UiO : Faculty of Law
University of Oslo

Transatlantic data flow under the EU-U.S. Privacy Shield: An adequate protection of the fundamental right to protection of personal data?

Candidate number: 7007

Submission deadline: 1. December

Supervisor: Gentian Zyberi

Number of words: 17 988

Acknowledgements

This thesis is a result of a journey that started as a class exercise and led me to discovering my deep academic interest in data protection, internet governance and law in information society in a human rights discourse. I owe my profound gratitude to Gentian Zyberi, my supervisor, who was supporting me over the last year and gave me confidence to pursue my academic interest in this field. Thank you for all your guidance that kept me structured and focused. Your comments have been most helpful and motivating throughout the writing process. It has been an inspiring experience leading me to further my legal education.

I would like to express my wholehearted gratitude to my loving parents for their unyielding support and encouragement in my academic pursuits. I could have not done this without you!

A special thank you to my *#girlgang*, Sarah and Zoe! Thank you Sarah for giving up on sleep for me to proofread my lengthy over-complicated sentences and for you amazing moral and cookie/chocolate support. Thank you Zoe for letting me ventilate my frustrations when most needed and for boosting my confidence at the finish line!

Thank you to all my friends at the Norwegian Centre for Human Rights, with whom I spent long nights behind a computer screen and who relentlessly cheered me up!

Nina Pupalova

Oslo, 01.12.2017

Abbreviations

ADR	**Alternative Dispute Resolution**
BCRs	**Binding Corporate Rules**
CFREU	**Charter of Fundamental Rights of the European Union**
CJEU	**Court of Justice of the European Union**
CLPO	**Civil Liberties and Privacy Office**
DoC	**United States Department of Commerce**
DoJ	**United States Department of Justice**
DoT	**United States Department of Transportation**
DPA	**Data Protection Authority**
DPC	**Data Protection Commissioner**
DPD	**Data Protection Directive**
DRI	**Digital Rights Ireland**
EC	**European Commission**
ECHR	**European Convention of Human Rights**
ECtHR	**European Court of Human Rights**
EDPS	**European Data Protection Supervisor**
EO-12333	**Executive Order 12333**
EP	**European Parliament**
EU	**European Union**
FISA	**Foreign Intelligence Surveillance Act**
FISA-702	**Section 702 of the Foreign Intelligence Surveillance Act**

FISC	**Foreign Intelligence Surveillance Court**
FISCR	**Foreign Intelligence Surveillance Court Review**
FIOA	**Freedom of Information Act**
FTC	**United States Federal Trade Commission**
GCHQ	**British Government Communication Headquarters**
GDPR	**General Data Protection Regulation**
IoT	**Internet of Things**
ITA	**United States International Trade Administration**
MS	**Member States of the European Union**
NSA	**United States National Security Agency**
ODNI	**United States Office of the Director of National Intelligence**
PCLOB	**Privacy and Civil Liberties Oversight Board**
PNR	**Passenger Name Record**
PPD-28	**Presidential Privacy Directive 28**
PS	**EU-U.S. Privacy Shield**
SCCs	**Standard Contractual Clauses**
SH	**EU-U.S. Safe Harbour**
TEU	**Treaty on the European Union**
TFEU	**Treaty on the Functioning of the European Union**
US	**United States of America**
WP29	**Article 29 Working Party**

Table of contents

1 Introduction

The relationship dynamics between individuals, tech companies, and the state has taken a shifty turn thanks to the new technologies close at hand. In the post-Snowden era, we revisit the notion of privacy and try to weigh our conception of it against competing economic, security, and individuals' interests. Individual claims of liberty and autonomy are being re-defined as we increasingly rely on smart technologies, upon which global political, economic, and social life depends.

"The conversation occurring today will determine the amount of trust we can place both in the technology that surrounds us and the government that regulates it. Together we can find a better balance, end mass surveillance, and remind the government that if it really wants to know how we feel, asking is always cheaper than spying."

-Edward Snowden, December 2013[1]

1.1 Background

In this digital age, we are capable of using an unprecedented amount of data. And, the rise of big data[2] holds great potential for problem-solving and informed decision-making. For example, scientists and policymakers can greatly benefit from the analysis of big data sets. However, any collection of data related to individuals on a massive scale raises issues of the human right to privacy and protection of personal data. Data processing is a transnational activity crossing multiple jurisdictions. Hence, there has been legal plurality and varying standards of personal data protection. It remains a challenge to provide and ensure the right to data protec-

*All developments and news considered until 25.11.2017

** All websites last accessed on 29.11.2017

[1] Associated Press, 'Raw: Snowden Sends Christmas Day Message to US',(25.12.2013), <https://www.youtube.com/watch?v=8iuLLkWefxs&list=PLa4kGB8ait51i52foaVvGJ7WJBpjmWl55&index=8>

[2] Big data is a multi-interpretable term depending on the context used in, but generally signifies a major development of technology that has enabled practical implications from handling big data sets. The International Telecommunication Union defines Big Data as "a paradigm for enabling the collection, storage, management, analysis and visualization, potentially under rea time constraints, of extensive datasets with heterogeneous characteristics"; see: M Ostveen, 'Identifiability and the applicability of data protection to big data', *International Data Privacy Law* [2016] 6(4), pp.299-309

tion, which is applicable regardless of the individual's location, of the data origins or the data processing.

Individuals daily conduct multiple transactions that involve the collection and use of our personal data. A characteristic of personal data is that they relate to an identified or identifiable individual that can be described as a data subject.[3] Individuals share their personal data to in exchange for free services, but with the expectation that their personal data is securely stored. And while the internet and smart-devices have fostered development and enhanced communication across the world, they have also advanced the ability of enterprises -- and consequently our governments -- to surveil every aspect of our daily lives and movement.

The global debate on privacy rights and data protection has gained momentum in the aftermath of the Snowden revelations in 2013. The first disclosed surveillance programme, *PRISM*, which was led by the US National Security Agency (NSA), allowed access to global internet traffic and communications from major US companies operating in Europe, and thus access to personal data of millions of Europeans.[4] The Snowden leaks further revealed a bulk interception of communication data from the fibre-optic cables that connect North America with Europe (programme *TEMPORA*). This time, however, the European Parliament (EP) decided to work more vigilantly in their follow up of inquiries. Having learned a lesson from the long buried *ECHOLON*[5] inquiry, Brussels reacted by calling for a *Habeas Corpus* to protect fundamental rights in the digital age.[6] This was a much needed push for legislators to realise that relevant legal protection must catch up with the level of pervasiveness of information technology. The reformative process led to the re-invention of a regulatory framework

[3] 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, and repealing Directive 95/46/EC (GDPR) [2016] OJ 2 119/1, Art.4(1)

[4] G Gellman, L Poitras, 'U.S., British Intelligence mining data from nine U.S. Internet companies in broad secret program', *The Washington Post* (06.06.2013) <https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.e30ae3d5521c>

[5] NSA's mass surveillance programme under which interception of data from Intelsat satellite was conducted, see: EP, Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), A5-0264/2001 PAR1

[6] EP, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, A7-0139/2014, pp 49-51

for cross-border data flow between the European Union (including European Economic Area states) and the US.

The giants of the internet services sector (e.g. social media networks, cloud storage, and online retail) are mostly American enterprises collecting data on a global scale. Cross-border data flow today contributes more to the global GDP than the trade of goods. Data flows in and out of the US are estimated at 80 terabytes per minute.[7] The transatlantic data flow between Europe and North America is the largest in the world and was estimated at more than 20 000 gigabit per second in 2014.[8] Yet, legal safeguards afforded for personal data protection are not universal and are often inferior to those afforded in the European Union (EU).

There is no global privacy protection that could correlate with global data flow. The protection surrounding the actual place of data transmission and storage is, as of now, supplemented by bilateral commitments. This paper will closely examine one of them: the special framework on cross-border data flow between the EU and the US known as the EU-U.S. Privacy Shield (PS) agreement. One consideration that falls under the scope of this examination is the hastened fashion in which the PS was designed and how it should make us wary of the existing disparities in the legal protection of privacy.

1.2 Aims and purpose

The purpose of this thesis is to examine the PS agreement, as a regulatory instrument that imposes obligations on US-based companies. Its aim is to ensure an adequate level of protection to European citizens according to data protection rules and the fundamental standards for human rights under the Charter of Fundamental Rights of the European Union (CFREU) -- namely the right to protection of personal data.[9] Thus, this paper will discuss the framework and the functioning thereof in the context of human rights, EU and US legislation, and EU and US case law. To that end, it will define the normative framework of European data pro-

[7] S Lund, M James, 'Defending Digital Globalization' *Foreign Affairs* (20.04.2017) < https://www.foreignaffairs.com/articles/world/2017-04-20/defending-digital-globalization>

[8] McKinsey Global Institute, 'Digital globalization: The new era of global flows' (2016) < https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>

[9] Charter of Fundamental Rights of the European Union (CFREU) [2012] OJ C 26/391, Art.8

tection; the obligations of American government and businesses; consider existing European jurisprudence on data protection; and asses the appropriateness of PS according to official findings by the European Commission (EC) since its entry into force. Accordingly, my research question is:

"Does the Privacy Shield framework offer and adequate level of protection for personal data of European data subjects?"

In order to comprehensively address the research question, I will support it further with the following sub-questions:

- Sq1: *"Can the Privacy Shield be considered an adequate tool to regulate data-transfer in the light of CJEU's jurisprudence?"*

- Sq2: *"Has the Privacy Shield been effective in providing essentially equivalent protection thus far?"*

1.3 Theory and normative background

1.3.1 Privacy

The topic of privacy and how our understanding of it changes in the digital era is enough for a single dissertation. However, here I will only shortly discuss the importance of privacy.

While we witness a golden age of cultural exchange on the Internet, there are differences across cultures and age groups in defining what is private. It is not only social media providers who collect our personal data, but also online retail services, financial services, transportation, and many more services that should be considered when talking about the re-invention of what is private. Does it mean that privacy is becoming obsolete? It could be the case according to those believing that privacy is a phenomenon shaped by historical and economic conditions and that the protection of privacy has various forms in historical periods. Therefore, we should embrace the possibility of re-inventing society with the use of big data.[10] The trend of

[10] A Weigend, '*Data for the People: How to Make Our Post-Privacy Economy Work for You'*, (Basic Books: NewYork 2017)

the “internet of things”[11] propels a complete digital recording of our life. So, why should we bother with personal data protection?

There are multiple compelling arguments for preserving traditional privacy and its translation into protection of personal data in a digital form. Privacy enables us to function as social beings in different environments and scenarios. Social scientists believe that privacy is important for individual development and self-realisation as it releases us from the oppression of commonness.[12] It helps us build intimate relationships,[13]be unique and escape societal dictates.[14] Having a private space is inextricably linked to human dignity. While privacy furnishes a certain level of solitude, it also offers space to develop our personality.[15]

Moreover, privacy is vital for democracy. It encourages development of personal autonomy and, in turn, the moral autonomy of individual citizens and their democratic competency as well.[16] It is essential for the freedom to vote, to hold political opinion, and to associate with others without the fear of reprisals.[17] Privacy creates space for civil dialogue, counter-culture or engagement in meaningful critique, and the competition of ideas and thus fosters lively democracies.[18]

In order to maintain privacy, it is necessary to understand the problems that privacy tackles: information collection, information processing, information dissemination, and invasion.[19] Equally, personal data protection norms are designed to regulate these categories of problems. Ultimately, data protection’s objective is to ensure human dignity in an information society.

---

[11] IoT: “A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these ‘smart objects‘ over the Internet, query their state and any information associated with them, taking into account security and privacy issues.” Definition by Haller, Karnouskos and Schroth; The Internet of things in an enterprise context, *Lecture Notes in Computer Science*, [2009] 5468, pp.14-28

[12] P Freund quoted in DJ Solove, *Understanding Privacy*(Harvard University Press: London UK 2008), p.79

[13] RS Gerstein, 'Intimacy and Privacy', *Ethics*[1978] 89(1), pp.76-81

[14] A Simmel quoted in *Solove* (n.12)

[15] EJ Eberle, ‘Human dignity, privacy, and personality in German and American constitutional law’, *Utah Law Review*, [1997] Fall(4),pp.963-1056

[16] V Boehme-Neßler, ‘Privacy: a matter of democracy. Why democracy needs privacy and data protection’, *International Privacy Law*,[2016] 6(3), pp.222-229

[17] CK Boone, ‘Privacy and Community’, *Social Theory and Practice* [1983] 9(1)

[18] *Solove*(n12) p.80

[19] Id.

Data protection can further human dignity as it provides us with autonomy over the selective process of accessing and limiting one's self in the digital world.[20]

1.3.2 Protection of personal data as a human right

When defining limits for one self, one must also have sovereignty over one's own personal information and it must be equivalent in both the analogue and digital world. The human rights regime in the EU recognises the discrepancy of these worlds, while also taking protection of privacy seriously. Initially, data protection was recognised in market regulation. Now it is defined by the CFREU as a fundamental right on its own, however this has not always been the case.

In the European human rights regime, the definition of the right to privacy under the European Convention of Human Rights (ECHR)[21] has undergone evolving interpretation. The European Court of Human Rights (ECtHR) has given a jurisprudential basis for interpreting protection of personal data within the right to private life.[22] In the EU, data protection was codified in the Data Protection Directive in 1995 as an act of harmonising market regulation.[23] Afterwards, CFREU stipulated the protection of natural persons in relation to the processing of personal data as a fundamental right under Article 8.[24]

Before the CFREU entered into force, the right was recognised by the Court of Justice of the EU (CJEU) in the case of *Promusicae* in 2006.[25] Data protection was elevated to the status of

[20] *Boehme-Neßler* (n16)

[21] European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 (ECHR) [1950] ETS 5, Art.8

[22] ECtHR: Gaskin v UK, App.no.10454/83 (07.07.1989); Amann v. Switzerland, App.no.27798/95 (16.02.2000); Rotaru v. Romania, App.no.28341/95 (04.05.2000); S. and Marper v. UK, App.no.30562/04 and 30566/04 (4.12.2008)

[23] 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 (DPD) [1995] OJ L281/31

[24] CFREU was adopted with the Treaty of Nice in 2001 but was not legally binding until Lisbon Treaty entered into force on the 1.12.2009 (n.9)

[25] Case C-275/06 Promusicae v Telefonica [2008] ECLI:EU:C:2008:54, para.63

a fundamental right with the adoption of the Lisbon Treaty[26]. The Treaty on the Functioning of the European Union (TFEU) provided that everyone has the right to the protection of personal data concerning him or her.[27] Since, the CJEU has continued in interpreting the right's *ratione materiae*.

Not all legal systems give data protection the status of a fundamental right. The EU regime has set high standards despite not always being exemplary in adhering to its own principles.[28] It is not an absolute right and it must be considered in relation to its function in society according to the principle of proportionality. Nonetheless, having afforded this fundamental right to data subjects, the threshold of admissible restriction or limitations is conditioned. The CFREU stipulates that any limitation on the exercise of the rights and freedoms provided in the Charter must be provided for by law and respect the essence of those rights and freedoms.[29] Therefore, any limitation must never impact the essence of a right. The essence of fundamental rights lies on the edge of an interference scale used to assess proportionality of limitations placed on a right.

Personal data protection recognises the inviolability of a person. The fact that most data are now in a digital form means that protection of the physical person replicates into an equal protection of the digital avatar. Even though data sets with personal data are now a costly commodity, the individual's right to protection of his or her personal data is not equal to protection of property. The objective of the norm should be understood as protection of personality. Hence, certain data should never be considered as goods, such as DNA-data.[30] The final decision of what happens to personal data lies with the right holder/data subject, while democratically elected legislators can determine constitutional limits of data sovereignty.

The best way to avoid infringement of protection of personal data is to end the collection of data, but that is not plausible in a data-driven economy. Nevertheless, data protection is char-

[26] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (Lisbon Treaty) [2007] OJ C306/1

[27] Consolidated version of the Treaty on the Functioning of the European Union (TFEU) [2012] OJ C326/47, Art.16(1)

[28] Directive 2006/24 on data retention proclaimed invalid in Case C-293/12 Digital Rights Ireland Ltd. [2014] ECLI:EU:C:2014:238

[29] CFREU(n.9) Art.52(1)

[30] S Rodota, 'Data Protection as a fundamental rights', in S Gitwirth et al. (eds.) *Reinventing Data Protection?* (Springer 2009)

acterised by the principle of data minimization. This means that collection of data should be purposeful, relevant, and proportional. On the other hand, in the world of big data, no data is irrelevant and it can always be interlinked with other data to generate new information (smart data).[31] Reinventing data protection means relentless interpretation of current human and societal conditions. It is an industrious task to satisfy the adequate protection of a fundamental right to personal data.

1.3.3 Normative background of EU law in general

In order to present the legal background of data protection, it is helpful to introduce the EU law and its legislation -- the so-called EU *acquis*.[32]The law of the EU entails different forms of law in a particular hierarchical order. First, when starting at the top, the supreme source of law or primary law is the original source of law. **Primary law** consists of the founding treaties that constitute the EU. The last treaty amending the establishment of European Communities and the structure of the European Union was the Lisbon Treaty and it consists of two parts: the Treaty on the European Union (TEU)[33] and the Treaty of Functioning of the European Union (TFEU).[34] Second, the CFREU codifies fundamental rights and freedoms protected in the EU within a single document. Since solemnly declared at the Council of Nice in 2000, it was not legally binding until it entered into force together with the Lisbon Treaty in 2009 and became binding upon the EU institutions and Member States (MS).

Third, under the terms of EU law we include **secondary law**, which is the EU's original legislation that contains several forms of norms. Under Article 288 of the TFEU, the EU adopts regulations, directives, decisions, recommendations, and opinions. Regulations are directly and entirely applicable to Member States. Thus, as they enter into force, they automatically become a part of the domestic legislation for a MS. Directives are binding as to the result to be achieved. Directives leave discretion to the MS to choose the form and method by which it will implement it. MS usually have up to 24 months to transpose a Directive into their national laws. Decisions are binding upon those to whom it is addressed. They often address particu-

---

[31] *Boehme-Neßler*(n.16) p.224

[32] See <http://eur-lex.europa.eu/summary/glossary/acquis.html>

[33] Consolidated version of the Treaty on European Union (TEU) [2012] OJ C326/13

[34] TFEU(n.27)

lar MS but can also address private parties. Recommendations and opinions have no binding force and constitute soft law. They should be observed alongside other soft law instruments.[35]

Although Article 288 does not provide an exhaustive list of legislative instruments, under secondary legislation are also included international agreements between the EU and non-EU states binding upon EU and its Member States.[36] International agreements have legal effect within the scope reaching EU competencies and are directly or indirectly applicable to MS depending upon their phrasing. The rationale behind this wide range of instruments is the fact that MS's national legislators should more or less have discretion on matters in different policy fields.[37]

1.3.4 Normative background of EU data protection and transfer

The fundamental right to protection of personal data has been shaped by the interpretation of the right to private life under Article 8 of the ECHR. The CFREU itself stipulates a requirement to parallel interpretation with the rights within the ECHR.[38] While the accession of EU to the ECHR has been delayed,[39] the interpretation of fundamental rights must still be parallel to the Convention. The CFREU stipulates the right to protection of personal data separately in Article 8 from the right to private life in Article 7. While bound by the interpretation of ECHR, Union law can provide more extensive protection. By now, the CJEU rulings have given the right to protection of personal data a broader interpretation than the ECtHR.[40]

The **Data Protection Directive** (DPD) is the legal instrument that has been regulating EU data protection since 1995.[41] This Directive was shaped in the early days of the internet and did not foresee the force and pace of its expansion today. Yet the wording of the DPD was

---

[35] E.g. resolutions, declarations, action programmes and so; see *Chalmers et al.*, *European Union law* (3rd eds. Cambridge University Press: Cambridge UK 2014) p.101

[36] TFEU(n.27) Art.216(2)

[37] *Chalmers et al.*, (n.35) p.99

[38] CFREU(n.9) Art.52(3)

[39] Case Opinion 2/13 [2014] ECLI:EU:C:2014:2454

[40] E.g. "the right to be forgotten" means that a data subject has a right to request removal of links in search results on the basis of his/her personal name, in Case C-131/12 Google Spain and Google Inc. [2014] ECLI:EU:C:2014:317

[41] DPD(n.23)

simple enough to catch the issue of internet-related data processing.[42] The recognition of data protection as a fundamental right also propelled the CJEU to apply and interpret the Directive in the appropriate context of the information society.[43]

The Directive recognises the necessity of cross-border data flow in the interest of international trade and provides a legal basis for data transfer outside Europe. The protection granted to data subjects under DPD does not hinder transfers to countries outside the EU but lays down a condition of adequate level of protection in a third country that must be afforded to personal data. The level of protection by a third country must be assessed in light of all circumstances surrounding the transfer operations. Such an assessment is done by the EC.[44]

The legal framework for transferring personal data to third countries, that are non-EEA states, is based on Article 25 and 26 of the DPD. Under Article 25, any transfer of personal data that are undergoing processing or are intended for processing after transfer may take place if the third country in question ensures and adequate level of protection. When assessing adequacy of the level of protection, the Directive non-exhaustively lists issues to consider. For example: the nature of the data; the purpose and duration of the proposed processing operation(s); country of origin and country of final destination; rules of law -- both general and sectoral in force -- in the third country; and the professional rules and security measures to be complied with in that country.[45] The EC can find that a third country ensures an adequate level of protection considering necessary assessment of its domestic law and international commitments for the protection of the private lives, basic freedoms, and rights of individuals in the form of a Decision.

Since the DPD takes a form of a Directive, it disseminated diverse domestic legislations in 28 MS. To ensure effective data protection, the framework needed to undergo a review. The TFEU emphasises the fundamental right to protection of personal data and establishes a horizontal legal basis for regulation under Article 16, which provides comprehensive protection in

---

[42] DPD(id.) Art.3(1), also see: A L Bygrave, 'Data privacy law and the Internet: Policy challenges' in N Witzleb, D Lindsay, M Paterson, S Rodrick (eds.), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press: Cambridge UK 2012), pp. 259-289

[43] E.g. Case C/101/01 Bodil Lindqvist [2003] ECLI:EU:C:2003:596, Case C-465/00 Rechnungshof v Österreichischer Rundfunk [2003] ECLI:EU:C:2003:294

[44] DPD(n.23) Rec.56

[45] DPD(n.23) Art.56(2)

all EU policy areas.[46] The DPD has undergone a total legislative reformation. The result of much anticipated reform came forth in April 2016 when the EU Council adopted the new General Data Protection Regulation (GDPR).[47] This framework has been in force since May 2016, however it must be noted that is enforceable from 25th May 2018. The new GDPR, which replaces the DPD, is a regulation that is directly applicable to MS, thus it avoids any differences between national laws and aims to achieve more efficacy in practice. A harmonising regulation can improve legal consistency and clearly define legitimate expectations across the EU, both in commercial areas and public sector other than law enforcement.[48] This reform brings forward the implementation of the EU's Digital Single Market Strategy and aims to simplify data protection across the EU.

As the GDPR, like the DPD, will govern data protection in general terms and adhere to the same principles, there is much continuity. However, there are some clarifications and improvements. The most noteworthy changes relate to a stronger focus on data minimization (processing only as much as is strictly necessary)[49] and "privacy by design" (including privacy at the design stage rather than adding it later).[50]

In the following chapters, this thesis will refer to the DPD, upon which the PS agreement is based. It will also ascertain relevant novelties in the framework within the context of the GDPR. This paper emphasizes that if the PS is to be a long-term solution for transatlantic data transfer, despite the PS Adequacy Decision being based on the DPD, it would require a revision applicable to the new GDPR.

---

[46] P Hustinx, 'The reform of EU data protection: towards more effective and more consistent data protection' in N Witzleb, D Lindsay, M Paterson, S Rodrick (eds.), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press: Cambridge UK 2012), pp. 62-72

[47] 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, and repealing Directive 95/46/EC (GDPR) (Text with EEA relevance) [2016] OJ 2119/1

[48] Data protection with in the context of law enforcement is now regulated by Directive 2016/680

[49] GDPR(n.47) Rec.39; Art.5(1)(c)

[50] Id., Art.25

1.3.5 Institutional background for regulation of transatlantic data transfer

Within the EU, each MS provides an independent Data Protection Authority (DPA) that is to monitor the application of the data protection norms. They are public authorities established to protect fundamental rights and freedoms of data subjects in the context of data processing. DPAs can investigate, monitor, and ensure the application of data protection norms. They are vested with both investigative and corrective powers. Now under the GDPR, DPAs have been vested with more powers.[51] In relation to the oversight of the PS, DPAs cooperate with US companies that adhere to the framework commitments and can refer individual complaints to relevant authorities in the US.

Additionally, there is the European Data Protection Supervisor (EDPS) that works similarly to national authorities only on the EU level. It can also hear and investigate complaints, monitor the application of the GDPR, and intervene and provide expertise in front of the CJEU on interpretation of data protection. Furthermore, it cooperates with national DPAs in pursuit of better consistency in data protection practice and laws. And finally, it provides its own opinion on the PS to the EC.[52]

Representatives of all 28 national DPAs form together with the EDPS and a representative from the EC, an independent advisory body, to form the Article 29 Working Party (WP29).[53] The WP29 operates under the Article 29 of the DPD and provides advice on data protection matters and gives opinions on the level of data protection by MS and third countries. Article 29 WP is to be soon superseded by the European Data Protection Board.[54]

In the US, the US Department of Commerce (DoC) administers and monitors the application of the PS system based on its commitments made by the Secretary of Commerce. The designated enforcement agency is the Federal Trade Commission (FTC). Exceptions to the jurisdiction of the FTC are the US and foreign airline companies, with the latter being regulated by the Department of Transportation (DoT).

---

[51] DPD(n.23) Art.28, GDPR(n.47) Art.51

[52] EDPS, Opinion 4/2016 Opinion on the EU-U.S. Privacy Shield draft adequacy decision (2016) <https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf>

[53] DPD(n.23) Art.29

[54] GDPR(n.47) Art.68

1.4 Methodology

The regulatory framework for data transfer between two jurisdictions implies two legal systems, thus the research is based in both EU and US law. The legal doctrinal research uses a specific methodology in identifying relevant legislation, cases, and secondary materials. This thesis focuses on black-letter law instruments assessed through the reading of judgments, opinions, and reports.

First, this study takes an approach based in legal positivism by referring to EU *acquis* and the interpretation thereof made by the jurisprudence of the CJEU. The PS framework is based in the DPD, which provides the EC with the authority to issue adequacy decisions on the level of protection provided for in the legal systems of a third country in order to transfer personal data to that country. In this way, the difference between the levels of data protection afforded by the two different jurisdictions can be overcome. Yet the minimal, "essentially equivalent protection", must be provided in that third country for the transfer to be compliant with the EU laws of data protection interpreted in light of the CFREU. Therefore, this thesis includes recourse to legal safeguards provided in the US law to EU data subjects. As such, the research required the consultation of other relevant sources, such as federal acts of law, the US President's executive orders, and presidential policy directives.

The PS scheme is specific in its form and is composed of written assurances made by the US government and not in the manner of a binding bilateral treaty. For that reason, this thesis refers to the letters with the political promises made and makes further links to the formal norms that these letters infer. In order to explain the legal and administrative links, this paper refers to official opinions, inter-institutional communications, press releases, and staff working papers.

Second, the discussion includes a method of comparison because there are two different legislative approaches to protecting the rights of data subjects in the EU and the US, as well as the oversight and recourse mechanisms provided in each of the legal systems. The focus is placed on the discrepancies in the context of necessity and proportionality of data collection for national security and law enforcement purposes.

Third, as the PS framework includes an annual review mechanism, this paper refers to the findings of the first report from October 2017 to analyse the functioning of the system and possible disparities between the commitments of the US government and the real state of af-

fairs. Considering the results of the review, the ongoing developments of legislative reform in the US, and the upcoming judicial review of the PS, the paper intends to discuss the *de-lege ferenda* dimension of transatlantic data transfer regarding the continuation, revision or even suspension of the existing framework.

1.5 Reader's guide

This thesis is structured into six main chapters. *Chapter 1* has sought to provide a contextual, normative and institutional background to protection of privacy and personal data under the EU legal framework; aim of the research; the research question; and the methodology chosen to answer it. *Chapter 2* analysis the court case that led to invalidation of the Safe Harbour and consequently placed conditions of minimal protection to be protected in subsequent regulation of cross-border data flow. *Chapter 3* assess the PS-framework, self-certification mechanism, its core Principles and available redress mechanisms. In *Chapter 4*, the thesis assess the access and use of personal data by the US public authorities, both for national security and law enforcement purposes. *Chapter 5* addresses the first annual review of the PS and considers recent jurisprudence on data transfer that may influence future judicial review of the PS. Finally, *Chapter 6* provides brief conclusion to the main research question.

2 The road from Safe Harbour to Privacy Shield

2.1 Building the legal regime for transatlantic data transfer

In July 2000 the EC adopted the Safe Harbour Adequacy Decision recognizing the Safe Harbour Principles and FAQs issued by the DoC as providing adequate protection for the transferral of personal data from the EU to US. [55] The framework became operational later that year and American businesses initially approached the framework with reservations. However, to avoid sanctions and blocking of data flow by DPAs, companies increasingly subscribed to the system.[56]

The EU-U.S. Safe Harbour (SH) was developed to allow US organisations to transfer personal data by means of self-certification without further approvals. Businesses that self-certified must have adhered to the principles of SH and incorporate them into their privacy policies.[57] Compliance to the principles was declared to the DoC. Organisations that declared compliance, were bound by the Federal Trade Commission Act, which prohibits unfair and deceptive acts.[58] The US law applied to interpretation and issues of compliance with SH-Principles upon subscription of organisations, except those who committed themselves to co-operate with DPAs.[59]

The Commission's report in 2004 on the implementation of SH highlighted the number of self-certified organisations that publish their privacy policies incomplete or not at all.[60] And, organisations that did not have publicly available privacy policies escaped from the FTC's jurisdiction and subsequent enforcement actions. Furthermore, the DoC did not implement a monitoring mechanism or functional sanctions mechanism, rendering SH ineffective for over-

[55] 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 (notified under doc.no. **C(2000) 2441**) (Text with EEA relevance.) [2000] OJ L 215/7

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

[57] C(2000)2441(n.55)Annex I.

[58] Federal Trade Commission Act (FTC Act) 15 U.S. Code §57a

[59] SEC(2004)1323 (n.56) p.12

[60] id, p.6-7

sight of non-compliance. Nonetheless, at that time the EC deemed the SH-framework to be satisfactory.

2.2 The beginning of the end for Safe Harbour

DPA's have criticised the SH-regime and its heavy reliance on self-certification and thus self-regulation. Moreover, in Europe the industry has also voiced concerns over distortion of competition due to lack of enforcement.[61] In 2010, a German DPA issued a decision that required companies transferring data from Europe to actively check that US companies on the receiving end actually comply with SH-Principles.[62] After the turmoil following the Snowden revelations, the German DPAs voiced their concerns for the significant likelihood that infringements of the SH-Principles and violations of data subjects' rights were happening again. For example, the DPA in Bremen requested that companies transferring data to the US inform them whether and how the receiving companies in the US prevented access to personal data by the NSA.[63]

The Commission turned to the EP with a new review on functioning of the SH. By September 2013, 3246 US companies self-certified and the framework was still confronted with persisting problems of false claims of adherence to the SH-Principles, missing privacy policies on organisations' websites and consequently credibility of the scheme. Furthermore, the DoC did only limited evaluation of actual practice of organisations that sought after certification renewal. As late as March 2013 the DoC made it mandatory for SH companies to make their privacy policies readily available on their public websites. Reviewing the functioning of the framework anew showed little improvement of its deficiencies from 2004. Lastly and most notably, that same year we got to know that SH became a conduit through which NSA collected personal data from the EU.[64]

---

[61] EC, 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 in the EU, COM(2013)847, p.5

[62] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht- öffentlichen Bereich (28./29.04.2010 in Hannover, Germany)<https://www.datenschutzzentrum.de/internationaler-datenverkehr/Beschluss_28_29_04_10neu.pdf>

[63] COM (2013)847 (n.61) p.5

[64] Id., p.16

In light of the scale of inconsistencies in the functionality of the scheme and the revelations about US surveillance programmes, the EC established an *ad hoc* Working Group that came up with discomforting findings. *First*, the US law has allowed large-scale collection and processing of personal data that included data transferred from the EU.[65] The nature of the surveillance programmes conducted by US authorities was clearly beyond strict measures of necessity and proportionality for interests of national security.[66] *Second*, the safeguards to provide effective remedy were not available to individuals outside the US. This meant that European data subjects could not effectively obtain access to their data, their rectification or erasure through administrative or judicial redress mechanisms. *Finally*, companies did not systematically provide any information about possible exceptions to the SH-Principles.[67] Organisations processing personal data under the SH were bound to ensure transparency and indicate the possible application of exceptions to meet national security.[68]

To that end, the EC suggested to make SH safer. When faced with the option to revoke the entire framework, it considered opting instead for improving the framework to meet the interests of companies on both sides of the Atlantic.[69] At that time, the EU and the US were negotiating an umbrella agreement on transfers of personal data in the context of police and judicial cooperation in criminal matters. The EC attempted to clarify in these negotiations that European personal data should be accessed through "formal channels of cooperation".[70] The EP took a different view and called for immediate suspension of the SH Adequacy Decision until the umbrella negotiations were concluded.[71] Before the EC made any tangible progress in the talks with the US, the CJEU struck down the Safe Harbour scheme in its entirety.

[65] Id., p.17

[66] Adherence to the Principles may be limited to the extent necessary to meet national security, public interest, or law enforcement requirements, see C(2000) 2441 (n.55)Annex I.

[67] COM(2013)847 (n.61) p.17

[68] C(2000)2441(n.55)Annex I.

[69] EC, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Rebuilding Trust in EU-US Data Flow, COM(2013) 846final

[70] Id., e.g. Terrorist Finance Tracking Program Agreement and Passenger Name Records Agreement

[71] A7-0139/2014 (n.6)para.39

2.3 The Schrems case: a not so safe Safe Harbour

It began with a case initiated by a young Austrian citizen and lawyer, Maximilian Schrems, which led to the invalidation of the SH Adequacy Decision and to the subsequent Privacy Shield. His initial petition, addressed to the Irish Data Protection Commissioner (DPC), was based on the transfer of his personal data as a Facebook subscriber from Facebook Ireland, a subsidiary of Facebook Inc. His and other Europeans' personal data collected by Facebook Ireland were being transferred to its parent company servers in California under the SH for further processing. [72]

Schrems' complaint was based on the inadequate data protection offered by the US. In the light of the Snowden revelations he pointed out that there were serious grounds to suspect that his personal data was made available to the NSA. The US law did not sufficiently protect EU data from practices of the US Intelligence Community. Yet, the Irish DPC found Schrems' complaint unfounded, since there was no evidence of his data being accessed ("pulled") by the NSA. The Irish DPC in its dismissal of the complaint referred to the Commission's SH Adequacy Decision in which the US was deemed safe for providing an adequate level of protection under the SH scheme as formally required under the DPD.[73]

Thereafter, Mr. Schrems appealed to the Irish High Court, which addressed the matter of conducting surveillance in the public interest. The Court agreed that interception of data through intelligence gathering programmes like PRISM constitute a "significant overreach" of the US governmental agencies.[74] Therefore, the Irish Commissioner was responsible for investigating the complaint and suspension of data transfer to the US.

Because this case concerns implementation of EU law, the High Court looked into the SH Adequacy Decision and said it did not meet the standards set out by Articles 7 and 8 of the CFREU referring to the CJEU's decision in *Digital Rights Ireland and Others*[75]. The oversight of intelligence services such as the NSA is conducted *ex parte* and in a secret procedure. This leaves individuals with no effective right to remedy for interference with their fundamen-

[72] Case C–362/14 Maximilian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650

[73] Id., para.29

[74] C-362/14 (n.72) para.30

[75] C-293/12 (n.28)

tal rights.[76] The inviolability of the right to private life and the right to protection of personal data precedes an adequacy decision.

According to the Advocate General, Yves Bot, a Commission's decision of adequacy cannot prevent a national DPA from investigating a complaint. Such a decision cannot eliminate or reduce powers of a DPA under the DPD and should be considered invalid.[77] Indeed, the findings of the Irish High Court and the Commission showed that the law and practice of the US have allowed for mass collection of personal data of EU citizens without possibility to seek an effective remedy. The access of the US intelligence services constituted interference with the right to respect personal life, the right to protection of personal data, and the right to an effective remedy.[78]

The CJEU did not divert from the General Advocate's opinion and was consistent with its previous recent judgments on EU data privacy law.[79] The Court drew a hard line insomuch as the protection of personal data must be interpreted in the light of the fundamental rights guaranteed by the Charter. Specifically, the DPD stipulates the protection of the fundamental right to privacy with respect to the processing of personal data.[80] The Court emphasized that the protection must be both effective and complete.[81]

First, the Court looked at the competencies of national DPA's when assessing adequacy of the protection afforded by a third country. According to the Commission, national investigation should not jeopardise the Commission's power to renegotiate terms of such decision. However, the Court reaffirmed the role of DPA's as the guardians of fundamental rights and freedoms in the context of data processing.[82] Hence, the national authorities should be independent and free from any restraints imposed by a Commission's decision. In order to ensure a

[76] C-362/14 (n.73) para.31

[77] Case C–362/14 Maximilian Schrems v Data Protection Commissioner, Opinion of Advocate General Bot [2015] ECLI:EU:C:2015:627

[78] Id.

[79] C-293/12(n.28); C-131/12(n.39); Case C-212/13 *Ryneš* [2014] ECLI:EU:C:2014:2428; Case C-230/14 *Weltimmo* [2015] ECLI:EU:C:2015:639

[80] DPD (n.23)Art.1(1), Rec.(2) and (10)

[81] C-362/14 (n.72)para.39

[82] Case C-288/12 Commission v Hungary [2014]ECLI:EU:C:2014:237, para.51; also in Case C-518/07 Commission v Federal Republic of Germany [2010]ECLI:EU:C:2010:125

process of check and balances, investigatory powers remain in the hands of a DPA when a complaint raises the question of adequacy.[83]

Thereafter, the Court examined the SH Adequacy Decision and considered two issues. The first was the necessity of a continuous adequate level of protection in a third country. According to Article 25(1) of the DPD the protection afforded by a third state must be adequate and according to Article 25(6) the level of protection must be ensured. The Court followed Advocate General's opinion and interpreted Article 25 as intending to ensure that a high level of protection continues when personal data is transferred to a third country.[84] The Court observed that "adequate protection" does not mean the same or an identical level as under the EU law. However, the protection must be "essentially equivalent" to the one guaranteed within the EU by virtue of the DPD read in light of the Charter.[85] In its decision, the CJEU did not elaborate how high the level of protection must be, although it required the protection granted to prove to be "effective in practice"[86].

The second issue was that the EC ought to have conducted periodical checks of assessment in order to guarantee justified adequacy and ought to have examined new evidence raising doubt of the de facto protection afforded in the US. Nonetheless, in 2002[87] and 2004[88] the Commission released working papers on the implementation of SH that pointed to deficiencies and weaknesses of its effective enforcement. Yet, it deferred to review the Decision and relied on resolving the flaws by working with US institutions to improve the enforcement of the SH-Principles.[89] In the aftermath of the Snowden revelations, the Commission itself admitted that the processing and transferral of data to the US was incompatible with measures of strict necessity and proportionality for protection of national security, while the data subjects had no

---

[83] F Coudert, 'Schrems v. Data Protection Commissioner: A Slap on the wrist for the Commission and New Powers for Data Protection Authorities' *European Law Blog* (15.10.2015)<https://europeanlawblog.eu/2015/10/15/schrems-vs-data-protection-commissioner-a-slap-on-the-wrist-for-the-commission-and-new-powers-for-data-protection-authorities/>

[84] C-362/14 (n.72)para.72

[85] Id.,para.73

[86] Id.

[87] EC, COMMISSION STAFF WORKING PAPER The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC(2002) 196

[88] SEC (2004)1323 (n.55)

[89] *Coudert*(n.83)

means of redress.[90] As the Court references the Commission's Communication from 2013, it reiterates the Commission's reduced discretion to decide on a third country's adequacy of protection and that its decisions are subject to judicial review.[91]

The Court looked at the Principles stemming from Article 25 of the DPD and said that requirements set out by the provision must be read in a strict manner. Yet the SH allowed exceptions to derogate from these SH-Principles.[92] The CJEU made an analogy from the *Digital Rights Ireland* case in the context of the legitimacy of surveillance measures. It considered legislation permitting the public authorities to have access on a general basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect private life, as guaranteed by Article 7 of the CFREU.[93] Making personal data available to the government authorities automatically triggers Article 8 of the CFREU and there is no need to provide evidence that certain persons' data has been "pulled".

Similarly, legislation that fails to afford effective remedy to individuals in order to rectify or erase their personal data is interfering with the essence of the fundamental right to an effective remedy, as guaranteed in Article 47 of the CFREU.[94] On the basis of the Court's consideration, it annulled Article 1 and 3(1) of the Decision and because these articles are principal to the Decision it was found null and void in its entirety.[95]

Notably, the Court's assessment of interference found a breach of the essence of rights on the scale of proportionality. The SH's successor will now have to pass the "*Schrems test*". This means that new framework will have to provide for an *essentially equivalent protection* by means of oversight and recourse mechanisms available to the European data subjects.

[90] COM(2013) 847(n.61), and C-362/14(n.72) para.90

[91] C-362/14 (n.72)para.78; and by analogy C-293/12 (n.28)para.47

[92] C(2000)2441(n.55)

[93] C-362/14 (n.72)para.94

[94] Id.,para.95

[95] Id.,para.107

2.4 What came next after Safe Harbour fell

After the *Schrems* ruling, the EC immediately announced negotiations with the US government to make a new arrangement for transatlantic data flow.[96] Although the Court invalidated the SH scheme, it did not exclude future self-certification schemes as long as there are effective detection and supervision mechanisms that enable identification and sanctioning of non-compliance with the data protection rules.[97] The WP29 swiftly reacted to recommend alternative solutions for the interim period and set out a deadline for the EC to draft an agreement for a new framework agreement. Otherwise, it would lead the DPAs in taking coordinated enforcement action.[98]

Because there was no decision on the US having an adequate level of protection, the alternative legal regime stepped in. According to Article 26 of the DPD, if there is no decision on adequacy that is based on an overall assessment of a third country then data transfer can be based in contractual solutions. The contractual solution, however, must include essential elements of protection. In this manner, the data controller adduces adequate safeguards with respect to protection of the privacy and fundamental rights of individuals. These safeguards may result from appropriate contractual clauses.[99]

To facilitate data transfer, the EC approved four sets of Standard Contractual Clauses (SCCs). Each one stipulates obligations of data exporters and importers and Binding Corporate Rules (BCRs) for transfer within a corporate group. When relying on contracts, it is the responsibility of a data exporter under the supervision of a respective national DPA to provide that the conditions for relying on SCCs or BCRs are implemented.[100]

After two years of mutual negotiations, the EU and the US agreed on new safeguards to achieve a high level of protection of the fundamental rights in Europe and ensure legal certainty for businesses. In early February 2016, a final political agreement was reached on the EU-U.S. Privacy Shield framework. The new legal regime, along with the data protection

[96] EC, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), COM(2015) 566final

[97] Id.,p.14

[98] Id.

[99] DPD(n.23) Art.26(2)

[100] COM(2015) 566final (n.96) p.14

reform reflected in the GDPR, aim to restore the trust of Europeans in the digital economy. The Commission presented it as an improvement that incorporates its previous recommendations to improve Safe Harbour[101]and a response to the *Schrems* judgement.

3 Privacy Shield: restoring transatlantic data flow

The EU-U.S. Privacy Shield (PS) is a self-certification scheme, through which US companies commit to adhere to a set of privacy principles issued by the DoC. The protection applies to EU data subjects whose personal data have been transferred from an EU organisation to self-certified organisation in the US.[102]

The whole framework is found in the PS package, which is a collection of materials that are the results of the negotiations between the DoC and the EC. These make up the basis upon which the EC found its PS Adequacy Decision.[103] The PS package comprises assurance letters signed by the heads of relevant US authorities that are addressed to the EU Justice Commissioner. The PS-Principles come attached with a letter from the International Trade Administration (ITA) of the DoC, which administers the scheme. The ITA letter describes the commitments of the DoC that will ensure efficacy in the operationalization of the PS. The PS-package includes further written assurances from: the FTC describing its enforcement of the PS; the DoT describing its enforcement of the PS; the Office of the Director of National Intelligence (ODNI) regarding safeguards and limitations applicable to national security authorities; the Department of State and accompanying memorandum describing the State Department's commitment to establish a new Privacy Shield Ombudsperson for submission of inquiries regarding US signals intelligence practices; and the Department of Justice (DoJ) regarding safeguards and limitations on government access for law enforcement and public interest purposes.

The basis of the PS framework lies in the written commitments of the US administration and the Commission’s implementing decision on adequacy of the US provided by the Privacy

[101] COM (2013)847 (n.61)

[102] Commission Implementing Decision (EU) 2016/1250 of 12 July 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 (notified under document **C(2016) 4176**) (Text with EEA relevance) [2016] OJ L 207/1, Rec.(16)

[103] Id.

Shield.[104] After having consulted the EDPS, the EC adopted the Adequacy Decision that entered into force by 12 July 2016. The Adequacy Decision was found on the basis of information about the US legal order, including the representations and commitments of the US government. It concluded that the PS meets the standards of Article 25 in the DPD, interpreted in light of the CFREU and the conclusions of the *Schrems* judgment.[105]

3.1 Self-certification and commercial oversight

Self-certification means that US companies can join PS on a voluntary basis. By now, more than 2550 US companies have self-certified under the PS framework.[106]Companies are bound to the framework once they publicly commit to comply with it. The commitment to comply with PS Principles is enforceable under US law by the relevant enforcement authority, which is either the FTC or the DoT. PS organisations must re-certify on an annual basis in order to enjoy continuous benefits of the PS-framework.

A data transfer framework based on self-certification scheme is not contrary to the DPD as long as the third country in question ensures an adequate level of protection.[107] A system of self-certification can be reliable, yet it must fulfil requirements of effective detection of non-compliance, supervision, and sanction mechanisms. To that end, any non-compliance should be detected and any infringement of the rules punished.[108] Therefore, the PS framework must be utilised not merely for the initial checking of the boxes as required by the certification submission process but also for the full implementation of the PS-Principles in organisations' privacy policies.

Once an organisation is placed on the PS-List of self-certified companies, it can receive personal data transferred from the EU. The list is administered by the DoC, which processes the submissions of companies.[109] A self-certification submission must contain information on the organisation, a description of its activities with respect to personal data from the EU, and most

[104] See **Annex I.**
[105] Id.,Rec.(140)(141)
[106] See: <https://www.privacyshield.gov/list>
[107] DPD(n.23) Art.25(6)
[108] C-362/14(n.72) para.81
[109] See **Annex II.**

importantly, the organisation's privacy policy.[110]The DoC maintains and updates the PS-List and has made it available on the PS's official website. The DoC is responsible for its accuracy and keeps a list of removed companies including the reasons of their removal.

Organisations that persistently fail to comply with the PS-Principles will be removed from the PS-List and must return or delete personal data received under the PS. The DoC monitors organisations removed from the PS-List (either voluntary withdrawal or failure to re-certify) to verify whether they have returned, deleted, or retained personal data previously received. The DoC acts *ex officio* as a monitoring body and oversees false claims of PS participation or the improper use of the PS certification mark. It conducts compliance reviews of self-certified organisations when: it receives a complaint on a particular organisation; organisations do not provide a satisfactory response to its enquiries; or when there is credible evidence that the organisation is not complying with the PS-Principles.

3.2 The Principles

The Principles and Supplemental Principles (hereinafter the Principles) are set out in the Annex II of the PS Adequacy Decision.[111]They apply to both controllers and processors of personal data. The EU controller determines the purpose and means of processing personal data.[112]The processor is contractually bound to act according to the instructions of the EU controller and assist when responding to individuals' claims.[113]

The seven main principles are the basis for the commitments made by US organisations. First, the ***Notice Principle*** obligates the organisation to declare its participation in Privacy Shield.[114] More importantly, the declaration obligates organisations to provide information to data subjects concerning matters such as what type of data they collect, the purpose of their processing, and whether the subsidiaries of the organisation are adhering to the Principles. The Notice Principle establishes organisations' obligation to inform on all key elements of data

[110] C(2016) 4176(n.102), Annex II. Supplemental Principle 6

[111] Id.

[112] 'controller' can be a natural or a legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; see GDPR(n.47),Art.(4)7

[113] 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; see GDPR(n.47) Art.(4)8

[114] C(2016)4176 (n.102), Annex II. Principle 1

processing, organisations' liability, and available recourse mechanisms in their privacy policies.

The ***Choice Principle*** ensures that personal data is used in a manner that meets data subjects' expectations and choices. The data subjects are given the right to object to having their personal data disclosed to a third a party or to be used for different purpose than originally collected for.[115] This gives individuals an opportunity to *opt-out* or in case of sensitive data *opt-in* choice (affirmative consent).[116]

The ***Principle of accountability for onward transfer*** applies to transfers of personal data to a third party controller or a processor.[117] The Principle is closely linked with the Notice and Choice Principles, thus any further transfer of personal data from the US recipient must be executed according to the aforementioned principles. Organisations often outsource data processing to third parties and this is when accountability for onward transfer steps in. While complying with the previous principles, organisations must enter into a contract with a third party controller that must adhere to the limitations and specifications of processing to which an individual has given consent.[118]

Since data transfers between organisations may happen between separate companies or within a corporate group, the onward transfer is not limited to the US jurisdiction and can be conducted in a third country. Therefore, it is critical for it to provide sufficient safeguards for onward transfers to countries with inadequate data protections and particularly for those with laws allowing access to personal data for surveillance purposes. The concern about possible risk posed by an onward transfer to jurisdictions other than the US is relevant. Nevertheless, PS does not obligate organisations to conduct legal due diligence of their sub-contractor countries. [119]

[115] Id., Principle 2

[116] Sensitive data are not exhaustively defined but encompass a wide range of information that may specify one's health condition, race or ethnicity, religion or belief, and sex life

[117] C(2016)4176 (n.102), Annex II. Principle 3

[118] C(2016)4176 (n.102), Annex II. Supplemental Principle 10

[119] WP29, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision (16/EN WP 238, 2016), p.21

The ***Security Principle*** outlines the obligation of organisations to take reasonable and appropriate security measures, to consider the risks of processing, and the nature of the data.[120] The security measures translate to measures taken in order to prevent loss, misuse, disclosure or unauthorised access, alteration, or destruction of personal data. The security obligation is not further specified and demands "reasonable and appropriate" measures. Companies should continually ensure their data security policies are up-to-date.[121] The security aspect of data controlling and processing is critically necessary for the prevention of any data breach. There is no federal law in the US that would impose equal data protection obligations across the US. The Security Principle does not specify what security measures must be fulfilled. However, the high European standards should be applied in order to prevent mass-scale data breaches, such as the cybersecurity breach in the US credit agency, Equifax, this summer[122]and the Uber hack this November.[123]

The ***Principle of data integrity and purpose limitation*** embeds a limitation to processing data for purposes relevant to processing. Thus, a PS organisation must limit personal data to such data that is relevant to the intended purpose of processing. A company cannot process personal data in a way that is incompatible to the purpose for which the data has been collected or subsequently authorised by the data subject.[124] With respect to the obligation concerning the accuracy of collected data, PS organisations must take reasonable steps to ensure that the data is accurate, complete, and current to the extent necessary for processing purposes. However, according to the WP29, the accuracy of data should not depend on the purposes of processing.[125]

The ***Access Principle*** assures that data subjects have access to their personal information. Rights can be exercised without need for justification and only against non-excessive fees. Individuals should be able to correct inaccurate information about themselves, amend it, or

---

[120] C(2016) 4176 (n.102), Annex II. Principle 4

[121] E.g. keeping access controls and procedures for data breach investigation at the state of the art

[122] J MacCrank, 'Equifax says 15.2 million UK records exposed in cyber breach' *Reuters*(10.10.2017) <https://www.reuters.com/article/us-equifax-cyber/equifax-says-15-2-million-uk-records-exposed-in-cyber-breach-idUSKBN1CF2JU>

[123] J Fioretti, 'EU privacy regulators to discuss Uber hack next week' *Reuters*(23.11.2017) <https://www.reuters.com/article/us-uber-cyberattack-eu/eu-privacy-regulators-to-discuss-uber-hack-next-week-idUSKBN1DN1X4>

[124] C(2016) 4176 (n.102), Annex II. Principle 5

[125] WP29(n.119) p.24

even request its deletion. Data subjects also have this right when their data is processed in breach of the Principles. To that end, individuals have the right to obtain confirmation from the organisation, whether such organisation is processing data related to them, and have the data communicated within a reasonable time.[126]

Where individuals are subjected to automated decisions that have either legal effects or that significantly affect the individual, the PS does not provide any legal guarantees. However, when individuals could be affected by computer-made decisions using inaccurate data, they should have sufficient safeguards. Automated processing can be intended to analyse and predict individuals' health, behaviour, personal preferences, movement, etc. According to the WP29 individuals should be given the right to know the logic involved in the decision-making and to request reconsideration on a non-automated basis.[127]

The increased use of automated processing, including profiling, as a basis for decision-making is greatly impacting individuals in the modern digital economy. The explanatory text of the Adequacy decision only remarks that this area needs to be closely monitored. The difference between EU and US on the approach to automated processing was an issue addressed in the first annual review. However, the first review did not deliver any concrete conclusions. The EC has yet to commission a study to collect factual evidence and further assess the relevance of automated decision-making for transfers carried out on the basis of the PS.

Within the EU, the GDPR ensures safeguards against potential risks arising from damaging decisions based on automated processes. EU data subjects have the right to obtain human intervention, express their opinions, and obtain an explanation of the decision and challenge it.[128]

Finally and most important, ***the Recourse, Enforcement and Liability Principle*** obligates Shield organisations to provide potent mechanisms to ensure compliance with the Principles and provide a mechanism for redress. Of vital importance, PS organisations must provide recourse for EU data subjects whose data was processed in a non-compliant manner, including effective remedies. PS organisation must remedy any issues of non-compliance. They are obligated to conduct follow-up procedures that verify their practices conform to their privacy

[126] C(2016)4176 (n.102), Annex II. Principle 6

[127] WP29(n.119) p.17

[128] GDPR(n.47) Art.22, see also Art.4(4) for 'profiling'

policies and their de-facto compliance with the PS-Principles.[129] These procedures should verify that the attestations and assertions made about PS privacy practices are true and being implemented accordingly. This can be done through self-assessment (e.g. internal procedure, training of employees, periodical review) or outside compliance reviews (e.g. auditing or random checks). Both methods of verification are further explained in the supplemental principles, which define an obligation of transparency and retention of records for investigation of individual complaints.[130]

3.3 Redress mechanisms and complaints

The PS organisations are required to provide effective and readily available independent redress mechanisms. Individuals affected by non-compliance have the right to have their claim investigated and expeditiously resolved at no cost. As mentioned in the previously, there are several ways an individual can lodge a complaint.[131]

First, individuals can lodge a complaint directly with a ***PS organisation***. Hence, an organisation's privacy policy must be clear and provide a contact point -- a self-regulatory body -- that will handle complaints by means of an independent redress procedure.

Second, complaints can be brought in front of an ***independent alternative dispute resolution*** (***ADR***) body designated by the PS organisation. The DoC has committed itself to check whether organisations are registered with the ADR body they claim to be registered with. This body can either be in the US or EU and must provide an appropriate recourse free of charge. Sanctions and penalties imposed by an ADR body must be sufficiently rigorous to ensure compliance with the Principles. It should provide a reversal or correction of the effects of non-compliance by the organisation or terminate further processing of and delete personal data.

When an organisation fails to comply with the decision of an independent ADR body, or a self-regulatory body, it must notify the DoC and the FTC or the DoT. These departments have

[129] C(2016)4176 (n.102), Annex II. Principle 7

[130] C(2016)4176 (n.102) Annex II., Supplemental Principle 7

[131] See **Annex III.**

jurisdiction over investigations of unfair and deceptive practices. If none of these departments are competent enough to handle the case, such notification can be brought to a court.

Third, individuals can submit their complaints to their ***national DPAs***. The PS has an option for organisations to choose to cooperate with EU DPAs. An organisation can make this selection with its self-certification submission to the DoC.[132] If an organisation chooses to cooperate with DPAs, they must comply with their informal advice to take action to comply with the Principles or take remedial measures when necessary.

Advice from DPAs is delivered through a DPA-panel that is to be established on the EU level. The panel should ensure a harmonised and coherent approach to a particular complaint. If the organisation fails to comply with the advice within 25 days and has not offered a satisfactory explanation for the delay, the matter will be referred to the FTC, which can lead to enforcement action under the FTC Act. The DPA-panel then concludes that the commitment to cooperate has been seriously breached, which leads to DoC consideration of the organisation's refusal to comply and, as a persistent failure to comply, removal from the PS-List.

Furthermore, European data subjects can bring a case against the EU exporter of personal data to the relevant DPA. In this scenario, the DPA considers whether the transfer from EU is conducted while the exporter has reason to believe that a US organisation on the receiving end is not complying with PS-Principles and such transfer is in violation of EU data protection law. Thus, if necessary, the DPA must order suspension of the data transfer.

Fourth, the ***DoC*** has committed to receive, review, and undertake best efforts to resolve complaints. For this purpose, the DoC provides special procedures for DPAs to refer complaints to a dedicated contact point that tracks and follows up with companies to facilitate resolution. The contact point works closely with the respective DPA during the processing of a complaint and provides the DPA with updates its status. The direct liaison between a DPA and the DoC enables data subjects to lodge a complaint with their national DPA through a more familiar procedure. However, the expediency of settling a complaint in this manner is relevant.

The fifth option is the DPA's referral to the ***FTC***, which gives priority consideration to referrals of non-compliance received from an ADR-body, the DoC, a national DPA, or possibly

[132] When processing human resources data collected in the context of employment, cooperation with DPAs is mandatory, C(2016)4176 (n.102) Annex II., Supplemental Principle 9

even directly from individuals. The FTC then considers the violation of the Act. In cases when the FTC obtains complaints directly from individuals, it has committed itself to conduct a PS investigation. Although it lacks the power to conduct on-site inspections, it has the power to produce documents and provide witness statements. The FTC is an enforcement authority that can also issue administrative orders (also referred to as consent orders) and monitor compliance with these orders.[133]

Thus far, the FTC has brought actions against three US companies for misleading their consumers about their participation in the PS. The companies did not complete the application process, yet they claimed compliance with the Principles and self-certification.[134] The press release came a couple of weeks before the EC came to Washington to conduct the annual review of the framework -- an attempt to showcase how committed the US is to its promises to the EU.

Finally, the ***Privacy Shield Panel*** provides the last resort mechanism. Once the prior redress mechanism fails to resolve a complaint to the full satisfaction of an individual, s/he can invoke binding arbitration by the PS Panel. The panel consists of 20 arbitrators designated by the DoC and the EC. This invocation is done by delivering a notice to the concerned PS organisation. The PS-Panel is an appeal mechanism within the framework that is cost free for data subjects. It has not been operational, however, due to the fact that so far only 16 arbitrators out 20 have been selected.[135]

Alternatively, there is the possibility for individuals to pursue their case within the ***court system***. A judicial redress may be available where the US state court provides for legal remedies under US tort law and in cases of fraudulent misrepresentation, unfair or deceptive acts or practices, or breach of contract.

---

[133] FTC Act(n.57) Sec.20

[134] FTC, 'Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework' (8.9.2017)<https://www.ftc.gov/news-events/press-releases/2017/09/three-companies-agree-settle-ftc-charges-they-falsely-claimed>

[135] EC, COMMISSION STAFF WORKING DOCUMENT *Accompanying the document* REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the first annual review of the functioning of the EU–U.S. Privacy Shield, SWD(2017)344final, p.17

4 Access and use by US public authorities

Adherence to the PS-Principles is limited to the extent necessary to meet national security, public interests, or law enforcement requirements.[136] Thus, an interference with data protection is allowed if it is lawful and justifiable. The WP29 has stressed that derogations allowed under the framework must be justifiable in a democratic society.

The PS-Principles are not absolute and can be derogated from under the condition that the essential guarantees are met. When US law allows for derogations, PS organisations should strive for the highest protection attainable.[137] Limitations to adherence to PS-Principles may be posed by statute, government regulation, or case law that create conflicting obligations or explicit authorisations. Moreover, a limitation is allowed if the effect of the DPD or MS' domestic law allows for exceptions or derogations, provided they are applied in a comparable context.[138]

4.1 Access and use by US public authorities for national security purposes

US law entails numerous limitations on access and use of personal data transferred under the PS for national security purposes. For this reason, the PS framework establishes oversight and redress mechanisms that provide safeguards for data subjects' right to protection of personal data. Following the *Schrems* judgement, the Commission found that the safeguards provided by the PS are sufficient to ensure protection against unlawful interference and risk of abuse.[139]

Among the PS written assurances, the letter from the ODNI, regarding limitations to PS Principles and its commitments in the context of US signals intelligence collection, describes the restrictions established by law, namely by: the Presidential Policy Directive 28 (PPD-28); Executive Order 12333 (EO-12333), Foreign Intelligence Surveillance Act (FISA); and the USA FREEDOM Act.

The national security falls within the authority of the US President whose scope of responsibility includes foreign affairs and intelligence. Meanwhile, the Director of ODNI serves as the

[136] C(2016)4176 (n.102) Annex II, Rec.(5)
[137] WP29(n.119) p.34
[138] C(2016)4176 (n.102) Annex II, Rec.(5)
[139] Id., Rec.(67)

head of the intelligence community and acts as the principal advisor to the President. While the US Congress is empowered to place legislative limitations to intelligence activities, the President can impose executive orders or presidential directives within this delimited scope. For the PS, the following instruments are relevant: PPD-28 and the EO-12333.

First, **the EO-12333** governs all foreign intelligence data collection at the discretion of the President based on his orders. However, it does not provide delimitation of its territorial scope, nor does it provide further information on the extent to which data can be collected or the kind thereof. This all-catching order was claimed to be the legal basis upon which the NSA collected non-encrypted data transiting from Google and Yahoo data centres.[140] However, reading the order in the context of the FISA Act, it could provide the basis for data collection only outside the US territory. The ODNI letter does not explain how the EO-12333 functions, and its application is unclear. It does not provide for any judicial review, oversight, or redress mechanism for the surveillance programmes for which it provides a legal basis.

The PPD-28, adopted during the Obama presidency, is binding upon US intelligence authorities and relevant to non-US subjects. In reaction Snowden revelations, it provides unambiguous limitations for signal intelligence operations. The limitations of data collection are based on the legitimacy of its authorisation, thus require a presidential authorisation and must be in compliance with the US Constitution (particularly the Fourth Amendment) and law.[141] The PPD-28 as such is not a basis for data collection. It imposes limitations upon bodies conducting signals intelligence that must be implemented in their policies and procedures. In particular, the PPD-28 applies to intelligence activities regardless of their location; hence it also applies to data collection for signals intelligence purposes when transferred from the EU to US.

It stipulates that such activities must be "as tailored as feasible". What "as tailored as feasible" implies is difficult to ascertain. Most significantly, limitations and safeguards in PPD-28 impose procedures of data minimization, conditions for retention and dissemination, data security and access by relevant staff, data quality, and oversight. In the ODNI-letter, the office commits to apply the PPD-28 safeguards and limitations to data while it is transmitted. This

---

[140] S Ackerman, 'NSA reformers dismayed after privacy board vindicates surveillance dragnet', *the Guardian* (02.07.2014)<https://www.theguardian.com/world/2014/jul/02/nsa-surveillance-government-privacy-board-report?CMP=ema_565>

[141] US Constitution, Fourth Amendment guarantees privacy, dignity, and protects against arbitrary and invasive acts by officers of the Government

would apply to data transmitted via the transatlantic cables. The legality of such conduct is not determined and the US does not want to reveal whether or not it conducts cable interception.

The PPD-28 does not deny that data collection can still happen *en masse* (bulk collection). The permission of bulk collection is permitted "in order to identify new or emerging threats and other national security information that is often hidden within the large and complex system of modern global communications".[142] A bulk data collection can be authorised due to technical or operational considerations. In this way, data are collected without specific selection terms (selectors).

The PPD-28 permits bulk collection for six purposes that should enable measures to detect and counter threats from: espionage, terrorism, weapons of mass destruction, threats to cybersecurity, to the Armed Forces or military personnel, and transnational criminal threats related to the other five purposes.[143]These measures must be reviewed on annual basis as a minimum. The limitation of mass interception is still quite wide and cannot be deemed as targeted collection. All but one of the five permissible purposes can be reasoned to be legitimate. Permitting bulk collection for purposes related to cybersecurity is too wide, as it does not provide any definition of what cybersecurity means. Cybersecurity is generally a broad term.

Furthermore, the PPD-28 stipulates that all individuals, including non-U.S. persons, should be treated with dignity and respect. It approaches the privacy of data subjects not in terms of rights but as privacy interests. When handling personal data, intelligence agencies must establish policies that include appropriate safeguards designed to minimize data retention and further dissemination.

Evidently, the PPD-28 is an instrument that allows for collection of personal data, the scale of which remains unknown. Although, the ODNI Director considers any bulk collection activities involving internet communications that the US Intelligence Community performs through signals intelligence to be operated on only a small proportion of the internet.[144] The assurance in a letter is hardly solid ground for evident transparency when applying these 6 limitations to data transfer through transatlantic cables.

---

[142] C(2016)4176 (n.102) Annex VI, p.3

[143] Id., Rec.(74)

[144] C(2016)4176 (n.102) Annex VI, p.4

On the other hand, these limitations can be interpreted in the sense of the principle of necessity and proportionality. While exceptions to bulk collection exist, targeted interception is prioritised. When bulk collection cannot be avoided, further use of such data through access is strictly limited to specific, legitimate national security purposes.[145] Lastly, PPD-28 is the most significant instrument for protecting EU data subjects from warrantless and indiscriminate surveillance. Ideally, the PPD-28 should be transposed into a legislative act to ensure standing protection.

Furthermore, the **FISA Act**[146] governs the conduct of physical and electronic surveillance. FISA establishes a legal basis for authorisation of surveillance and, more importantly, for the intelligence programmes, PRISM and UPSTREAM, that are operated by the NSA. Under Section 702 of the FISA (FISA-702), data can be collected from non-US citizens who are outside US territory for purposes of collecting foreign intelligence.[147] Through this, US-based communication services are targeted to provide foreign intelligence information. It is worth noting that under the term “foreign intelligence information” there are many information categories that cause uncertainty as to what information can actually be collected.[148] Meanwhile the PS leans on the non-binding explicit assurances that the US has given to the EC provided that the US Intelligence Community "does not engage in indiscriminate surveillance of anyone, including ordinary European citizens".[149]

The **USA FREEDOM Act**[150]was originally introduced to the US Congress a few months after the Snowden revelations and was enacted in 2015. Essentially, it was tailored to prohibit mass surveillance in the context of collection of communications metadata. However, it does not preclude data surveillance under FISA-702 and EO-12333. It establishes legal obligations for intelligence agencies to use specific selection terms in order to target the data collection.[151]

---

[145] Id., Rec.(76), also see C-362/14 (n.72) para.93

[146] Foreign Intelligence Surveillance Act of 1978 (FISA) 50 U.S.C. § 1801 *et.seq.*

[147] Title VII, Section 702 of the FISA, “Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons” 50 U.S.C. sec. 1881a, (FISA-702)

[148] WP29(n.119), p.36

[149] C(2016)4176 (n.102) Annex VI, p.18

[150] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act), Pub. L. No. 114-23, H.R. 2048, (Codified in scattered sections of 12 U.S.C., 15 U.S.C., 18 U.S.C., and 50 U.S.C.)

[151] C(2016)4176 (n.102) Annex VI, p.5

4.1.1 Forthcoming: The FISA-702 reform

Remembering the invalidation of Safe Harbour, the CJEU found the scheme in violation of fundamental rights due to warrantless surveillance that was authorised under the FISA-702. The PS is going to be reviewed by the CJEU and, in order for it to succeed, Section 702 has to be reformed. Notably, FISA-702 includes a sunset clause that put it under review in 2017.[152] The newly proposed bills to reform Section 702 are the USA Rights Act and the USA Liberty Act of 2017. In November 2017, at a hearing in the US House of Representatives, the House Judiciary Committee passed the latter bill. If it is made into an act of law, it would be a careful compromise to reform FISA-702.

It is not yet clear whether the proposed Liberty Act will make it to the Senate. The current leader of the Senate majority, Mitch McConnell, has been vocal about non-amending re-authorisation of FISA-702.[153] The Liberty Act attempts to maintain the core function of FISA-702, which is the collection of electronic communications of non-US persons for purposes related to national defence. The novelty incorporated includes slightly enhanced protections and requirements for transparency that would ensure principles of privacy and due process. Most significantly, it proposes limits on queries of the databases of information collected under FISA-702 to queries with a legitimate national security or law enforcement purpose.[154] Furthermore, it would codify the prohibition of acquisition of information that goes beyond (either to or from) the intelligence target (address lines), also known as "about surveillance" of the internet communications or "upstream activity".[155] The bill would codify a part of the PPD-28 that recognizes the privacy interests of non-US citizens; thus the principle of international comity, based in US foreign relations law, would apply.[156] Finally, the bill would be renewed and be placed under review in six years.

---

[152] FISA-702(n.146) is to expire on 31.12.2017

[153] D.B. Johnson, 'House Panel Advances FISA reform', *FCW* (13.11.2017)<https://fcw.com/articles/2017/11/13/702-judiciary-markup-johnson.aspx>

[154] A Stepanovich, 'First take on Section 702 surveillance reform: progress on human rights, but more is needed', *AccessNow* (05.10.2017)<https://www.accessnow.org/first-take-section-702-surveillance-reform-progress-human-rights-needed/>

[155] This limitation was first imposed by the FISA Court in April 2017, see: NSA, 'NSA Stops Certain Section 702 "Upstream" Activities' (28.04.2017)<https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml>

[156] W.S. Dodge, 'International Comity in American Law', *Colombia Law Review*, [1983] 115/8, pp.2071-2141

4.2 Oversight mechanisms

One of the core safeguards of the PS framework is an independent oversight mechanism for intelligence agencies and their activities. For it is typical of US intelligence agencies to have multiple oversight mechanisms.[157] The first layer is made of internal bodies for oversight within each agency. Internal oversight is demanded by the PPD-28 and obligates agencies to facilitate oversight of the implementation of safeguards protecting personal information. The US intelligence and security agencies have designated staff members who are ensuring compliance within the existing law. Additionally, the DoJ and the Department of Defence provide oversight of intelligence activities.

Second, each agency has an Inspector-General that is mandated with oversight of foreign intelligence. They are authorised to investigate complaints, allegations of unlawful conduct, or abuse of authority. Furthermore, they can conduct audits and review programmes -- including fraud, abuse, or violation of law -- and can recommend corrective actions. Although, the Inspector-General's recommendations are not legally binding, her/his reports are public and passed on to Congress. Thus, Congress is informed of non-compliance and can exercise punitive measures towards the agency. The Inspector-Generals are statutorily independent. According to the WP29, Inspector-Generals can meet the criterion of organisational independence as defined by the CJEU and ECtHR once an authority that is independent from the agency they are supposed to oversee has appointed them.[158]

Third, another internal oversight mechanism is the ODNI's Civil Liberties and Privacy Office (CLPO) charged with ensuring that the intelligence community operates in a manner that advances national security while protecting civil liberties and privacy rights.[159] All agencies have Privacy and Civil Liberty Officers, who assist with the compulsory self-reporting system with Congressional oversight.[160] With regard to the external oversight, Congress, specifically the House and Senate Intelligence and Judiciary Committees, has oversight responsibilities concerning all US foreign intelligence activities.

---

[157] See **Annex IV.**

[158] WP29(n.119) p.40

[159] C(2016)4176 (n.102) Annex VI, p.8

[160] WP29(n.119) p.41

Fourth, the Privacy and Civil Liberties Oversight Board (PCLOB) is an independent body established by a statute within the executive branch. It is tasked with analysing and reviewing counterterrorism programs and policies, including the use of signals intelligence. PCLOB is a bipartisan body with a five-member board appointed by the President (with Senate approval) for a fixed six-year term. It ensures that considerations for liberty are made in the development and implementation of laws, regulations, and policies related to efforts to protect the nation against terrorism. It is supposed to report on the implementation of the PPD-28 in the near future.

The proposed USA Liberty Act reforming FISA-702 would give PCLOB the ability to function without an appointed chair, which has been a chronic issue for the body. It would also put in place new reporting requirements. Since the PS-framework entered into force, the PCLOB has had only one member. The EC's first annual review of the PS addresses this issue in which the EC calls for a swift appointment of the remaining members so that the Board is able to fulfil all duties for its full functionality. The Board members should have extensive national security and privacy expertise. Thus far, President Trump has nominated only one person to be the chair of the Board.[161] The PCLOB still lacks a quorum to conduct any business. Filling the remaining posts is especially important in the context of the ongoing FISA-702 reform and consequently the PS judicial review at the CJEU.

Moreover, the PCLOB is supposed to report on the implementation of the PPD-28 in the near future. Similarly, given the relevance of PPD-28 for the limitations and safeguards that apply to government access for signals intelligence, the annual report demands a speedy release of this report.

The Foreign Intelligence Surveillance Court (FISC or FISA Court) provides judicial oversight. The FISC is composed of 11 independent federal judges and is responsible for oversight and ensuring compliance of any signals intelligence collection activities conducted pursuant to FISA. The Foreign Intelligence Court Review (FISCR) can review FISC decisions and the next level for appeal is the Supreme Court. The procedure in front of the FISC is ex parte. However, after adopting the USA FREEDOM Act, the standing panel is now supported by an

[161] The White House, 'President Donald J. Trump Announces Intent to Nominate Personnel to Key Administration Posts'(25.08.2017)<https://www.whitehouse.gov/the-press-office/2017/08/25/president-donald-j-trump-announces-intent-nominate-personnel-key>

Amicus Curiae Advisory Panel that comprises individuals with expertise in national security and civil liberties. After passing the prerequisite security clearances, the panel provides technical advice, attends FISC hearings and supplies briefs, and argues on the merits of a case from the perspectives of privacy and civil rights. The panel is active only in important cases and when new legal interpretation is required. [162]Its duty is to give unbiased advice, not to defend the interest of an individual upon request.

Under FISA-702, FISC authorises surveillance programs (like PRISM and UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence. This certification is a one-sided performance. Once approved by FISC, it allows targeting of persons reasonably believed to be outside the US and identifies the categories of foreign intelligence information. The Court does not have to be presented with specifications for particular persons who will be targeted. FISC assesses whether targeted communications can be reasonably believed to be communicating foreign intelligence.

With regard to the FISA-702, FISC could be required to appoint an *amicus curiae* to assist it in reviewing the annual certification from the Attorney General and the Director of National Intelligence. Thus, the amicus curiae could check the proportionality of targeting and application of minimisation procedures. Nonetheless, FISC could dispose of the appointed amicus whenever it found it to be inappropriate.

4.3 Judicial remedies available to the individuals

The limits of the judicial redress emanate from the Fourth Amendment of the US Constitution. The protections provided do not apply to non-U.S. persons located abroad. Therefore, foreign individuals targeted under FISA-702 have no Fourth Amendment rights.[163]

Moreover, there are other obstacles for bringing a civil claim against US officials according to US legal doctrines. The *standing doctrine* conditions the establishment of the federal court's jurisdiction over a claim in the first instance. For that reason, the plaintiff's complaint must include factual allegations that, accepted as true, plausibly allege the three elements of stand-

[162] WP29(n.119) p.41

[163] US Supreme Court, *US v. Verdugo-Urquidez*, 494 U.S. 259 (28.02.1990); US Court of Appeal, 9th Circuit, *US v. Mohamud*, No.14-30217 (05.12.2016)

ing under U.S. doctrine: (1) an injury in fact, (2) a sufficient causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favourable decision.[164] In simpler terms, the plaintiff has to demonstrate that s/he will or has sustain(ed) injury or harm and that this harm can be remedied. Hence, filing an action against governmental acts or federal law by an individual is prevented.[165] In Europe, individuals have to have the opportunity to access court when their fundamental rights have been violated.[166] Although the US Judicial Redress Act ensures rights to an effective redress mechanism, it excludes national security matters and consequently the rights of individuals affected by the national security intelligence surveillance cases.[167]

The available avenues for justice for European data subjects in the US are limited. Under FISA, individuals have the right to seek relief in the US court system, whereas plaintiffs have to be able to establish standing. FISA merely allows individuals subjected to unlawful electronic surveillance to sue government officials for damages.[168] However, it is virtually impossible to establish a standing because according to either FISA-702 or EO-12333 data subjects are not notified of surveillance. This shows how exceedingly difficult it is to establish standing to challenge surveillance in US court.

Notably, there is another barrier and that is the *secrets doctrine*. Surveillance based on the previous explained norms is conducted in secret. The US government is able to argue that a plaintiff's claim is mere speculation and insufficient to establish a standing.[169]Inevitably, the state secrets privilege prevents US courts from assessing the lawfulness of surveillance. The privilege allows the state to block disclosure of specific information by claiming potential harm to national security by that disclosure.

Additionally, the Freedom of Information Act (FIOA) provides for individual redress mechanism. The US government has claimed that FIOA provides a legal basis for seeking access to existing federal agency records, including where an individual's personal data is contained.

---

[164] The Irish High Court, EXPERT REPORT OF ASHLEY GORSKI ON BEHALF OF THE SECOND NAMED DEFENDANT (Maximilian Schrems), Record No: 2016/4809 P <https://iapp.org/media/pdf/resource_center/Schrems-testimony-Gorski.pdf>, para.50

[165] WP29(n.119) p.43

[166] ECtHR, *Roman Zakharov v. Russia,* App.no.47143/06 (04.12.2015), para.171

[167] Judicial Redress Act of 2015, 5 U.S.C. §552a

[168] FISA-702(n.146) §1810

[169] US Supreme Court, *Clapper v. Amnesty International*, 568 U.S. 398 (26.02.2013)

However, the FOIA permits the government to withhold certain classified information from disclosure[170] and such data gathered by foreign intelligence agencies is classified.

4.3.1 The Privacy Shield Ombudsperson

Because there were no options to have the legality of data processing assessed by an independent authority, the PS brought a novelty to the recourse mechanism tailored for European data subjects -- the Privacy Shield Ombudsperson. The PS Ombudsperson is a mechanism for EU individuals to submit requests regarding signal intelligence. The Ombudsperson can process requests relating to data that has been transmitted from the EU to the US pursuant to both the PS framework and on a contractual basis as found in the SCCs and BCRs. The PS establishes this tool to provide form independent oversight with regards to the signal intelligence and a complaint mechanism for individuals without having to prove standing.

An individual can submit a request to a MS' body that is competent for the oversight of national security services and/or the processing of personal data by public authorities. The request will be submitted to the Ombudsperson by an EU-centralized individual complaint management body. Once the Ombudsperson receives a proper complaint, s/he will investigate and provide the complainant with a response.[171]Nevertheless, in cases of non-compliance, the Ombudsperson cannot disclose to the complainant that s/he was the target of surveillance, nor can s/he provide information on specific remedial actions taken.

The Ombudsperson does not have the power to demand a governmental intelligence agency to implement a particular remedy. S/he may cooperate with intelligence agencies' Inspector Generals and may refer matters to the PCLOB. However, neither the Inspector Generals nor the PCLOB can issue recommendations that are binding on the executive branch.

The institute of the Ombudsperson is part of the State Department, raising questions and issues concerning independence and conflicts of interest. Most importantly, however, after more than a year of PS in force, the Ombudsperson has yet to be appointed. Similarly, as in case of the PCLOB-Board members, the EC asked in its first annual review for a swift and

[170] Freedom of Information Act of 1966 (FOIA) 5 U.S.C. § 552(b)(1)

[171] C(2016) 4176 (n.102) Rec.(121)

permanent appointment for the position. Considering that the FISA-702 has yet to be reformed, important oversight institutes lack staff.

4.4 Access and use by US public authorities for law enforcement and public interest purposes

The PS provides assurances with regard to interference with personal data transferred under the PS for law enforcement purposes. Again, in the form of a written assurance provided by the DoJ, the US government promises to ensure applicable limitations and safeguards to protection of European data subjects' rights. The letter gives an overview of the primary investigative tools used to obtain commercial data and other recorded information from corporations in the US for criminal law enforcement or public interest (civil and regulatory) purposes, including the access limitations set forth by those authorities. [172]

The assurance letter lists applicable procedures under the Fourth Amendment, statutory and procedural law, and Guidelines and Policies of the DoJ. The Fourth Amendment enshrines the obligation of law enforcement authorities to require a court-ordered warrant showing a probable cause prior to search and seizure. It gives a guarantee of privacy and dignity and protects from arbitrary and invasive acts by government agents. The exception to a warrant requirement applies when law enforcement is subject to a "reasonableness" test. Whether a search or seizure is reasonable is determined by assessing: first the degree to which the activity intrudes upon an individual's privacy, and second the degree to which it is necessary for the promotion of legitimate governmental interests.[173]

As explained earlier, the Fourth Amendment protections do not extend to non-US persons. The PS Adequacy Decision explains that European data subjects benefit indirectly from the safeguards. Law enforcement authorities have to seek judicial authorisation or at least respect the reasonableness requirement when accessing PS organisations' data sets, which include also European personal data.[174] However, it is not clear whether judicial remedies are available for EU individuals. The limitations inherent in the Fourth Amendment prevent non-US persons from successfully challenging warrants issued to access their personal data. In theory,

[172] Id.,Annex VII

[173] Id.,Rec.(126)

[174] Id.,Rec.(127)

this issue should be hindered by the Judicial Redress Act, which provides judicial redress for non-US persons.

5 Reviewing the Privacy Shield after its first year in force

5.1 Periodic review of adequacy finding

After mishandling Safe Harbour, the EC established an annual joint review mechanism. The Commission must periodically check whether its findings related to the Adequacy Decision meet the level of protection ensured by the US under the PS framework. The CJEU stressed in the *Schrems* judgment that an adequacy decision cannot be based only on justifiable findings at the time of issuing the decision, but it is subject to review in order to check the level of protection available over time.

If the Commission concludes that the level of protection offered by the PS can no longer be regarded as essentially equivalent to the one in the EU, it will start the process of suspending the PS. The EC can initiate the procedure leading to the partial or complete suspension or repeal of its adequacy decision. Alternatively, the EC may propose to amend its decision.[175]

The EC must continuously monitor the functioning of all aspects of the PS and examine whether its limitations and safeguards are factually and legally justified. In addition to the annual review, such a check is required when evidence inspires doubt in that regard.[176] To this end, the EC must draw on all sources of information available, including transparency reports from US businesses on access requests from the government, DPA reports, privacy groups, media reports, etc.[177]The review covers the exceptions for the operations of national security interests and law enforcement. Since the PS entered into force, a major reform of EU data protection law took place and thus the EC proclaims to assess the level of protection provided by the Privacy Shield following the entry into application of the GDPR.[178]

The annual review is a joint review, so the EC must meet with the DoC, the FTC, and other relative departments. The representative authorities must provide comprehensive information

[175] Id.,Rec.(150)
[176] C-362/14(n.72) para76
[177] USA Freedom Act(n.147)
[178] C(2016)4176 (n.102) Rec.(147)

on the functioning of PS including any referrals from the DPAs and results of compliance reviews performed *ex officio* by the DoC. While the review is conducted, representatives from the WP29 and the EU DPAs can be present.[179]

5.2 Annual review 2017

The first annual review was conducted on 18-19 September 2017, shortly year after the PS became operational and the final report was issued.[180] The EC has found that the PS continues to provide an adequate level of protection. The Commission considered the new recourse mechanisms provided for individuals, enforcement procedures, and cooperation with European DPAs as satisfactory, however it did make recommendations to improve the current state of the PS.

Namely, the DoC should be more proactive and regular with its compliance monitoring practices. This is largely due to the fact that companies can publicly identify as PS self-certified before their application has been finalised by the DoC. To this end, there might be a difference between the DoC's PS-List and the number of companies claiming self-certification. This creates uncertainty for EU data subjects. Moreover, it raises the risk of false claims participation and undermines the credibility of the framework.[181] For this reason, companies should not be able to claim self-certification before their submission has been accepted and finalised. Additionally, the DoC should actively and regularly conduct searches for false self-certification claims and non-compliance.[182] The latter should be pursued by demanding annual compliance reports from PS businesses and from those seeking to be re-certified. This will help to discover systematic deficiencies and subsequently address them as amendments to the PS.[183]Another recommendation was made regarding the improvement in inter-departmental cooperation to improve implementation and enforcement of the framework. Additional clarifications of the framework and guidance of companies could benefit from such cooperation.

---

[179] Id.,Rec.(148)

[180] EC, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the first annual review of the functioning of the EU–U.S. Privacy Shield, COM(2017) 611final

[181] Id.,p.4

[182] Id.

[183] Id.,p.5

As mentioned in the previous chapter, the Commission will commission a study on automated decision-making to understand its relation to transfers of data and data protection. Second, for the proper functioning of the recourse mechanisms and oversight of the framework, the US administrations must fill empty positions, namely the PS ombudsperson and the PCLOB Board Members. Finally, the protections of non-US persons provided by the PPD-28 should be included in the new FISA-702 reform.[184]

The positive conclusion of the Commission's review was to be expected. Naturally, the EC seeks to ensure continuous data flow. However, the opinions of important stakeholders are yet to be published. The EDPS and the WP29 commented on the framework and both voiced their concerns over the PS's validity, especially in regards to legality of mass surveillance in the US. Both of these authorities are going to issue their own opinion of the annual report. One can expect that their previous concerns will be highlighted and confirm remaining flaws of the PS.

5.3 CJEU review: postponed

There have been two complaints at the CJEU concerning the validity of the PS Adequacy Decision. The first action was lodged by the advocacy organisation Digital Rights Ireland (DRI) promoting human rights in the digital age a month after the PS entered into force. The organisation is claiming that the Decision is violating the CFREU and is incompatible with Articles 7, 8 and 47, as well as with the Article 25(6) of the DPD read in the light of the Charter and the *Schrems* judgement.

The action has been declared inadmissible since the applicant is a legal person and its official title did not identify any natural person. Thus, it cannot avail of the protection of personal data.[185] DRI claims that representations and commitments made in the letters from the US government cannot constitute political commitment within the meaning of 25(6) of the DPD. It also points to insufficient FISA-702 reform.

[184] Id.,p.6

[185] Case T-670/16 Digital Rights Ireland v European Commission [2017] ECLI:EU:T:2017:838

The second action was brought by the Paris-based privacy advocacy group La Quadrature du Net. The pleas in law are comparable to those brought by DRI.[186] However, since the action is brought by a legal entity too the action will most likely be deemed inadmissible as well. According to the recent decision, it would take an action lodged by a natural person to successfully challenge the PS in the future.

5.3.1 Suggestive EU-Canada PNR Agreement

In July 2017, the CJEU issued its opinion on the draft Passenger Name Record (PNR) agreement between EU and Canada. The opinion was given upon request by the EP under the TFEU, Article 218(11). It was the first time the Court assessed conditions under which the EU may allow cross-border data transfer through treaties. The Court has found that the PNR agreement could not be concluded unless amended.[187]

The length into which the CJEU went to examine the EU-Canada agreement illustrates the comprehensive nature of the Court's assessment. An interesting issue of the Court's concern is the independence of the Canadian oversight office. It deemed the office not sufficiently independent. Analogously, the US oversight system could face the same criticism if the CJEU would be to review the PS framework. While there are multiple oversight bodies in the PS framework, the level of their independence varies. However, it is difficult to foresee how similar the approach would be in the PS review because of the differences in intended use between PNR- and PS-based data transfers.

5.3.2 Awaiting the Schrems II.

In early October 2017, the Irish High Court issued another judgment on Facebook's data transfers between the EU and US in the context of US surveillance laws -- EO-12333 and FISA-702, and the surveillance programmes UPSTREAM and PRISM.[188] Yet again, this case was initiated by Maximilian Schrems and is therefore referred to as *Schrems II*. After the first

[186] Case T-738/16 La Quadrature du Net and Others v Commission [2017]

[187] Case Opinion 1/15 [2017]ECLI:EU:C:2016:656

[188] The Irish High Court Commercial, *Data Protection Commissioner v. Schrems and Facebook Ireland* [2016 No. 4809 P.] (03.10.2017)

Schrems case that led to the invalidation of the Safe Harbour, personal data were transferred to the US on the Standard contractual Clauses (SCCs or Model Clauses). The case continued with an updated complaint in 2015. This time the Irish DPA took the same view as Schrems and claimed that the change of legal basis for data transfer is meaningless if US law continues to allow mass surveillance while an effective redress mechanism is missing. While Schrems' complaint asked for the cessation of Facebook's data transfer, the Irish DPC took the proceedings to another level and asked for invalidation of the SCCs as basis for data transfer in their entirety.

The Irish DPC then adopted a decision that determined the SCCs as insufficient for the protection of EU data subjects and, because it does not have the authority to suspend data transfer alone, it referred the case to the Irish High Court. Before the Irish High Court referred the case to the CJEU, it inquired expert testimony from Schrems and Facebook on US surveillance law and intelligence practice as well as the adequacy of remedial mechanisms accessible to EU citizens. The expert testimonies attached to the referral to the CJEU invite the CJEU to evaluate third country law.[189] For that purpose, the Court may commission its own expertise on US law as a measure of inquiry.[190] The Court could decide to view US law as an issue of fact. This could shed some light on the level of transparency and quality of expert studies on third countries commissioned by the EC prior issuing adequacy decision.[191]

To a certain extent, the first *Schrems* case did evaluate US legal standards. It took into account the effect of US law and practices of the US Intelligence Community on the fundamental rights of European data subjects.[192] The opinion of the Advocate General also included an evaluation of the US FTC supervisory powers.[193] Similarly, in the PNR Opinion, Canadian law provisions required interpretation.[194] Thus, if the CJEU proceeds to the judicial review of the PS in the future, it could not avoid evaluating the relevant US laws.

---

[189] E.g. *Gorski*(n.154)

[190] CJEU, Rules of Procedure of the Court of Justice [2012] OJ L 265/1-42, Art.64(2)

[191]C Kuner, 'Third Country Law in the CJEU's Data Protection Judgments' *European Law Blog* (12.07.2017)<http://europeanlawblog.eu/2017/07/12/third-country-law-in-the-cjeus-data-protection-judgments/>

[192] C-362/14(n.72) para.90

[193] Advocate General Bot(n.77) para.207

[194] Opinion 1/15(n.183)

5.4 Privacy Shield under scrutiny

The hasty solutions for EU-US data flow after the fall of the Safe Harbour have been heavily criticised. The system of the PS, based in signed letters by the US governmental representatives, does not project confidence of this becoming a long-term regulatory solution. The written assurances were given by the outgoing Obama administration. In January 2017, the Trump administration acknowledged the importance of the PS for trade and the relationship with the EU.[195] Although, the pace of nominating staff for crucial spots leaves the PS handicapped.

The European institutions expressed their concerns and negative opinions,[196] but the EC has stood by its political commitment to the EU-US relationship. The PS was described as a solid transatlantic partnership relating to common values, shared political and economic objectives, and close cooperation in the fight against common threats to security.[197] Nonetheless, the EDPS, Giovanni Buttarelli, described the transatlantic agreement as an interim instrument for the short term and that something more advanced needs to be conceived.[198] Buttarelli said that privacy and data protection must be a priority. Additionally, the newly adopted GDPR standards will require more transparent data protection laws in third countries for the cross-border data flow to be allowed. This does not give the PS much credit. However, with the inadmissibility order for the DRI challenge, the PS is safe for now and the US administration has more time to implement its promises and relevant legal reforms.

[195] DoC, U.S. Secretary of Commerce Wilbur L. Ross, Jr. Addresses Department of Commerce Employees (01.03.2017)<https://www.commerce.gov/news/secretary-speeches/2017/03/us-secretary-commerce-wilbur-l-ross-jr-addresses-department-commerce>

[196] WP29 (n.119); and EDPS (n.52)

[197] EC, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117final,p.2

[198] C Stupp, 'EU privacy watchdog: Privacy shield should be temporary', *Euractiv* (03.08.2017)<http://www.euractiv.com/section/data-protection/interview/eu-privacy-watchdog-privacy-shield-should-be-temporary/>

6 Conclusions

Classifying protection of personal data as a fundamental right offers a strong basis for ensuring rights of individuals in the digital sphere in the EU. However, the stronghold of data processing is currently located in the US where the data protection is based in sector-specific laws and aims to place as little legislative burden as possible on electronic commerce. At the same time, the US Intelligence Community can access personal data of European data subjects on an indiscriminate basis. The EU seeks to overcome the disparity of the legal systems by placing obligations upon companies receiving data in the US accompanied by robust framework of oversight and recourse mechanisms ensured by the political promises of the US government.

This thesis has examined the EU-US Privacy Shield regulating data transfer in the context of legislative and judicial developments and assesses whether it provides an adequate protection to European data subjects. As explained in detail, the PS framework is multi-layered and substantial in its volume. The circumstances under which this model came about show the economic importance and interest of continuous transatlantic data flow. While the EU offers substantial legislation on data protection, there are no general data protection laws in the US. The PS was established by means of a unique political agreement, the basis of which the EC adopted the decision that the US must ensure an adequate level of protection for personal data while it adheres to its commitments.

First, the reason why this framework was designed stems from the Snowden revelations. Since the previous agreement failed to ensure what the CJEU articulated as an essentially equivalent protection, the PS aimed to provide better safeguards and redress mechanisms to the EU data subjects. The failure of SH was influential in how the PS was built. The PS seeks to reprehend the mistakes of the SH and thus enhances the commitments of the US government authorities. As the previous chapters show, the framework is complex and difficult to navigate in. The level of protection provided under PS is generous in size, but at the same time its effectiveness is questioned. This is mainly due to the fact that it has not yet been fully implemented.

Second, the *Schrems* case reiterates that enabling intelligence agencies to have access on a generalised basis to the content of electronic communications must be regarded as compro-

mising the essence of the fundamental right to respect for private life, as guaranteed by CFREU.[199] The PS-package includes assurances prohibiting mass bulk collection of personal data for both US and non-US persons. However, it also refers to lawful purposes as exceptions to prohibition of bulk collection with regard to activities on the internet. The reading of the PS can be quite ambiguous, as it refers to legislation excluding bulk data collection and at the same time admits mass collection in practice.

Third, the US administration needs to take steps to guarantee effective oversight over activities of the Intelligence Community and to provide for a institutionally independent redress mechanism in the form of an Ombudsperson. Even though the PS is now in its second year in force, it is still in an early stage of implementation. It passed its first annual review by the EC and further opinion may be issued soon by the WP29. The lessons learned from the PS could be applied in future trade deals incorporating data protection (e.g. JEFTA – Japan-EU-Free Trade Agreement).[200]

Finally, now that the first possibility of a judicial review for the PS has been dismissed, the framework has gained some time to reach its full potential. Since it entered into force, it has been dismissed by many as an interim measure bound to fail. This perception is propelled by the state of US legislation allowing mass surveillance of data. This could be overcome in a meaningful reform of the FISA-702 that would incorporate the PPD-28.

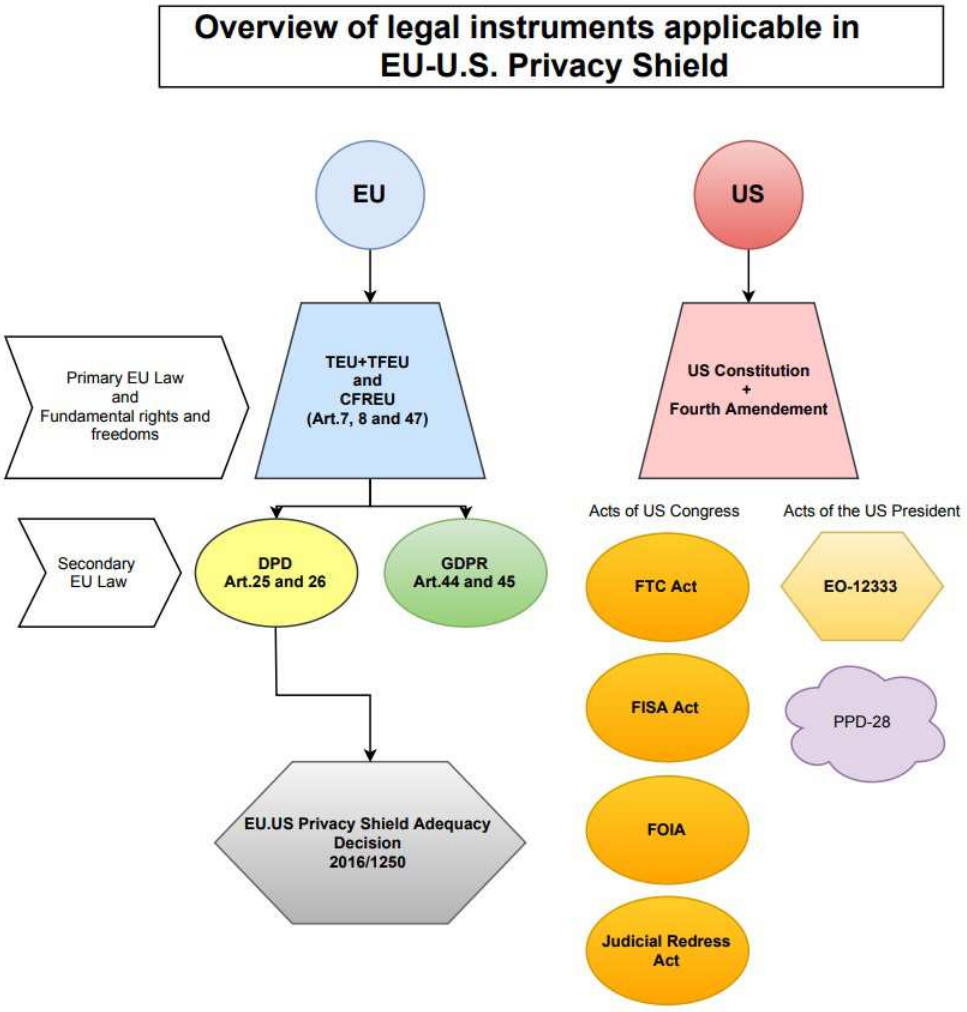
Given that the guarantees of implementation, oversight and redress mechanisms are contained in assurances letters from US officials, the framework is reliable only as long as the US sees the work as necessary for the administration and worthwhile for the economic benefits that transatlantic data flow brings. However, any regulatory framework of data transfer should have the interests and rights of individual data subjects at the centre.

---

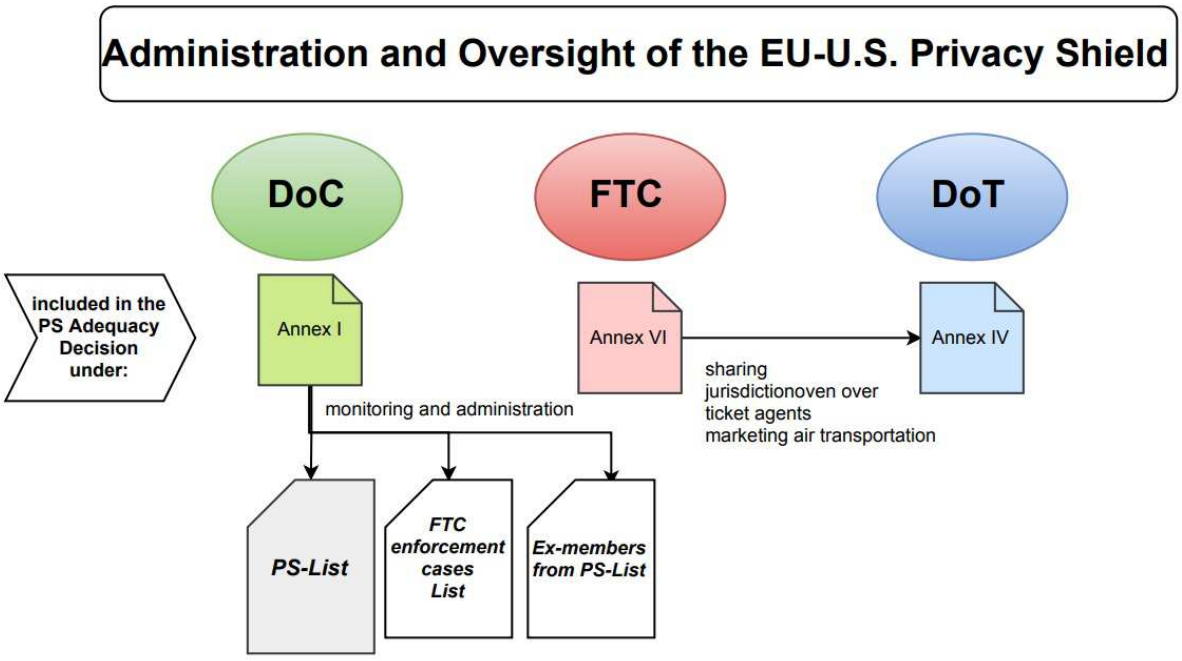
[199] CFREU (n.9) Art.7

[200] K von Paczinsky, Tenczin, JEFTA:Zweites Privacy Shield“ mit Japan in Sicht, *Internationaler Datenschutz* (21.11.2017)<https://www.datenschutz-notizen.de/jefta-zweites-privacy-shield-mit-japan-in-sicht-0119512/>

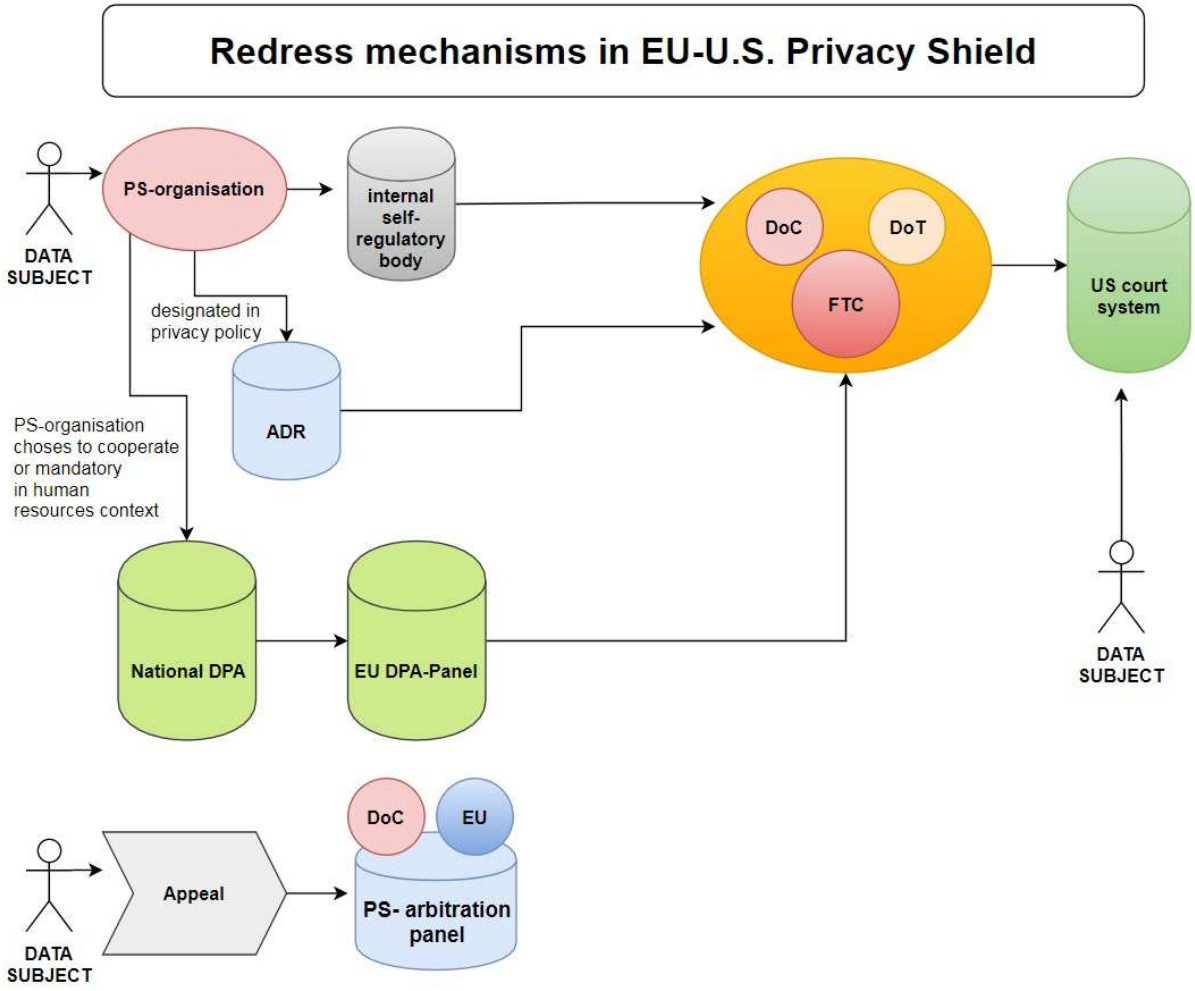
Annex I.


Overview of legal instruments applicable in EU-U.S. Privacy Shield
EU
US
Primary EU Law and Fundamental rights and freedoms
TEU+TFEU and CFREU (Art.7, 8 and 47)
US Constitution + Fourth Amendement
Secondary EU Law
DPD Art.25 and 26
GDPR Art.44 and 45
Acts of US Congress
Acts of the US President
FTC Act
EO-12333
FISA Act
PPD-28
FOIA
Judicial Redress Act
EU.US Privacy Shield Adequacy Decision 2016/1250

Annex II.


Administration and Oversight of the EU-U.S. Privacy Shield
DoC
FTC
DoT
included in the PS Adequacy Decision under:
Annex I
Annex VI
Annex IV
sharing jurisdictionoven over ticket agents marketing air transportation
monitoring and administration
PS-List
FTC enforcement cases List
Ex-members from PS-List

Annex III.


Redress mechanisms in EU-U.S. Privacy Shield
DATA SUBJECT
PS-organisation
internal self-regulatory body
DoC
DoT
FTC
US court system
designated in privacy policy
ADR
PS-organisation choses to cooperate or mandatory in human resources context
National DPA
EU DPA-Panel
DATA SUBJECT
DoC
EU
Appeal
PS- arbitration panel
DATA SUBJECT

Annex IV.

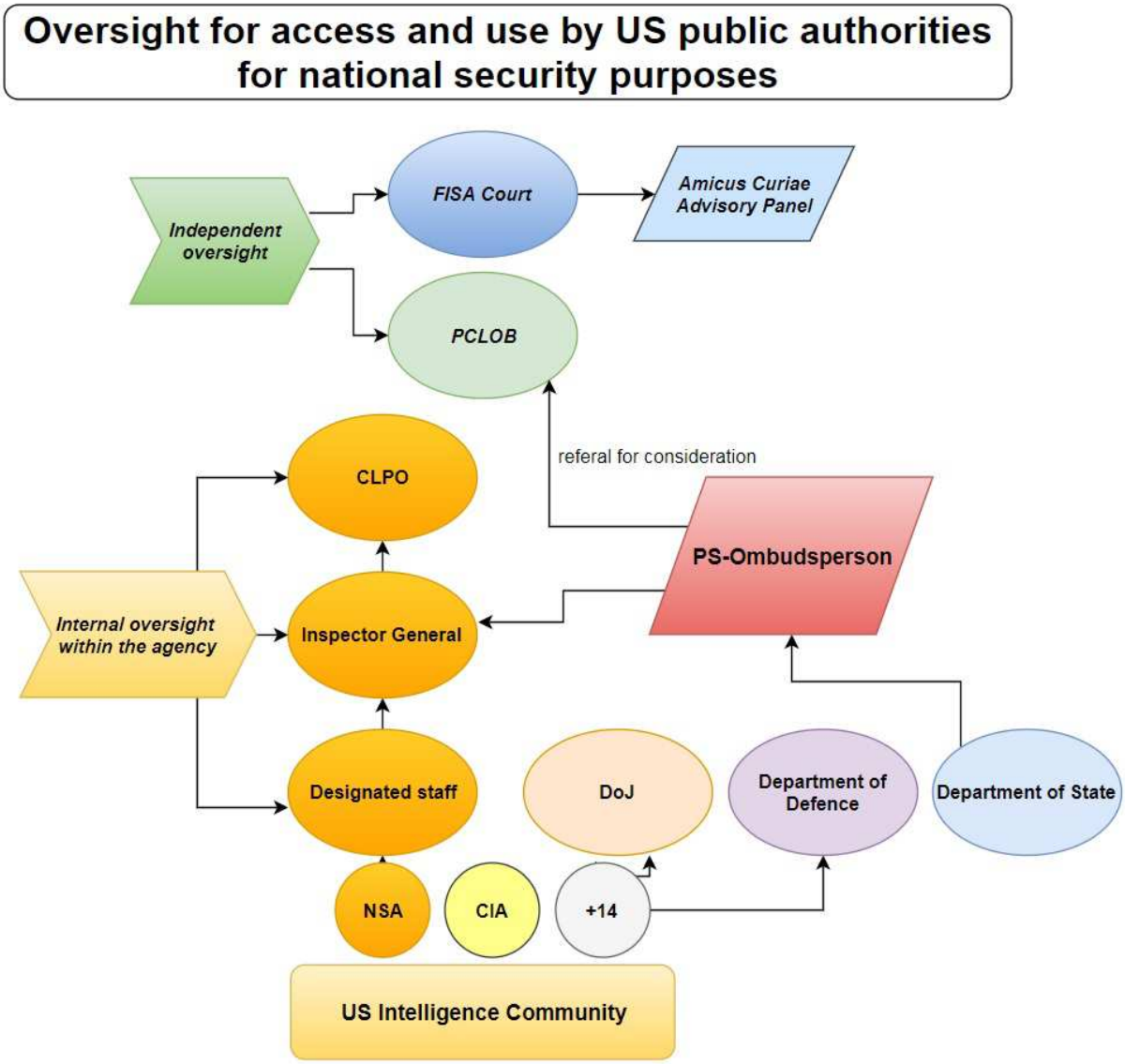

Oversight for access and use by US public authorities for national security purposes
Independent oversight
FISA Court
Amicus Curiae Advisory Panel
PCLOB
referal for consideration
CLPO
PS-Ombudsperson
Internal oversight within the agency
Inspector General
Designated staff
DoJ
Department of Defence
Department of State
NSA
CIA
+14
US Intelligence Community

Table of references

Treaties

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 (ECHR) [1950] ETS 5

Charter of Fundamental Rights of the European Union (CFREU) [2012] OJ C 26/391

Consolidated version of the Treaty on the Functioning of the European Union (TFEU) [2012] OJ C326/47

Consolidated version of the Treaty on European Union (TEU) [2012] OJ C326/13

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (Lisbon Treaty) [2007] OJ C306/1

European Union Statutes

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 (notified under document number C(2000) 2441) (Text with EEA relevance.) [2000] OJ L 215/7

Commission Implementing Decision (EU) 2016/1250 of 12 July 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 (notified under document C(2016) 4176) (Text with EEA relevance) [2016] OJ L 207/1

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (DPD) [1995] OJ L281/31

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89

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, and repealing Directive 95/46/EC (GDPR) (Text with EEA relevance) [2016] OJ 2119/1

Rules of Procedure

CJEU, Rules of Procedure of the Court of Justice [2012] OJ L 265/1-42

United States Statutes

Federal Trade Commission Act (FTC Act) 15 U.S. Code § 41-77

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261 (codified in scattered sections of 50 U.S.C.).

Freedom of Information Act of 1966 (FOIA) 5 U.S.C. § 552

Judicial Redress Act of 2015, 5 U.S.C. § 552a.

Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act), Pub. L. No. 114-23, H.R. 2048, (Codified in scattered sections of 12 U.S.C., 15 U.S.C., 18 U.S.C., and 50 U.S.C.)

Exec. Order No. 12333, 3 C.F.R. 200 (1981 Comp.), reprinted in 50 U.S.C. § 401 (Supp. V 1981) (EO-12333) <https://fas.org/irp/offdocs/eo/eo-12333-2008.pdf>

THE WHITE HOUSE, OFFICE OF THE PRESS SEC'Y, Presidential Policy Directive, Signals Intelligence Activities, (PPD-28) (Jan. 17, 2014) <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>

United States Bills

USA Liberty Act of 2017 (H.R.3989) <https://www.congress.gov/bill/115th-congress/house-bill/3989/all-info>

USA Rights Act of 2017 (H.R.4124) <https://www.congress.gov/bill/115th-congress/house-bill/4124>

Judicial decisions

CJEU decisions

Case C/101/01 Bodil Lindqvist [2003] ECLI:EU:C:2003:596

Case C-131/12 Google Spain and Google Inc. [2014] ECLI:EU:C:2014:317

Case C-212/13 Ryneš v Úřad pro ochranu osobních údajů [2014] ECLI:EU:C:2014:2428

Case C-230/14 Weltimmo v Nemzeti Adatvédelmi és Információszabadság Hatóság [2015] ECLI:EU:C:2015:639

Case C-275/06 Promusicae v Telefonica [2008] ECLI:EU:C:2008:54

Case C-288/12 European Commission v Hungary [2014] ECLI:EU:C:2014:237

Case C-293/12 Digital Rights Ireland Ltd. [2014] ECLI:EU:C:2014:238

Case C–362/14 Maximilian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650 (*Schrems*)

Case C-465/00 Rechnungshof v Österreichischer Rundfunk [2003] ECLI:EU:C:2003:294

Case C-518/07 European Commission v Federal Republic of Germany [2010] ECLI:EU:C:2010:125

Case T-670/16 Digital Rights Ireland v European Commission [2017] ECLI:EU:T:2017:838

CJEU Opinions

Case Opinion 2/13 [2014] ECLI:EU:C:2014:2454

Case Opinion 1/15 [2017] ECLI:EU:C:2016:656

CJEU Applications pending

Case T-738/16 La Quadrature du Net and Others v Commission [2017]

ECtHR

Gaskin v UK, App.no.10454/83 (07.07.1989)

Amann v. Switzerland, App.no.27798/95 (16.02.2000)

Roman Zakharov v. Russia, App.no.47143/06 (04.12.2015)

Rotaru v. Romania, App.no.28341/95 (04.05.2000)

S. and Marper v. UK, App.no.30562/04 and 30566/04 (4.12.2008)

National case law

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht- öffentlichen Bereich (28./29.04.2010 in Hannover, Germany) <https://www.datenschutzzentrum.de/internationaler-datenverkehr/Beschluss_28_29_04_10neu.pdf>

The Irish High Court Commercial, *Data Protection Commissioner v. Schrems and Facebook Ireland*, 2016 No. 4809 P. (03.10.2017)

US Supreme Court, *Clapper v. Amnesty International*, 568 U.S. 398 (26.02.2013)

US Supreme Court, *United States v. Verdugo-Urquidez*, 494 U.S. 259 (28.02.1990)

US Court of Appeal, 9th Circuit, *United States v. Mohamud*, No. 14-30217 (05.12.2016)

Non-binding opinions

CJEU, Case C–362/14 Maximilian Schrems v Data Protection Commissioner, Opinion of Advocate General Bot [2015] ECLI:EU:C:2015:627

CJEU, Case-468/16 Maximilian Schrems v Facebook Ireland, Opinion of Advocate General Bobek [2017] ECLI:EU:C:2017:863

EDPS, Opinion 4/2016 Opinion on the EU-U.S. Privacy Shield draft adequacy decision (2016) <https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf>

The Irish High Court, EXPERT REPORT OF ASHLEY GORSKI ON BEHALF OF THE SECOND NAMED DEFENDANT (Maximilian Schrems), Record No: 2016/4809 P <https://iapp.org/media/pdf/resource_center/Schrems-testimony-Gorski.pdf>

WP29, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision (16/EN WP 238, 2016)

Communications and Reports

EC, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Rebuilding Trust in EU-US Data Flow, COM(2013) 846final

EC, 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 in the EU, COM(2013) 847

EC, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), COM(2015) 566final

EC, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117final

EC, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the first annual review of the functioning of the EU–U.S. Privacy Shield, COM(2017) 611final

EP, Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), A5-0264/2001 PAR1

EP, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, A7-0139/2014

Documents

EC, COMMISSION STAFF WORKING DOCUMENT *Accompanying the document* REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the first annual review of the functioning of the EU–U.S. Privacy Shield, SWD(2017) 344final

EC, COMMISSION STAFF WORKING PAPER The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy

Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC(2002) 196

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

Press releases

CJEU, Advocate General's Opinion in Case C-362/14 Maximilian Schrems v Data Protection Commissioner, PRESS RELEASE No106/15 (2015)

DoC, 'U.S. Secretary of Commerce Wilbur L. Ross, Jr. Addresses Department of Commerce Employees' (01.03.2017) <https://www.commerce.gov/news/secretary-speeches/2017/03/us-secretary-commerce-wilbur-l-ross-jr-addresses-department-commerce>

FTC, Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework (8.9.2017) <https://www.ftc.gov/news-events/press-releases/2017/09/three-companies-agree-settle-ftc-charges-they-falsely-claimed>

NSA, 'NSA Stops Certain Section 702 "Upstream" Activities' (28.04.2017) <https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml>

THE WHITE HOUSE, OFFICE OF THE PRESS SEC'Y, 'President Donald J. Trump Announces Intent to Nominate Personnel to Key Administration Posts' (25.08.2017) <https://www.whitehouse.gov/the-press-office/2017/08/25/president-donald-j-trump-announces-intent-nominate-personnel-key>

Secondary literature

Books

A L Bygrave, 'Data privacy law and the Internet: Policy challenges' in N Witzleb, D Lindsay, M Paterson, S Rodrick (eds.), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press: Cambridge UK 2012), pp. 259-289

A Weigend, *'Data for the People: How to Make Our Post-Privacy Economy Work for You'*, (Basic Books: NewYork US 2017)

D Chalmers et al., *European Union law* (3rd eds. Cambridge University Press: Cambridge UK 2014)

D J Solove, *Understanding Privacy* (Harvard University Press: London UK 2008)

P Hustinx, 'The reform of EU data protection: towards more effective and more consistent data protection' in N Witzleb, D Lindsay, M Paterson, S Rodrick (eds.), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press: Cambridge UK 2012), pp. 62-72

S Rodota, 'Data Protection as a fundamental rights', in S Gitwirth et al. (eds.) *Reinventing Data Protection?* (Springer 2009)

Journal Articles

CK Boone, 'Privacy and Community', *Social Theory and Practice* [1983] 9(1)

EJ Eberle, 'Human dignity, privacy, and personality in German and American constitutional law', *Utah Law Review*, [1997] Fall(4), pp.963-1056

Haller, Karnouskos and Schroth; The Internet of things in an enterprise context, *Lecture Notes in Computer Science*, [2009] 5468, pp.14-28

M Ostveen, 'Identifiability and the applicability of data protection to big data', *International Data Privacy Law* [2016] 6(4), pp.299-309

RS Gerstein, 'Intimacy and Privacy' *Ethics*,[1978] 89(1), pp.76-81

V Boehme-Neßler, 'Privacy: a matter of democracy. Why democracy needs privacy and data protection', *International Privacy Law*, [2016] 6(3), pp.222-229

W.S. Dodge, 'International Comity in American Law', *Colombia Law Review*, [1983] 115/8, pp.2071-2141

Web-resources

Associated Press, 'Raw: Snowden Sends Christmas Day Message to US' **(**25.12.2013), <https://www.youtube.com/watch?v=8iuLLkWefxs&list=PLa4kGB8ait51i52foaVvGJ7WJBpjmWl55&index=8>

A Stepanovich, 'First take on Section 702 surveillance reform: progress on human rights, but more is needed', *AccessNow* (05.10.2017) <https://www.accessnow.org/first-take-section-702-surveillance-reform-progress-human-rights-needed/>

D.B. Johnson, 'House Panel Advances FISA reform', *FCW* (13.11.2017) <https://fcw.com/articles/2017/11/13/702-judiciary-markup-johnson.aspx>

C Kuner, 'Third Country Law in the CJEU's Data Protection Judgments' *European Law Blog* (12.07.2017) <http://europeanlawblog.eu/2017/07/12/third-country-law-in-the-cjeus-data-protection-judgments/>

C Stupp, 'EU privacy watchdog: Privacy shield should be temporary', *Euractiv* (03.08.2017) <http://www.euractiv.com/section/data-protection/interview/eu-privacy-watchdog-privacy-shield-should-be-temporary/>

F Coudert, 'Schrems v. Data Protection Commissioner: A Slap on the wrist for the Commission and New Powers for Data Protection Authorities' *European Law Blog* (15.10.2015) <https://europeanlawblog.eu/2015/10/15/schrems-vs-data-protection-commissioner-a-slap-on-the-wrist-for-the-commission-and-new-powers-for-data-protection-authorities/>

G Gellman, L Poitras, 'U.S., British Intelligence mining data from nine U.S. Internet companies in broad secret program', *The Washington Post* (06.06.2013), <https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.e30ae3d5521c>

J Fioretti, 'EU privacy regulators to discuss Uber hack next week' *Reuters* (23.11.2017) <https://www.reuters.com/article/us-uber-cyberattack-eu/eu-privacy-regulators-to-discuss-uber-hack-next-week-idUSKBN1DN1X4>

J MacCrank, ‘Equifax says 15.2 million UK records exposed in cyber breach’ *Reuters* (10.10.2017) <https://www.reuters.com/article/us-equifax-cyber/equifax-says-15-2-million-uk-records-exposed-in-cyber-breach-idUSKBN1CF2JU>

K von Paczinsky, Tenczin, JEFTA: „Zweites Privacy Shield“ mit Japan in Sicht, *Internationaler Datenschutz* (21.11.2017) <https://www.datenschutz-notizen.de/jefta-zweites-privacy-shield-mit-japan-in-sicht-0119512/>

McKinsey Global Institute, ‘Digital globalization: The new era of global flows’ (February2016) < https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>

S Ackerman, ‘NSA reformers dismayed after privacy board vindicates surveillance dragnet’ *the Guardian* (02.07.2014)<https://www.theguardian.com/world/2014/jul/02/nsa-surveillance-government-privacy-board-report?CMP=ema_565>

S Lund, Susan, M James, ‘Defending Digital Globalization' *Foreign Affairs* (20.04.2017) < https://www.foreignaffairs.com/articles/world/2017-04-20/defending-digital-globalization>