E. Gilman, 'The Class Differential in Privacy Law', 77 *Brooklyn Law Review* 4 (2012), p. 1389-1445.
- M. Gilles, 'Representational Standing: U.S. ex rel. Stevens and the Future of Public Law Litigation', 89 *California Law Review* (2001), p. 315-367.
- P. M. Schwartz, 'The E.U.-U.S. Privacy Collision: A Turn to Institutions and Procedures', 126 *Harvard Law Review* 7 (2013), p. 1966-2009.
- P. M. Schwartz and D. J. Solove, 'Reconciling Personal Information in the United States and the European Union', *102 California Law Review* 4 (2014), p. 877-913.

- P. Rees, C. Fairweather O'Donoghue and J. L. Nicholson, 'Transferring Personal Data Outside the EEA: The Least Worst Solution', 13 *Computer and Telecommunications Law Review* 66 (2007), p.66-69
- S. Warren, & L. Brandeis, 'The Right to Privacy', 4 *Harvard Law Review* 5 (1890), p. 193-220.
  S. Simitis, 'Privacy- An Endless Debate', 89 *California Law Review* 6 (2010), p. 1989-2005.

3.3. Other

- Ad hoc EU-US Working Group on Data Protection, Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection (2013).
- Andreas Geiger, 'EU Will Ramp Up Data Protection in Wake of Snowden', *The Hill Congress Blog* (2014), http://thehill.com/blogs/congress-blog/foreign-policy/317061-eu-will-ramp-up-data-protection-in-wake-of-snowden- (last visited 26 August 2016).
- Article 29 Working Party, 'Statement of the Article 29 Working Party on the Opinion on the EU-U.S. Privacy Shield' (2016), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf (last visited 23 August 2016).
- Article 29 Working Party, Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (1998), DG XV D/5025/98 WP 12.
- Article 29 Working Party, WP 12 Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (2016), 16/EN WP 238.
- Allen & Overy, 'The EU General Data Protection Regulation', *Authoritative Legal Report* (2016), http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf (last visited 13 August 2016).
- BBC News, 'EU and US clinch data-transfer deal to replace Safe Harbour' (2016), http://www.bbc.com/news/technology-35471851 (last visited 22 August 2016).
- C. Hoofnagle, 'Country Studies B.1 – United States of America' in D. Korff, (Ed.) Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments' European Commission D-G Justice, Freedom and Security (2010), http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_-challenges/final_report_country_report_B1_usa.pdf (last visited 2 August 2016).
- C. Kerry, 'Missed Connections: Talking With Europe About Data, Privacy, And Surveillance', *Center for Technology Innovation at Brookings* (2014), https://www.brookings.edu/wp-content/uploads/2016/06/Kerry_EuropeFreeTradePrivacy.pdf (last visited 25 August 2016),

- C. Kuner, ‘The European Commission’s Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law’, *BNA Bloomberg Privacy and Security Law Report* (2012), http://www.kuner.com/my-publications-and-writing/untitled/kuner-eu-regulation-article.pdf (last visited 7 July 2016).
- D. Scheer, ‘Europe's New High-Tech Role: Playing Privacy Cop to the World’, Wall Street Journal (2003), http://www.wsj.com/articles/SB106574949477122300 (last visited 13 August 2016).
- European Commission, ‘Commission decisions on the adequacy of the protection of personal data in third countries’ (n.d.), http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (last visited 6 July 2016).
- European Commission, ‘Ensuring transparency in EU-US trade talks: EU publishes negotiating positions in five more areas’, *Memorandum* (2014), http://trade.ec.europa.eu/doclib/presslindex.cfm?id=1076 (last visited 24 August 2016).
- Europa Rapid Press Release, *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*, 2 February 2016, IP/16/216.
- European Commission, ‘Data transfers outside the EU’, http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm (last visited 6 July 2016).
- European Commission Press Release, *European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows*, 12 July 2016, IP-16-2461.
- European Rapid Press Release, *PRISM scandal: The data protection rights of EU citizens are non-negotiable* 14 June 2014, SPEECH-13-536.
- European Data Protection Supervisor, Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision (2016).
- European Digital Rights, ‘Transfer of Data to Third Countries’, (n.d.), https://protectmydata.eu/topics/transfers-to-third-countries/ (last visited 11 August 2016).
- European Rapid Press Release, EU-U.S. joint statement on data protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson, Brussels, 19 March 2012, MEMO-12-192.
- European Rapid Press Release, *Viviane Reding Vice-President of the European Commission, EU Commissioner for Justice on Today's Justice Council – A Council of Progress*, 6 June 2014, SPEECH/14/431.
- European Rapid Press Release, *V. Reding Vice-President of the European Commission, EU Commissioner for Justice on the Outdoing Huxley: Forging a High Level of Data Protection for Europe in the Brave New Digital World*, 18 June 2012, SPEECH/12/464.
- European Rapid Press Release, *"Stepping up a gear": Press Statement by EU Trade Commissioner Karel De Gucht following the stocktaking meeting with*

USTR Michael Froman on the Transatlantic Trade and Investment Partnership (TTIP), 18 February 2014, Statement-12-12.

- European Parliament, 'Parliamentary questions on the Protection of personal data in the context of the TTIP negotiations' (2016), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2016-003858+0+DOC+XML+V0//EN&language=it.
- European Parliament News, 'Sending data to the US: how to safeguard your privacy' (2016), http://www.europarl.europa.eu/news/en/news-room/20160314STO19279/Sending-data-to-the-US-how-to-safeguard-your-privacy (last visited 29 August 2016).
- G. Greenleaf, 'Do not dismiss "adequacy": European data privacy standards are entrenched', *Privacy Laws & Business International Report* 114 (2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2001825 (last visited 22 August 2016), p. 16-18.
- G. Greenleaf, 'Global Tables of Data Privacy Laws and Bills', *Privacy Laws & Business International Report 133* (2015), *UNSW Law Research Paper No. 2015-28*, http://ssrn.com/abstract=2603502 (last visited 13 August 2016), p. 18-28.
- Hogan Lovells, 'Legal Analysis of the EU-U.S. Privacy Shield: An adequacy assessment by reference to the jurisprudence of the Court of Justice of the European Union', *Authoritative Legal Report* (2016), http://www.hldataprotection.com/2016/03/articles/international-eu-privacy/hogan-lovells-issues-authoritative-legal-analysis-of-the-eu-u-s-privacy-shield/ (last visited 11 August 2016).
- J. Brill 'Remarks to the Mentor Group for EU-U.S., *Legal Economic Affairs 1* (2013), https://www.ftc.gov/public-statements/2013/04/remarks-mentor-group-forum-eu-us-legal-economic-affairs-brussels-belgium (last visited 25 August 2016).
- J. P. Melther, 'The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment', *Report Brookings Institute* (2014), https://www.brookings.edu/research/the-importance-of-the-internet-and-transatlantic-data-flows-for-u-s-and-eu-trade-and-investment/ (last visited 12 August 2016).
- J.R. Nicholson and R. Noonan, 'Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services', *Economics and Statistics Administration* (2014), http://www.esa.doc.gov/sites/default/files/digitaleconomyandcross-bordertrade.pdf
- K. Neelie, 'Europe Needs Data Protection, Not Data Protectionism', *World Economic Forum Blog* (2014), http://forumblog.org/2013/12/europe-needs-data-protection-not-data-protectionism/ (last visited 11 August 2016).
- L. A. Bygrave, 'Transatlantic Tensions on Data Privacy', *Transworld Working Paper* 19 (2013), http://pubblicazioni.iai.it/content.php?langid=2&contentid=893 (last visited 24 August 2016), p. 1-21.
- M. Schrems, '"EU-US Privacy Shield": Towards a new Schrems 2.0 Case?', *European Area of Freedom Security &Justice Free Group* (2016), https://free-

group.eu/2016/04/06/eu-us-privacy-shield-towards-a-new-schrems-2-0-case/ (last visited 12 August 2016).

- M. Schrems, 'Privacy Shield: Safe Harbour with teeny tiny changes' (2016), https://www.youtube.com/watch?v=EdCmpmL1UJk (last visited 13 August 2016).
- M. Weiss & K. Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield', *CRS Report* (2016).
- NDR Kultur, 'Johannes Casper zum "Privacy Shield" (2016), http://www.ndr.de/kultur/Johannes-Caspar-zum-Privacy-Shield,journal440.html (last retrieved 19 August 2016).
- N. Singer, 'Data Protection Laws, an Ocean Apart', *The New York Times* (2013), http://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html?_r=0 (last visited 3 July 2016).
- N.M. Richards, 'The Dangers of Surveillance', *Harvard Law Review* (2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239412 (last visited 23 August 2016).
- PCLOB Report on the Surveillance program operated pursuant of Section 702 FISA (2014).
- Pinsent Masons (2013), 'US diplomat warns of "trade war" if "right to be forgotten" proposals are followed through', *Out-Law.com*, http://www.out-law.com/en/articles/2013/february/us-diplomat-warns-of-trade-war-if-right-to-be-forgotten-proposals-are-followed-through/ (last visited 14 August 2016).
- Swedish Tax Agency, 'Taxes in Sweden', Tax Statistical Yearbook of Sweden (2015), https://www.skatteverket.se/download/18.3810a01c150939e893f29d0f/1455280476021/taxes-in-sweden-skv104-utgava16.pdf (last visited 24 August 2016).
- V. Pop, 'ECJ President On EU Integration, Public Opinion, Safe Harbor, Antitrust', *The Wall Street Journal* (2015), http://blogs.wsj.com/brussels/2015/10/14/ecj-president-on-eu-integration-public-opinion-safe-harbor-antitrust/ (last visited 13 August 2016).
- W. H. Cooper, 'EU-US. Economic Ties: Framework, Scope and Magnitude', *Congressional Research Service* (2013), http://www.hsdl.org/?view&did=735058 (last visited 12 August 2016).

Annex I

Abbreviations and Definitions

Adequacy Decision I	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.
Adequacy Decision II	Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.
Article 29 Working Party	Working Party set up under Article 29 of the Data Protection Directive. It has advisory status and consists of representatives of the national data protection authorities of each EU Member State, the European Data Protection Supervisor and the European Commission.
BCR	Binding Corporate Rules
CJEU	Court of Justice of the European Union
Commission	European Commission
CoE	Council of Europe
Two Commission Communications	Two communications from the Commission to the European Parliament and the Council on 27 November 2013f, followed by 13 recommendations: - On the functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU COM (2013) 847 final - Rebuilding Trust in EU-US Data Flows COM (2013) 846 final
Data Protection Agency (DPA)	Each EU Member State must provide for one or more independent public authorities responsible for protecting personal data.

Data Protection Directive (DPD)	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.
EO 12333	The Executive Order 12333 lays down the powers and responsibilities of US intelligence agencies.
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
EDPS	The European Data Protection Supervisor is an independent EU body responsible for monitoring the application of data protection rules by EU institutions.
ECtHR	European Court of Human Rights
EEA	European Economic Area
'Essentially Equivalent'-test	Test laid down by the CJEU in the 'Schrems' judgment to assess adequacy.
EU	European Union
EU Charter	Charter of Fundamental Rights of the European Union
FBI	Federal Bureau of Investigation
FISA	Foreign Surveillance Act
FISC	Foreign Intelligence Surveillance Court
Foreign intelligence	Information relating to the capabilities, intentions, or activities of foreign governments, foreign organizations, foreign persons, or international terrorists.
FOIA	The Freedom of Information Act is a federal law authorizing the full or partial disclosure of previously unreleased information and documents controlled by the US government.
FTC	The Federal Trade Commission is responsible for the enforcement of various consumer protection laws in the US.
General Data Protection Regulation (GDPR)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of

	natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC [2016] OJ L 119.
Intelligence Activities	All activities agencies of the Intelligence Community are authorized to conduct.
MS	Member States
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OECD	Organisation for Economic Cooperation and Development
PCLOB	Privacy and Civil Liberties Board
Principles I (Safe Harbour Privacy Principles)	The seven privacy principles of the Safe Harbour framework set out in Annex I to the Adequacy Decision I.
Principles II (Privacy Shield Principles)	The seven privacy principles of the Privacy Shield framework set out in Annex II to the Adequacy Decision II.
Privacy Shield	The EU-US Privacy Shield framework was agreed by the USDC and the European Commission in 2016. Consists of 7 Annexes to the Adequacy Decision II, it is a framework for transatlantic exchange of personal data for commercial purposes between the EU and the US.
PPD-28	The Presidential Policy Directive 28 is a presidential directive with binding force for US intelligence authorities, imposing limitations on signals intelligence operations. It is of importance for EU individuals as it recognizes that non-US persons should also be treated with dignity and respect.
Safe Harbour	The Safe Harbour framework was agreed by the USDC and the European Commission in 2000, consisting of the Safe Harbour Privacy Principles and the Frequently Asked Questions in the Annex to the Adequacy Decision I.
'Schrems' case	In C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd.* [2015], the CJEU had to deal with the regulation of

	personal data transfers to a third country, in this case the US, for the first time
Signals Intelligence	Intelligence-gathering by interception of signals; two types exist: - Communication intelligence - Electronic intelligence
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
TTIP	Transatlantic Trade and Investment Partnership
Umbrella Agreement	Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses
US	United States of America
USDC	United States Department of Commerce
US Intelligence Community	The US Intelligence Community comprises the following agencies or organizations: 1. The Central Intelligence Agency (CIA); 2. The National Security Agency (NSA); 3. The Defence Intelligence Agency (DIA); 4. The offices within the Department of Defence for the collection of specialized national foreign intelligence through reconnaissance programs; 5. The Bureau of Intelligence and Research of the Department of State; 6. The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy; and 7. The staff elements of the Director of Central Intelligence.

Translations

Amici Curiae	Friend of the court
Ibidem	Same
Inter alia	Among others
Opus citatum	The Work cited

Annex II

CJEU Criteria to Determine Essential Equivalence

1) The third country must provide a *high level* of fundamental rights protection under the EU Charter, the ECHR[445] and the CJEU's case law[446] interpreting the EU Charter[447], which must be judged *strictly.*[448]
2) The protection must be *effective in practice*[449] considering *all the circumstances* surrounding a transfer of personal data to a third country.[450]
3) The Commission must *periodically review* the adequacy finding to determine whether it is yet factually and legally justified,[451] taking into account the *circumstances that have arisen after* the adequacy finding.[452]
4) A Commission adequacy decision must justify that a country can ensure an *adequate level of protection,*[453] by reference to *domestic law or international commitments*.[454]
5) There must be effective detection and *supervision mechanisms*.[455]
6) Any interference with Articles 7 and 8 of the EU Charter occurring in course of the transfer of personal data from the EU to US based organizations under the Privacy Shield must be in line with Article 52 of the same Charter. It
    - Must not be based on *conflicting third country norms* that take *primacy over EU fundamental rights*.[456]
    - Must be authorized to *pursue legitimate objectives* such as national security.[457]
    - Must be limited to what is *strictly necessary and proportionate* to the protection of national security.[458]
    - Must be governed by *clear and precise rules* on the scope and application of a measure.[459]

---

[445] The Charter of Fundamental Rights must be interpreted in line with the ECHR. See Charter of Fundamental Rights of the European Union, Article 53.
[446] E.g. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others*; Case C-131/12 *Google Spain and Google*.
[447] Case C-362/14 *Maximillian Schrems v Digital Rights Ireland Ltd,* para. 38-39 and 73 (emphasis added).
[448] Ibid, para. 78 (emphasis added).
[449] Ibid, para. 74 (emphasis added).
[450] Ibid, para. 75 (emphasis added).
[451] Ibid, para. 76 (emphasis added).
[452] Ibid, para. 77 (emphasis added).
[453] Ibid, para. 83 (emphasis added).
[454] Ibid, para. 71 (emphasis added).
[455] Ibid, para. 81 (emphasis added).
[456] Ibid, para. 85-87 (emphasis added).
[457] Ibid, para. 88 (emphasis added).
[458] Ibid, para. 90 and 92 (emphasis added).

7) Legislation is not limited to what is strictly necessary, where pubic authorities have access to personal data on a *generalised basis*.[460] Such legislation *compromises the essence of the fundamental right* to respect for private life.[461] *Exceptions* are made in the light of the objective pursued; the *purpose* must be *specific, strictly restricted* and capable of justifying the interference.[462]
8) Data subjects must have the right to pursue *effective legal remedies* before an independent court, in line with Article 47 of the EU Charter.[463]

[459] Ibid, para. 91 (emphasis added).
[460] Ibid, para. 93 (emphasis added).
[461] Ibid, para. 94 (emphasis added).
[462] Ibid, para. 93 (emphasis added).
[463] Ibid, para. 95 (emphasis added).