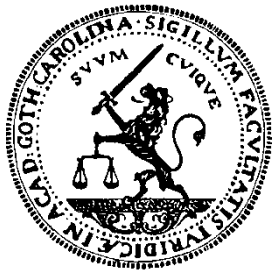

FACULTY OF LAW
Lund University

Siyuan Chen

Cross-border Data Transfer After *Schrems II*: The Globalization of EU Standards of Data Protection Through Adequacy Decisions or Trade Agreements?

JAEM03 Master Thesis

European Business Law
30 higher education credits

Supervisor: Eduardo Gill-Pedro

Term: Spring 2021

Contents

Summary

The *Schrems II* judgement delivered on 16 July of 2020 was the second time that an EU court invalidated an adequacy decision authorizing EU-US data transfer. Doubts gather around the suitability of adequacy decision being an instrument to govern cross-border data transfer. This thesis therefore wishes to explore the deficiencies of such an instrument posed by the current regime as established in the GDPR—which is to find adequacy.

This thesis finds that the requirement of finding adequacy, as stipulated by the GDPR and case law in light of the Charter, is a unilateral finding and may face the hard truth that there simply could not be such a finding in the US. Under the current US legal system, the disparity between the EU's approach to protection of personal data and that of the US remain fundamentally great. What's more, the national security grounds on which access to personal data by public authorities is authorized under US law, pose unacceptable interference to the fundamental rights of privacy and data protection of the EU data subjects, which would not be allowed under EU law.

Besides finding the legal requirements of adequacy finding from the GDPR and case law, this thesis also examines the adequacy decision regarding data transfer to Japan. Although that adequacy decision generally fulfils the legal requirements, there exist flaws and possible objections to such an adequacy finding in Japan. The Commission's approach to adequacy decision therefore seems to regard it as a tool for facilitating trade and risks making it merely a "formality".

This thesis also tries to evaluate the possibility of using trade agreements to govern cross-border data. The advantages of trade agreement compared with adequacy decision as an instrument to govern cross-border data transfer are explained but also the shortcomings and difficulties of it are exposed. Adequacy decision is beneficial to the global promotion of EU standards of data protection, to which the adequacy decision regarding data transfer to Japan is an example. However, with no international consensus, this thesis acknowledges the difficulty of ensuring the level of protection after personal data crosses borders and balancing fundamental rights with the interest of trade in a global trade context. Still, this thesis submits that the insistence on the use of adequacy decision as an instrument to govern cross-border data transfer should uphold the level of protection guaranteed by EU law.

Acknowledgement

I would like to thank first Eduardo Gill-Pedro, my supervisor, for his opinions and explanations on all the points which I harbour doubts about, and his guidance on this thesis throughout the whole process. Without him, this thesis would not be possible.

I would also like to thank Lund University for offering me both the opportunity and the scholarship to study the European Business Law program. And great thanks to all the teaching stuff at the faculty of law, for sharing with us all the knowledge and inspirations.

I would like to thank of course, my sister, my parents and all my loved ones, for always being there and supporting me along the way.

Siyuan Chen

Lund, Sweden

Abbreviations

APPI	the Act on the Protection of Personal Information
CJEU	The Court of Justice of the European Union
CFSP	Common Foreign and Security Policy
Data Protection Directive (DPD)	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31
EU	European Union
FISA	Foreign Intelligence Surveillance Act
FTA	Free Trade Agreement
GDPR	General Data Protection Regulation; 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 [2016] OJ L119/1
PPC	the Personal Information Protection Commission
Privacy Shield Decision	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 [2016] OJ L207/1

Safe Harbour Decision	Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce OJ L 215, 25.8.2000, p. 7–47
Schrems II	Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd* [2020] ECLI:EU:C:2020:559
Shrems I	Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650
TEU	Treaty of the European Union
TFEU	Treaty of the Functioning of the European Union
TTP	The Trans-Pacific Partnership
US	United States
WTO	World Trade Organization

1 Introduction

1.1 Background

1.1.1 Schrems II

On 16 July of 2020, the Court of Justice of the European Union (CJEU) delivered a judgement[1] striking down the Privacy Shield framework which authorizes the data transfer between the EU and the US. It came as the second time an EU court invalidated the Commission's adequacy decision authorizing EU-US data transfer. Although having made a lot of changes to bring the framework into compliance with the Court's decision in *Schrems I* after the Safe Habour was stricken down, the Commission failed again with the invalidation of the Privacy Shield Decision, only 4 years after its adoption. In its judgement, the Court invalidated that decision on the ground that the Commission disregarded the requirements under Art 45(1) of GDPR read in light of Art 7, 8 and 47 of the Charter.

The central point that the Court made was that the exceptions made in that decision to the Privacy Shield Principles, especially considering the surveillance program adopted, were not circumscribed in a way that satisfies the requirements of Article 52 of the charter when interfering with fundamental rights and that the right to effective remedy before a tribunal was violated under the mechanism designed by such a framework. Thus an equivalence to the protection guaranteed by EU was not found in the US, which contradicted the conclusions made by the Commission in its decision.

1.1.2 Data transfer between the EU and the US

Since the emergence of the Internet, the data flows across the Atlantic have increased. While there is a lack of the reports on the exact volume of data transfers, the importance of EU-US data transfers can be seen from the fact that EU is the largest digital trade partner and hundreds of billions of digitally delivered services were exported into the EU from the US.[2] And over 40% of data flows between the EU and the US are through the networks of business and research.[3] The large volume of data exchange across the Atlantic has served millions of Internet users and business from both sides have been using the 'bridge' to expand their service outside their own borders. However, the collection of data from millions of users by business outside the EU has raised enormous concerns over the safety and

---

[1] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd* [2020] ECLI:EU:C:2020:559.

[2] Oliver Patel and Nathan Lea, 'EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows' (UCL European Institute Policy Paper 2020), 10 <https://iapp.org/media/pdf/resource_center/eu_us_privacy_shield_brexit_data_flows_uclei_june_2020.pdf> accessed 26 March 2021.

[3] Congressional Research Service, 'Digital Trade and U.S. Trade Policy' (2017), 20 < https://epic.org/crs/R44565.pdf> accessed on 26 March 2021.

privacy of such business practice, especially in light of some serious data security breaches[4] and the disparity of the data protection regimes and approaches between the EU and the US.[5]

Take social media in the EU for example. According to Statcounter,[6] from February 2020 to February 2021, Facebook accounted for 79.73% of the market of social media, with Pinterest, Twitter, Instagram and YouTube taking up most of the rest. All of these companies are from the US and together they took away over 99% of the Market. For Google[7] and Facebook[8] it is common practice that their users' data would be transferred back to the US, where their servers are located, to be processed. This is an essential part of their global service, without which users could not make use of the full functions of their service.

The close trading partnership of the EU and the US determines that the channel for data transfers between the two regions must be open for the purpose of trade facilitation and from the perspective of customer welfare. But nevertheless, the concerns of privacy and data protection should be addressed to ensure the integrity and lawfulness of such data transfers.

The EU has made several attempts to regulate EU-US data transfers.

In 1995 Data Protection Directive[9] was adopted and Article 25 and 26 concerns the principles and derogations regarding the requirements for the 'transfer of personal data to third countries.' Article 25 of Data Protection Directive allows transfer of personal data to third countries only if the third country ensures an 'adequate' level of protection, which is to be decided by the Commission after assessment in accordance to the requirements from the directive, or where in the case of absence of such an adequacy decision, adequate safeguards are provided by the controller with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.

---

[4] Nicholas Confessore, 'Cambridge Analytica and Facebook: The Scandal and the Fallout So Far' *New York Times* (New York, 4 April 2018) < https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html> accessed 19 May 2021; Julia Carrie Wong and Kari Paul, 'Twitter hack: accounts of prominent figures, including Biden, Musk, Obama, Gates and Kanye compromised' *The Guardian* (London, 16 July 2020) < https://www.theguardian.com/technology/2020/jul/15/twitter-elon-musk-joe-biden-hacked-bitcoin> accessed 19 May 2021.

[5] Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) ch 2.

[6] Statcounter, 'Social media stats in Europe - April 2021' < https://gs.statcounter.com/social-media-stats/all/europe> accessed 26 March 2021.

[7] 'Google privacy& terms' <https://policies.google.com/privacy/frameworks?hl=en> accessed 25 March 2021.

[8] 'Facebook data policy' <https://www.facebook.com/about/privacy/update> accessed 25 March 2021.

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

Safe Harbour Decision

With the power conferred upon, the Commission in 2000 took action with US authorities to build a certification regime for US companies to legally transfer data from the EU back to the US by adopting the Implementing Decision 2000/520.[10] It was the first adequacy decision made with the United States. Under this so-called 'Safe Harbour' framework, business and organisations can self-certify to the Department of Commerce of the US its adherence to the 'Safe Harbour Privacy Principles' and data transfers under this regime will be deemed to have met the requirements of 'providing adequate level of protection'. The Safe Harbour Privacy Principles include the seven principles of notice, choice, onward transfer, security, data integrity, access and enforcement. By the year of 2013, over 3000 organizations including both small and big companies have listed as certified under the Safe Harbour.[11] The Safe Harbour regime was criticized for its reliance on the voluntary adherence and the self-certification of the certified companies and the enforcement commitments by public authorities.[12] It was indeed found by the Commission itself to be flawed in terms of enforcement of those principles.[13] However, it still functioned as the most important vehicle for EU-US data flows of personal data and relied on by thousands of companies, until it was invalidated by the CJEU in 2015.

Schrems I

In 2013, Mr. Maximillian Schrems, an Austrian Facebook user, lodged a complaint to the Commission asking for prohibition of Facebook Ireland from transferring his personal data to the United States where the servers of Facebook Inc. were located. The complaint was later rejected as unfounded, against which Mr. Schrems brought an action in Ireland, which was then referred to the Court of Justice for a preliminary ruling. The Court first answered the question regarding the power conferred to the national data protection authorities. After concluding that an adequacy decision shall not prevent the national supervisory authorities from examining the validity of such a decision while only an EU Court can declare it to be invalid, the Court itself went on to examine the validity of Decision 2000/520 Safe Harbour Decision.

In its judgement,[14] the Court first interpreted the term 'adequate level of protection' to mean 'essentially equivalent to that guaranteed within the

---

[10] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7 (Safe Harbour Decision).
[11] Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU COM(2013) 847 final, 4.
[12] ibid 5.
[13] ibid 17.
[14] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.

European Union' and confirmed that the discretion of the Commission is reduced and the review of the requirement stemming from the Directive 95/46 should be strict. The Court then went on to find that the general nature of the derogation, which laid down in Decision 2000/520 the primacy of 'national security, public interest, or law enforcement requirements' over the safe harbour principles, substantiated that the interference to fundamental rights thus established was not restricted in a way that is essentially equivalent to that in the EU legal order and would compromise the essence of the fundamental right to respect for private life. The same conclusion was reached to the right to effective remedy before a tribunal since no possibility to pursue legal remedies was provided for the individuals to access, rectify, or erase the data relating to them. It was concluded that the Commission failed to comply with the requirements from the Directive, read in light of the Charter. The Court also found that the Commission had exceeded its power by restricting the national supervisory authorities' powers in Decision 2000/520. Decision 2000/520 was therefore found to be invalid.

Privacy Shield Decision

Based on *Schrems I* and under the pressure from Member States to initiate a new framework for EU-US data transfer to be authorised,[15] the Commission in 2016 negotiated the Privacy Shield Framework with the US authorities and made substantive changes compared with the Safe Harbour regime in line with Union legislation and Court judgements. Later the Commission adopted Decision 2016/1250[16] and decided again that the US ensure an adequate level of protection while preserving the self-certification programs.

The new privacy shield principles involve many changes compared with the previous Safe Harbour Decision to address the concerns from the Commission itself and the Court of Justice in *Schrems I*. The changes include the US government's commitments on ensuring that access for national security and law enforcement purposes to data transferred to the US is subject to clear limitations, safeguards and oversight; the creation of an Ombudsperson responsible for following up the complaints and enquiries by EU individuals; the enhancement of the role of EU DPAs. There are also more commercial and compliance-focused changes, including rules regarding onward transfer to third parties and compliance monitoring. The redress options under Privacy Shield are also widely expanded to ensure the effective remedies for data subjects whose data is being transferred.[17] However, the derogation from the privacy shield principles was maintained.

---

[15] Christian Schröder and others, 'German DPAs Add Further Pressure to E.U.-U.S. Data Transfers' (2016) 28(1) IPTLJ 17.

[16] 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 [2016] OJ L207/1 (Privacy Shield Decision).

[17] Rosemary Jay, *Guide to The General Data Protection Regulation: A Companion to The Data Protection Law and Practice* (Sweet and Maxwell 2017) 147-53.

The adherence to these principles is still limited to the extent necessary to meet the need for national security, public interest or law enforcement requirements.[18] At the time of the third annual review of Privacy Shield by the Commission, over 5000 companies had participated in this mechanism.[19]

1.2 Purpose and research questions

Faced with the second failure and considering the importance of keeping the convenient tunnel for businesses to transfer data across the Atlantic, the Commission might take a third attempt to make an adequacy decision for the data transfer to the US. The aim of this thesis is to find out whether the incompatibilities found by the Court of Justice in both *Schrems* judgements, of the adequacy decisions regarding data transfer to the US, with existent legal requirements can be reconciled and what these incompatibilities suggest about adequacy decision as an instrument to govern cross-border data transfer, especially compared with the potential alternative of trade agreement. With regard to the current situations and the previous failures, the questions should therefore be summarized as:

1. What are the issues identified by the Court to be incompatible with existing legal requirements in the *Schrems* judgements and is it possible for the EU and the US to find common grounds for a solution under the mechanism of adequacy decision to authorize EU-US data transfer?

2. What deficiencies have been exposed of adequacy decision as an instrument to govern cross-border data transfer, and are trade agreements, the potential alternative instrument, better to guarantee the level of protection of personal data transferred internationally?

1.3 Methodology and materials

In order to answer the above questions, several methods shall be adopted to conduct research and reasoning. First, a legal dogmatic method is employed to the identification, interpretation and application of the relevant legal principles and requirements which are necessary to maintain compliance of adequacy decision for EU-US data transfer. Secondly, a comparative method is applied to the examination of the adequacy decision regarding data transfer to Japan under similar requirements applied in *Schrems* judgements and also, to find out the advantages and deficiencies of adequacy decision as an instrument to govern cross-border data transfer, after comparison with the potential alternative of trade agreements.

---

[18] Privacy Shield Decision, Annex II I.5.

[19] Report from The Commission To The European Parliament And The Council on the third annual review of the functioning of the EU-U.S. Privacy Shield COM(2019) 495 final <https://ec.europa.eu/info/sites/default/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf> accessed 13 May 2021.

Most of the materials used are case law, legislations, Commission working documents, books and journals about adequacy decision and data protection law. International agreements are also used. Press statements, statistics, guidelines and working papers from some organizations are also cited.

1.4 Outline

The first chapter gives an introduction to the background of two adequacy decisions invalidated by the Court and the purpose and methodology of this thesis.

The second chapter starts with the Internal Market and the appropriation of laws in terms of the free movement of personal data within the EU, and proceeds with the Common Commercial Policy and the developments of digital trade, in order to locate the position of data protection regime in the EU legal order and characterize the nature of adequacy decision.

The third chapter focuses on adequacy decision as an instrument to govern cross-border data transfer, identifying and analysing the legal requirements stemming from the GDPR and the Charter based on the Court judgements, as well as with the assessment of the possibility of reconciling the incompatibilities found and summarizing the deficiencies of this instrument.

The fourth chapter examines the adequacy decision with regard to data transfer to Japan under requirements similar to those applied to the decisions with regard to data transfer to the US, providing more perspectives as to the approach to adequacy decision by the Commission and the implications for the development of a sustainable authorization mechanism for cross-border data transfer.

The fifth chapter gives more insights to the task of adequacy decision and the dilemma the globalisation of EU standards faces, by comparison between the two instruments of trade agreements and adequacy decision. Both benefits and difficulties of trade agreement as an instrument are assessed and evaluated. The limitations of using adequacy decision to globalise EU standards of data protection and the hesitancy of the EU to use trade agreement as an instrument are discussed.

2 Internal Market and Cross-border Data Transfer

2.1 Internal market and data privacy

The Treaty of Rome[20] created the Common Market intended to contribute to 'establish the foundations of an ever closer union among the European peoples'. Article 3(3) of the Treaty of the European Union and Article 4(2)(a) of the Treaty of the Functioning of the European Union provide that the EU should establish an internal market. It is stipulated that the internal market should 'comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties'. With the technological development and the emergence of the Internet, and under the rapid change resulting therefrom to the way of conducting trade and business around the globe, the Union has realized the importance of ensuring the free movement of data in order to better achieve the four freedoms of the internal market. Thus, when adopting the Data Protection Directive, it was first established that the directive had as its objective that the free flow of personal data between Member States should not be restricted or prohibited for reasons with the protection of privacy and personal data.[21] Whilst under the age of big data, data has not only been a vehicle facilitating trade and business but itself has become a valuable resource,[22] the economic gains from ensuring the free movement of data are obviously one of the policy drives behind the regulations of data processing.

However, the Data Protection Directive also had as its objective to protect the fundamental rights and freedoms of natural persons. In fact, after the Treaty of Lisbon entered into force, Article 16 of TFEU provides that everyone has the right to protection of personal data concerning them. Repealing the directive, GDPR now refers directly to the right to protection of personal data.[23] In practice, the processing of personal data concerns interference with Article 7 and 8 of the Charter of Fundamental Rights and Freedoms of the European Union (the Charter)—the right to respect for

---

[20] Treaty establishing the European Economic Community.

[21] Data Protection Directive, art 1(2); GDPR, art1(1).

[22] 'The world's most valuable resource is no longer oil, but data' *The Economist* (London, 6 May 2017) < https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 27 March 2021.

[23] Data Protection Directive, art 1(1)
In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
Also, GDPR, art 1(2)
This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

private and family life and the right to protection of personal data.[24] EU data protection law therefore purses dual objectives,[25] of which the economic one is to contribute to 'the accomplishment of an economic union, the economic progress and the strengthening and the convergence of the economies within the internal market', while the other right-based objective is to 'accomplish an area of freedom, security and justice and promote social progress and the well-being of natural persons' .[26] And while the internal market objective was initially predominant, the fundamental right objective have been given a marked emphasis in the EU's data protection regime.[27]

2.2 Common commercial policy and cross-border data transfer

After two decades of harmonisation and as a response to criticism of the lack of uniform enforcement by the Member States of the Data Protection Directive, the GDPR now unequivocally states that 'the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data', again reaffirming the free movement of data within the internal market. Since the barriers within the internal market were eliminated and there is now a common market also for the movement of personal data, it is natural that there should also be a common policy or position from the EU with regard to the data movement to third countries, i.e. a concerted position and action led by the EU and supported by the Member States to interact with the outside world. Moreover, it follows from the fact that EU users' data is transferred back to the servers located in the United States where a large amount of the digital services in EU comes from, that there is a genuine and urgent need for data transfer across the Atlantic, which compels the EU to engage with the US government to create a better solution or channel for such transfer to be done. Such engagement with certain third countries raises the question whether it should be based on the EU's competence of external relations, in particular, the Common Commercial Policy.

It is to be remembered that the internal market is not an enclosed one. The EU needs to trade with the outside world and thus adopts a Common

---

[24] Charter of Fundamental Rights of the European Union [2012] OJ C326/391 art 7: Everyone has the right to respect for his or her private and family life, home and communications.
art 8: 1 Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.
[25] Lynskey (n 5) 46.
[26] GDPR, recital 2.
[27] Lynskey (n 5) 75.

Commercial Policy. Article 3(1) of TFEU states that the Common Commercial Policy is one of the exclusives competences of the EU. Article 207(1) maintains that the Common Commercial Policy shall include trade in goods and services, the commercial aspect of intellectual property and foreign direct investment, etc. Recital 101 of GDPR acknowledges the necessity of the exchange of personal data between the EU, and third countries and international organizations, for the expansion of international trade and international cooperation.

It is important to notice that the scope of Common Commercial Policy has not been explicitly to cover engagement with third countries regarding data protection. However, the possibility of addressing data protection matters under external relations competence can be discovered from the Court's opinion on the Passenger Name Record (PNR) agreement with Canada.[28] The PNR agreement was found by the Court to have two components including one relating to the necessity of ensuring public security and the other to the protection of PNR data, the latter of which was decided to be based on the legal basis of Article 16(2) TFEU after acknowledging that the transfer of personal data such as PNR data to Canada should take place only if an adequate level of protection is found. Thus, international agreement can be adopted by the EU on the basis of data protection and there have been precedents regarding PNR data. Although the scope of Common Commercial Policy has not yet been extended by the Court or Union law to cover cross-border transfer and in fact even if it did, it would focus more on the commercial side i.e., business and trade instead of data protection only, the agreements[29] signed by the EU regarding PNR data have proved that it is possible for data protection to form a legal basis for the external actions by the EU. The emergence and continuous development of digital trade could increase such possibility, which is to be illustrated in *Section 2.3*.

2.3 The regime for regulating cross-border data transfer

Before we dive into the specific rules concerning cross-border data transfer, it is first of all necessary to discuss which legal basis enables the EU's regulation on cross-border data transfer—the implied power from internal market, the Common Commercial Policy or the Article 16 TFEU itself.

2.3.1 The source from primary law

Article 16(1) of TFEU provides that everyone has the right to the protection of personal data concerning them. Article 16(2) compels the European Parliament and the Council to lay down rules relating to the protection of

[28] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017 [2017] ECLI:EU:C:2017:592.
[29] PNR is an area of data protection in which the EU has concluded agreements with several countries. Existent active agreements including the ones with the United States and Australia.

individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies and by the Member States when carrying out the activities which fall within the scope of Union law. However, Article 16(2) also provides that 'the rules…should be without prejudice to the specific rules laid down in Article 39 of the Treaty of the European Union'. Article 39 of TEU, which stems from the provisions of the Common Foreign and Security Policy (CFSP), gives a derogation to Article 16(2) TFEU by laying down specific rules for the processing of personal data by Member States carrying out activities which fall within the scope of CSFP. This constitutes what some describe as '*de facto* differentiated application of EU data protection rules to public and private sectors',[30] substantiated by the existence of both the GDPR and the Data Protection Law Enforcement Directive[31]. As Recital 1 of the GDPR suggests, the legal basis of the data protection regime except the rules under CFSP, is to be based on Article 8 of the Charter and Article 16 of TFEU.

2.3.2 From the Data Protection Directive to the GDPR

However, it is to be noted that GDPR repealing the Data Protection Directive, also signals a fundamental change in the legal basis of the rules regarding data protection. Whilst the Directive was based on Article 114 of TFEU and thus needed, according to that provision, 'to have as its object the establishment and functioning of the internal market', the GDPR based on Article 16 of TFEU is however, not reliant on the market integration legal basis. Since now the Directive has been repealed and the Regulation is in place basing itself on an independent legal basis stemming from the primary law of the EU, it is therefore understandable that the CJEU's approach to the interpretation of data protection rules has also moved from prioritizing market integration to placing equal footing on the dual objectives of data protection regime, which include both economic and right-based ones[32].

2.3.3 Digitalisation of trade and trade agreements

Although the above observations might lead to the conclusion that the present data protection regime is solely based on Article 16 of TFEU, there are new developments in trade and trade negotiations which might in the foreseeable future, provide new vehicle for cross-border data transfer to be authorised.

Digital trade is commonly agreed to 'encompass digitally enabled transactions in trade in goods and services that can be digitally or physically

---

[30] Lynskey (n 5) 18.
[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 L119/89.
[32] Lynskey (n 5) ch 3.

delivered'.[33]Not only can data flows serve the traditional trade in goods and services, but itself can be the component of international trade.[34] Cross-border data flows, which have increased 45 times since 2005, has become part of, and integral to digital trade which has accounted for around 3.5% of total world GDP.[35]Digitalisation, which enables and requires cross-border data flows, has played an important role in facilitating the cross-border movement of goods, services, people and finance. And trade agreements pursue eventually the same outcome.

Such digitalisation has also raised serious privacy and data safety concerns with data crossing different jurisdictions, propelling trade partners all over the world to seek a bilateral or multilateral solution to safeguarding data flowing out of its own country. EU is now trying to add a digital trade title into the trade agreements it is negotiating, under which lies the provisions on cross-border data flows and data protection, in order to address the vibrant and stark development of the digitalisation of trade.

One of the examples of the trade agreements including clauses regulating cross-border data flows is the EU's proposal of provisions in the trade negotiations with Indonesia. [36]The proposal would contain two main elements. One is to adopt a horizontal approach and address the restrictions that may impede data flows such as data localization, and the other is to ensure the safeguard of privacy and data protection and the transparency from both sides.[37]Such kind of proposal was also made by the EU in the trade negotiations with Tunisia.[38]

Therefore, it seems that trade agreements have the potential to become a powerful instrument for regulating cross-border data flow. In that case competence of external actions of EU may have the possibility to serve as the basis for regulating data transfer to third countries, if the agreements

---

[33] OECD, 'Trade in the Digital Era' (2019) OECD Going Digital Policy Note <www.oecd.org/going-digital/trade-in-the-digitalera.pdf.> accessed 12 May 2021.
[34] Habib Kazzi, 'Digital Trade and Data Protection: The Need for a Global Approach Balancing Policy Objectives' (2020) vol 4 iss 2 EJELS 42.
[35] ibid 45.
[36] EU provisions on Cross-border data flows and protection of personal data and privacy in the Digital Trade Title of EU trade agreements, explanatory note-July 2018, 5th Round of Trade Negotiations between the European Union and Indonesia. <https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157129.pdf> accessed 21 April 2021.
[37] EU proposal for provisions on Cross-border data flows and protection of personal data and privacy <https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf> accessed 21 April 2021.
Also, Francesca Casalini and Javier López González, 'Trade and Cross-Border Data Flows' (2019) OECD Trade Policy Papers, 27 <https://doi.org/10.1787/b2023a47-en.> accessed 12 May 2021.
[38] EU Proposal for a Digital Trade Title, explanatory note-January 2019, Negotiations on a Deep and Comprehensive Free Trade Agreement (DCFTA) between the European Union and Tunisia. <https://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157646.01.24%20-%20Factsheet%20-%20Digital%20Trade%20EN%20.pdf> accessed 21 April 2021.

reached could be relied on to achieve a mutual recognition of adequacy or equivalence enabling such transfer, i.e. going beyond than simply stating that "each party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data" as in the proposal texts.

2.3.4 The per se nature of the 'adequate level of protection' requirement

Now let us turn back to the requirements of adequacy protection in the GDPR concerning the data transfer to third countries. As one of the solutions to provide the equivalent protection guaranteed by EU law for data subjects when data is transferred to third countries, adequacy decision compels the Commission to engage with the third country in question and adopt such decisions after conducting an assessment required by law. Such engagement, in whatever form it may take, therefore involves the external actions of the European Union, at least in a general and non-binding sense.

The adequacy decision, however, involves only the finding by the EU of the adequate level of protection by the third country for personal data transferring from the EU to that country. The adequacy decision is itself adopted only by the EU and binding only on the Member States and EU institutions, while the adoption of such a decision may come after the third country has made substantial arrangements and commitments in its own legal order to qualify for an adequate finding, as in the case of the Privacy Shield Decision concerning the US and the adequacy decision concerning Japan. But formally there was never an international agreement achieved and the trade aspect of data transfer crossing borders is never a requisite for the transfer under an adequacy decision to take place.[39]

Therefore, without GDPR explicitly referring to any other objectives or legal instruments, it cannot be concluded that the specific rules of data transfer to third countries are based on the Common Commercial Policy or other legal basis. They are, instead, based on Article 16 of TFEU, an independent legal basis for data protection from the primary source of EU law.

---

[39] Most of the adequacy decisions were adopted after reaching a political agreement with third countries. Such political agreement has brought about data protection commitments from third countries and then the recognition of equivalence through adequacy decisions. See Communication from The Commission to The European Parliament and The Council Exchanging and Protecting Personal Data in a Globalised World COM (2017) 7 final (2017 Communication), 9 and footnote 42. An adequacy finding is a unilateral implementing decision by the Commission in accordance with EU data protection law, based on the criteria therein. The EU data protection rules cannot be the subject of negotiations in a free trade agreement.

2.4 The balance between data movement and fundamental rights

The Court has always stressed the importance of ensuring a fair balance between the observance of fundamental rights and the interests requiring free movement of personal data.[40]

The Court has previously ruled that it is the objective of Directive 95/46 (DPD) to ensure the free movement of personal data between the Member States, which is necessary for the establishment of and the functioning of the internal market.[41]And in fact in *Rundfunk*, the free movement of personal data was even stated as the directive's principal aim. Lynskey held that despite the court's initial emphasis on market integration due to Article 114 TFEU being the legal basis of the directive and the Charter's lack of binding force, there have been in recent years equal emphasis on fundamental rights, especially after the entry into force of the Lisbon Treaty.[42]Now the GDPR has vowed to respect fundamental rights and freedoms and is based on Article 16 of TFEU, which mandates a directly effective right to the protection of personal data, corresponding to the fundamental right to the protection of personal data in the Charter. And the emphasis on fundamental rights in data protection can be even better substantiated by the fact that the Court has overturned two adequacy decisions on the grounds of incompatibility with requirements of fundamental rights.

It is yet not clear whether, as regards the transfer of data to third countries, the EU is willing to extend the promise of free movement of data to international circumstances. Indeed, there seems to be no sign that such principle is explicitly upheld with regard to the data movements between the EU and places outside the Internal Market. Neither the directive or the later GDPR mandates such a principle for the free movement of personal data outside the internal market, and instead they made use of the term "only if" when stipulating the circumstances where such a transfer is allowed, implying that both placed a general prohibition for transfer of personal data from EU data subjects to third countries or international organisations. This is of course a reasonable ban since the personal data which would leave the jurisdiction of EU law should definitely not be presumed to continue enjoying the protection from EU law and thus, enter into an unknown space where it is unsure whether that level of protection under EU law will still be maintained.

However, in the case of transfer to third countries, even without an explicit principle of free movement of data, will the interests for promoting or facilitating cross-border data movement be strong and urgent enough to be

---

[40] *Schrems I*, para 42; Case C-518/07 *Commission v Germany* [2010] ECLI:EU:C:2010:125, para 24.
[41] *Commission v Germany* [2010], para 20; Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECLI:EU:C:2003:294, para 70.
[42] Lynskey (n 5) 62-3.

balanced against the fundamental right to protection of personal data? The answer is that it could be, and this could be drawn from what is happening in both international trade and international data protection cooperation.

This question shall be further explained in *Section 5*. But right now, it is first necessary to review the shortcomings of adequacy decision in fulfilling its intended objectives as an instrument to regulate cross-border data transfer.

3 Adequacy decision

This section and *Section 4* concerns only adequacy decision. This section seeks to find out and summarize the legal requirements of adequacy decision stemming from the GDPR and the case law (*Section 3.1*), and then identify the issues incompatible with the requirements and assess whether they are reconcilable given the circumstances from the EU and the US (*Section 3.2*). The deficiencies of adequacy decision as an instrument to govern cross-border data transfer are discussed in both *Section 3.3* and after comparison with the decision regarding data transfer to Japan, *Section 4*.

3.1 Adequacy to be found

The rules governing data transfer to third countries are laid down in Chapter V of GDPR. Article 44 of GDPR provides a general prohibition on data transfer to third countries, unless the conditions set in the GDPR are complied with. Data transfer to a third country may take place where the Commission has decided that the third country ensures an adequate level of protection[43], or where, in the absence of such an adequacy decision, appropriate safeguards have been provided by the controller or processor,[44] which can take different forms as listed in Article 46(2) of GDPR, including binding corporate rules[45] and standard contractual clauses.[46] In the case where there is neither an adequacy decision nor appropriate safeguards, derogations are also provided from the general prohibition, based on conditions under Article 49(1), including conditions where there is explicit consent from data subjects and where there is necessity for the performance of a contract.

Therefore, it is important to note that adequacy decision is not the only way under EU data protection regime for data transfer to a third country to be authorised. However, it remains the most powerful and convenient way to authorise cross-border data transfer since the effect of that decision usually benefits all the data transfers by business from the whole territory of that third country, unlike other instruments, by which data transfers can only be achieved on a case-by-case basis.

---

[43] GDPR art 45.
[44] GDPR art 46.
[45] GDPR art 47.
[46] For standard contractual clauses (SCC), there are decisions which issued the sets of SCCs: Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [2001] OJ L181/19; Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries [2004] OJ L385/74; Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council [2010] OJ L39/5.

The approach taken by the Commission to develop adequacy decisions is to actively engage with key trading partners and establish dialogue and close cooperation with the concerned third country. Before starting a dialogue with a third country, the Commission takes into account the EU's commercial relations with the third country, the extent of personal data flows, the pioneering role that country plays in the field of privacy and data protection and also the overall political relationship with that country.[47]

3.1.1 Essentially equivalent

As to the legal requirements stemming from both the GDPR, the Charter and the case-law, it is first of all to be noted that the requirement laid down in Article 45 of GDPR that the third country ensure an adequate level of protection does not require the country to ensure identical level of protection to that guaranteed by the EU. The term 'adequate level of protection' should be construed to mean that a level of protection of fundamental rights and freedoms that is '*essentially equivalent*' to that guaranteed within the EU in light of the Charter[48]. And although it is incumbent upon the Commission to make the assessment under Article 45(2) of GDPR and decide accordingly, whether to find the existence of adequate level of protection or not, the Commission's discretion is limited and subject to strict review.[49]

The Commission should in its assessment of the adequate level of protection, take into account the elements stated in the paragraph 2 of Article 45 of GDPR. Part a of that paragraph is most noteworthy, for it includes the elements, *inter alia*, (i) the rule of law and respect for human rights and fundamental rights, (ii) relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, and (iii) effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred. The appraisal of these elements in a third country must also be compatible with the protection of fundamental rights and freedoms, as the Court in both the *Schrems I* and *Schrems II* judgements affirmed[50]. When reviewing the validity of an adequacy decision, the Court shall examine whether such a decision complies with the legal requirements stemming from the GDPR read in light of the Charter[51]. In particular, Article 7, 8 and 47 of the Charter are the most important yet most problematic to comply with.

3.1.2 Article 7& 8 of the Charter

As both judgments have confirmed, the derogation based on the grounds of national security, public interest, or law enforcement requirements, etc., set

---

[47] 2017 Communication(n 39), 8.
[48] *Schrems I*, para 73.
[49] *Schrems I*, para 78.
[50] *Schrems I*, para 59; *Schrems II*, para 158.
[51] *Schrems II*, para 161.

out in both adequacy decisions[52], enables interference with the fundamental rights of data subjects whose data is transferred from the EU to the US[53]. And also, the communication of personal data to a third party constitutes an interference with fundamental rights enshrined in Article 7& 8 of the Charter[54]. The right to privacy and the right to protection of personal data are not absolute rights and they should be considered in relation to their function in society. However, the derogations and limitations in relation to the protection of personal data must be strictly necessary. Moreover, Article 8(2) of the Charter requires that 'such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law' and that 'everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'. And as stipulated in Article 52(1) of the Charter, any limitation to the fundamental rights and freedoms must be 'provided for by law and respect the essence of those rights and freedoms'. And subject to the principle of proportionality, they should also meet the requirements that 'they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.

It should be noted first, that the requirement of limitation being provided for by law implies that 'the legal basis which permits the interference with fundamental rights must itself define the scope of the limitation on the exercise of the right concerned.[55] And also the Court has ruled that access to personal data on a generalised basis by the public authorities is itself regarded as compromising the essence of the right to privacy enshrined in Article 7 of the Charter.[56]

And as regards the requirement of proportionality, it is settled case-law that the legislation permitting the derogations and limitations and entailing interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.[57]

3.1.3 Article 47 of the Charter

Article 45(2) of GDPR unambiguously requires that the Commission, when assessing the adequate level of protection, shall take into account effective

---

[52] Safe Harbour Decision (n 10) 10 Annex I.
[53] *Schrems I*, para 87; *Schrems II*, para 165.
[54] *Schrems II*, para 171.
[55] *Opinion 1/15*, para 139.
[56] *Schrems I*, para 94.
[57] *Opinion 1/15*, para 140-41.

and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred (element *iii* in section 3.1). Article 47 of the Charter also states that everyone has the right to an effective remedy before a tribunal when his rights and freedoms are violated and that everyone is entitled to a hearing by an independent and impartial tribunal.

Due to the clear contribution of Article 47 of the Charter to the level of protection in the EU, which is recognized by the Court, this article also needs to be complied with when the Commission adopts an adequacy decision pursuant to Article 45 of the GDPR.[58] The Court also stressed that the essence of the fundamental right to effective judicial protection enshrined in Article 47 of the Charter is not respected when individuals are not granted the possibility to pursue legal remedies in order to gain access to, or to obtain the rectification or erasure of personal data relating to him or her. The very existence of this right is inherent in the existence of rule of law, which is also an essential element in the assessment of adequacy.[59] Thus the appraisal or examination of whether any mechanism could be regarded as affording judicial protection compliant with Article 47 of the Charter should start from the premiss that such possibility is provided for the data subjects to bring legal actions.[60]

3.2 Adequacy to uphold

These requirements stemming from the treaties, regulations and case-law are the key to the legality of adequacy decisions. However, in the particular case of EU-US data transfer, it is by no means easy to comply with. The specialties of the US data protection regime and its approach to the regulation of public access to personal data proved the difficulties of finding a European-kind adequacy. Although adequacy decision partly wants to attract other countries to adopt the same standards—spreading the "Brussels effect",[61] the failures by the Commission could present an intrinsic conflict that might be prevalent in the instrument of adequacy decision as a vehicle for such purpose, compromising its most fundamental goal.

3.2.1 The "inadequate" adequacy

The adequacy of the level of protection found twice in the Commission's decisions to authorise the transfer of personal data from the EU the US turned out to be inadequate. They were stricken down by the Court mostly due to their incompatibility with the fundamental rights requirements inherent in the required finding of adequacy.

---

[58] *Schrems II*, para 186.
[59] *Shcrems II*, para 187.
[60] *Schrems II*, para 194.
[61] Anu Bradford, 'The Brussels Effect' (2012) 107(1) NULR 1.

It was found by the Court, as regards the Safe Harbour Decision, that it was the self-certified US organisations instead of the US public authorities that were required to comply with the safe harbour principles. The decision also contains a derogation based on national security and public interests which permits on a generalised basis, the storage of personal data and the access by public authorities to such data, whilst no finding of the rules from the US sides intended to limit such interference with the fundamental rights resulted from this derogation and also no possibilities which provide data subjects effective legal remedies against the interference of such kind. Thus an equivalence of the level of protection cannot be found without breaching the requirements under the GDPR in light of the Charter.

The Privacy Shield Decision made substantive changes in order to ensure compliance, which are shown in section 1.1. However, these changes were still not enough. The Court first found that the same kind of derogation based on national security and public interest set out in the Privacy Shield Decision would mean that, Section 702 of the FISA (Foreign Intelligence Surveillance Act) and E.O. 12333 as domestic legislation of the US could enable interference by the US public authorities with the fundamental rights of data subjects from the EU, through the implementation of the surveillance programmes such as PRISM and UPSTREAM.[62] The Court then discovered that Section 702 of the FISA does not indicate limitations on the surveillance powers. The data subjects were also not granted actionable rights before the court against the US authorities. By these reasons the Court concluded that the limitations on the fundamental right to the protection of personal data was not circumscribed in a way essentially equivalent as required under EU law by Article 52(1) of the Charter.[63]

The Court also elaborated on the violation of Article 47 of the Charter. The setup of the Ombudsperson Mechanism was first, not sufficient enough to guarantee its independence, since the appointment of such a position is decided solely by the US government without any particular guarantees, and also not capable of adopting decisions which could be binding on the surveillance powers or providing possibility for effective remedy as those required by Article 47. The finding by the Commission in the Privacy Shield Decision of an adequate level of protection was thus overturned by the Court of Justice.

3.2.2 American peculiarity

For adequacy to be found in the United States then, it would involve changes to the US legal system. In particular, it must be answered whether there lies the possibility for the surveillance powers based on the national security and public interests to be circumscribed in a way that satisfy the requirements similarly under EU law and for the grant of actionable rights before the court against US public authorities under surveillance

[62] *Schrems I*, para 165.
[63] *Schrems I*, para 185.

circumstances. This would entail, of course, an examination of US legal system, especially in terms of data protection regime.

The data protection regime in the US differs in a lot of aspects than that in the European Union. Most notably, the US regime is a sectoral one. This means that there is no single and comprehensive regime regulating personal data collection and use. Such a regime does not impose on the entire private sector of the economy, but instead only protects personal data in specific areas which are sensitive or where the processing of data is likely to have harmful effects.[64] Therefore, only personal data in sensitive areas such as health care and banking are regulated with most of the other private sector left unregulated.

In the second place, although privacy is also considered as a fundamental right in the US, such a right can only receive constitutional protection against the action of State while in the EU the constitutional exercise of the fundamental rights of privacy and da protection also extends to the private sectors. Thus, violations of privacy in the private sectors in the US are regarded as a transactional or consumer protection matter, instead of a human right violation.

Also, such a regime would mean that rules are enforced sector by sector and thus it is fragmented. And it also decides that in the US there is no data protection authorities like in the EU. With regard to the cross-border transfer of personal data of US data subjects to outside the US, there is currently no regulation at all.

Under the broad picture of US data protection regime, the approach the US has taken regarding the regulation of access by public authorities to personal data can be shown accordingly, especially in terms of conducting surveillance programmes.

It is apparent that the Court disagreed very much with the Commission's assessment in the Privacy Shield Decision of the limitations and legal redress under US law to the interference from the access of personal data by the US public authorities. Admittedly in that decision, it was recognized that once the data is transferred to the United States, the U.S intelligence agencies can seek personal data only where their request complies with the FISA or is made by the FBI based on a so-called National Security Letter.[65] Among the legal bases FISA provides, the Section 702 FISA lies where the most concerns from the Court went to. It provides the basis for two important intelligence programmes from the US—PRISM and UPSTREAM. These programmes work by firstly, identification of non-US persons outside the US the surveillance of which may lead to the collection of the anticipated foreign intelligence, and secondly, upon the approval by a review mechanism within the NSA, the task of surveillance after the

[64] Lynskey (n 5) 24.
[65] Privacy Shield Decision, recital 78.

selection of identifying communication facilities used by the one targeted such as e-mail address or telephone number. Access of personal data of this kind is said to be subject to limitations from the PPD-28 and E.O. 12333. FISC (FISA Court), which is an independent tribunal with the power of review and in some cases prior authorisation of the measures regarding the intelligence activities, admittedly authorises surveillance programmes on an annual basis instead of on the basis of individual cases. The certifications to be approved by FISC only contains categories of foreign intelligence information and no information about individual persons.[66]

And a number of avenues of remedies were named in the Privacy Shield Decision relating essentially to areas including interference under FISA, unlawful, intentional access to personal data by government officials and access to information under Freedom of Information Act (FIOA). The redresses can be done by bring civil action for damages, or under administrative and judicial review. However, it was also admitted that despite these avenues of redress available, at least some legal bases that the US intelligence authorities may use (e.g. E.O. 12333) are not covered. The creation of a new Ombudsperson Mechanism was also deemed to constitute adequate and effective guarantees against abuse with its involvement of independent oversight bodies and its own independence of function, ensuring that the complaints of individuals will be properly and fairly handled. However, the Court disagreed on this point with the Commission too.

3.2.3 American security as a justification for the intrusion of European privacy?

The question would then become whether the US is willing to undertake changes to comply with the requirements of adequacy under GDPR, especially when it would affect its ability to undertake activities concerning national security or foreign intelligence gathering, or whether this would be allowed under its own national legal system.

While the intention is not to examine US legal system and propose a reforming plan about how to be compliant with legal requirements under EU law, it would be insightful to find out what changes are needed for an adequacy finding for EU-US data transfer to go on after the *Schrems II* decision.

Such changes would at least involve, for example, the redress to a judicial review on case-by-case basis which would examine whether individuals are properly targeted, the limitation of the foreign intelligence surveillance powers, in particular the requirement for them to define their scope and provide guarantees, and also the inclusion of all the legal bases which the US intelligence authorities may use under the judicial review. These are not simple efforts to make, especially when they involve national security

[66] Privacy Shield Decision, recital 109.

issues, which have always been heavily dependent on the discretion of executive powers and sensitive and secretive even in a trial.

It is also true that the Commission contended in the decision that obtaining foreign intelligence information or national security, which the surveillance measures are intended to do, is a legitimate policy objective recognized by the Court of Justice.[67] However, it remains puzzling whether essential equivalence of the level of protection would allow, in the case of European data transferred to the US, the interference based on the legitimate interests of national security of the US, as it allows interference based on national security objectives here in the EU. US national security and national security within EU member states are obviously two quite different things. Such divergence becomes even bigger when the two sides across the Atlantic try to balance this matter against civil liberties.

The US approach

As mentioned before, there is neither a comprehensive definition of "privacy" nor a comprehensive approach to "privacy" in US law. Using a "patchwork of federal and state statues"[68], the balancing between competing state interests and civil liberties is difficult under US data protection regime. A number of legal basis were provided in a lot of legal acts in order to authorise the surveillance programmes and foreign intelligence activities. As part of the legal system of law enforcement, surveillance is far more permissive in US law than in EU law due to the principle that "surveillance is legal unless forbidden".[69] Such an approach to surveillance or personal data processing is actually at the opposite of that of the EU, by which surveillance or personal data processing is not allowed unless otherwise provided with a legal basis.[70]

It was in *Katz v United States (1967)* that the US Supreme Court held that any intrusion, be it physical or electronic, of a place where a person has a "reasonable expectation of privacy", may constitutes a violation of the Fourth Amendment.[71] This case thus confirms the interference of electronic surveillance with privacy. However, in later cases, it was recognized that there exists a foreign intelligence exception to the *Katz* and that foreign security surveillance remains within the hands of the Executive exempted

---

[67] Privacy Shield Decision, recital 89. Footnote 97 there continued the explanations with the references to the case law of national security being a legitimate objective.
[68] Martin A. Weiss and Kristin Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield' (2016) Congressional Research Service, 3. <https://fas.org/sgp/crs/misc/R44257.pdf> accessed 12 May 2021.
[69] Anna Dimitrova and Maja Brkan, 'Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair' (2018) 56(4) JCMS 751, 755-80, citing: Neil Richards, 'The Dangers of Surveillance' (2013) 126 (7) HLR, 1942.
[70] ibid Dimitrova and Brkan (n 67), 755, citing: Francesca Bignami, 'European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining' (2007) 48(3) BCLR 609.
[71] *Katz v. United States*, 389 U.S. 347 (1967).

from oversight.[72] As a result, there is a distinction of the treatment under US law between domestic and foreign security surveillance and, thus, "a double-track system" which treats non-US persons differently. More worryingly, a number of attempts to challenge the Section 702 FISA has ended up being rejected by the Court, indicating the balance in favour of national security interests. Such a preference has essentially stayed the same even after the Snowden revelations.[73]

The difference of treatment under the Fourth Amendment between US citizens and non-US persons poses yet another difficulty to find the adequacy of the level of protection in the US, besides the difference in the general schemes of US and EU data protection regimes. Indeed, while the EU holds privacy and data protection as fundamental rights, the US has been quite reluctant to limit its power to conduct surveillance and intelligence activities, especially with regard to foreign security surveillance.

The EU approach

What makes it even harder to find adequacy is that there seems to lack a corresponding or identical concept of "national security" within the EU. Since the GDPR applies to neither national security[74] nor public security[75], the comparison of EU to the US regarding data protection in the case of balance against national security should logically be based on the case law. Article 8 of ECHR has expressly admitted the possibility that public authorities can interfere with the right of privacy in the interests of national security or public security. The case law from ECtHR suggests that ECtHR has taken a neutral stance when balancing the two.[76] But after the Snowden revelations, case law from the Court of Justice shows that the Court has been putting more weight on privacy more than other potentially overriding reasons including public security.[77]

One cannot find the total equivalence of authorised foreign intelligence activities at the level of EU. Again, as Article 4(2) TEU stipulates, the EU does not have competence in the realm of national security. Therefore, how

---

[72] Dimitrova and Brkan (n 67), 759, citing: *United States v United States District Court for the Eastern District of Michigan*, 407 U.S. 297 (1972); *United States v Truong Dinh Hung*, US Court of Appeals for the Fourth Circuit, 629F.2nd 908 (4th Cir. 1980).
[73] Dimitrova and Brkan (n 67), 760.
[74] TEU, art 4(2): national security remains the sole responsibility of each Member State.
[75] GDPR, art 2(2)(e).
[76] Dimitrova and Brkan (n 67), 761, citing: *Klass and Others v Germany* App no 5029/71 (ECtHR, judgment of 6 Sep 1978); *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000); *Association '21 December 1989' and Others v Romania* App no 33810/07 (ECtHR 24 May 2011); *Segerstedt-Wiberg and Others v Sweden* App no 62332/00 (ECtHR 6 June 2006).
[77] Dimitrova and Brkan (n 67), 763, citing: Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications* [2014] ECLI:EU:C:2014:238; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016] ECLI:EU:C:2016:970; *Schrems I.*

Member States implement and enforce their own national security objectives varies among different Member States and there exists nothing such as the concept of a common "EU national security". In fact, when one compares the case in the EU with the case in the US trying to find an essentially equivalence of the level of protection of personal data, as required by the GDPR, problem arises as to which references of national security or public security should the comparison be against, corresponding to the "US national security" against which data subjects' privacy rights are balanced.

However, it does not mean that the EU law has left the surveillance powers of the Member States unregulated. It was only after the *Schrems II* ruling that attention was drawn to EU's Member States' own surveillance powers. While confirming the disproportionate nature of general and indiscriminate retention of traffic data and location data in *Tele2 Sverige*, the Court still held that the directive on privacy and electronic communications[78] precludes Member States requiring providers of electronic communications to carry out general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security, or to carry out the general and indiscriminate retention of such data as a preventive measure.[79] However, the Court also held that that directive allows the general and indiscriminate retention of such data in situations where the Member States is facing "a serious threat to national security that proves to be genuine and present or foreseeable",[80] with necessary safeguards in place. Some member states like Germany also examined its own foreign surveillance power and asked for a better design of surveillance regime in line with fundamental rights enshrined in its constitution.[81]

---

[78] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11.

[79] Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2020] ECLI:EU:C:2020:790; Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* [2020] ECLI:EU:C:2020:791.

[80] Joined Cases C-511/18, C-512/18 and C-520/18, para 168.

[81] Kenneth Propp, 'Transatlantic Data Transfers: The Slow-Motion Crisis' (*Council on Foreign Relations*, 13 January 2021) <https://www.cfr.org/report/transatlantic-data-transfers> accessed 20 May 2021, citing: Bundesverfassungsgericht, 'In their current form, the Federal Intelligence Service's powers to conduct surveillance of foreign telecommunications violate fundamental rights of the Basic Law' (Press Release No. 37/2020, 19 May 2020)

Difficult to compare and to justify

So at least the CJEU takes a very firm stand in prohibiting the sort of massive surveillance programs on a general and indiscriminative basis allowed in the US, prioritizing fundamental rights unless faced with a serious threat to national security. In this respect alone, the EU differentiates itself with the US in its stance towards public access of personal data on national security ground. The comparison of the approaches taken by both sides in balancing national security and fundamental rights is nevertheless complicated and entails more comparison than in this respect only.

The "double-track" system in the US also further diminishes the plausibility for a finding of adequacy. Even if the comparison could take place and be convincing, the different treatment to non-US persons would mean that even if all the assessment of the elements as required under Article 45(2) of the GDPR turns out to be satisfying, the adequate level of protection may still not be found. It is worth noting that in the Recital 101 of the GDPR, the purpose of regulating data flows to third countries is to ensure that the level of protection under the EU law is not "undermined". The level of protection is not maintained, therefore, when after assessing the elements in Article 45(2) of GDPR involving the rule of law, relevant legislation and legal system of that third country, it is found that that country affords the "essentially equivalent" level of protection as in the EU law, but that protection does not extend to persons other than its own citizens.

And as a final point, it is obvious from the analysis of the Court in the *Schrems II* judgement that for the interference with the fundamental rights of privacy and data protection of the EU data subjects to be circumscribed in a way that satisfies Article 52 of the Charter, such interference resulting from the surveillance activities would need to be proportionate with a legitimate objective of general interest. That objective can only be to protect the national security interests of the US. Perhaps here lies the most mystical complexity for the adequacy to be found in the US—can it really be possible for the intrusion into the privacy of European citizens to be justified by US national security? Even if the answer is in the affirmative, then to what extent can the interference be regarded as proportionate? Or as the Court's judgement determines, will the US government be actively willing to subject itself to a decision from an EU court to limit its national security powers, in order for adequacy to be found in the US so that adequacy decision could still be a channel to authorise EU-US data transfer? And this question lingers despite that the personal data mainly flows from the EU to the US and that adequacy decision is only one of the eligible legal safeguards required by the GDPR to authorise cross-border data transfer. The absurdity needs not an answer from these questions to be proven.

<https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html> accessed 26 May 2021.

3.3 Adequacy to abolish?

The difficulties to find the required adequacy for cross-border data transfer particularly in the case of transfer to the US, propose the inevitable doubts over the effectiveness and suitability of adequacy decision as an instrument to authorise such data transfer. Is adequacy decision fit for the task it is expected to perform?

3.3.1 The goal and the task of this instrument

It is first worthy of recalling the initial intention and the goal of setting up this instrument. The most direct goal of adequacy decision is of course to secure the level of protection under the EU law is not undermined after the data of EU data subjects is transferred to third countries. But to achieve such a goal, there are a number of safeguards that might be suitable and in fact also recognized to give the required adequate level of protection. So why was adequacy decision chosen to be the one that has the most general and widest application to transfer to a certain country?

The policy goals of creating the adequacy decision regime may be seen from its effect. The Commission called it a dynamic approach to "build mutual trust, guarantee uninhibited flow of personal data and foster the convergence of the level of protection in the EU and the third country".[82] Adequacy decisions are part of the efforts of the EU to endow its data protections laws with extraterritorial effect. Such an effect could be seen from Article 2 and 3 of the GDPR regarding the material and territorial scope of the GDPR.[83] Adequacy decisions can, by applying the European data protection rules to third countries, have the effect of exporting the European standards to outside world, thus appropriating the laws in other countries. They reveal and facilitate the EU's ambition to set the universal high standards for data protection all over the world. And it did achieve the outcome of bringing the data protection laws of some other countries in line with the European standards.[84]

---

[82] 2017 Communication (n 39), 9.

[83] W Gregory Voss, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) 29 Wash Int'l LJ 485, 494-98. The GDPR gives protection to natural persons regardless of their nationality or place of residence. The territorial scope of the GDPR also reaches outward by applying to the processing of personal data "in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not" (GDPR art 3(1)).
Also, Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317, where the Court interpreted the term "establishment" to include the case where Google Inc., a US company was subject to the 1995 directive due to the fact that the activities of Google Spain, its Spanish establishment helped financing the US parent company's search engine. Also, GDPR art 3(2), the GDPR applies to certain companies with no establishment in the European Union.

[84] Bradford (n 59) 23.

3.3.2 Can it do the job?

The vision that adequacy decision will bring about the acceptance of European Standards all over the world finally met the hard truth that this instrument failed twice to authorise data transfer to the US while protecting the fundamental rights of EU data subject. Resistance from the US showed that while imposing EU standards on some countries is not difficult to realize, the influence from the EU cannot reach across the Atlantic without a fight, a fight for which neither side is willing to compromise.

As already showed in *Section 3.2*, the confusion caused by the unclear definition and enforcement of "national security" within the EU undermines the legitimacy and logical consistency of the EU to hold third countries up to a standard which do not bind itself.[85] And technically speaking, the finding of adequacy requires the comparison of EU legal system against that of a third country. This would involve the study on the legal system of that third country, with difficulties arising from the disparity among legal concepts, linguistic texts and different approaches to data protection. Besides, such a finding is also complicated by the political actors, while this process is also dependent upon political influences, values and economic ties.[86] As Kuner argued, the procedure to have adequacy in a third country to be found by the Commission is a "triumph of bureaucracy and formalism over substance".[87]

Therefore, it seems that adequacy decisions have limited efficacy in promoting European standards around the world. In countries like the US, China or India where there exists a greater amount of data exchange and therefore a greater need for adequacy decisions, there is no adequacy or potential adequacy to be found whilst nobody would foresee the concession to EU standards by those country in the near future.

It makes sense then, that adequacy decision may also not be able to fulfil its most important job, which is to ensure the "essentially equivalent" level of protection in the third country to which data is transferred. As mentioned in *Section 2.3*, adequacy decision is a unilateral decision with legal effects only within the EU and the third countries are not bound but it. And the formalistic requirements and the lack of enforcement of data protection authorities further pose doubts to the effectiveness of adequacy decision as the protector or gatekeeper of privacy and personal data as fundamental rights with regard to cross-border data transfer.[88]

---

[85] Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post *Schrems*' (2017) 18(4) GLJ 881, 898.
[86] Christopher Kuner, 'Developing an Adequate Legal Framework for International Data Transfers' (2009) 263 in: S.Gutwirth and others, *Reinventing Data Protection?*(Springer 2019), 265.
[87] Kuner (n 79) 911.
[88] Kuner (n 79) 912.

Back to reality, the double failures of both Safe Harbour and Privacy Shield certainly question the legal certainty this instrument can afford to businesses and undertakings across the Atlantic. The mistrust in this instrument has accumulated, substantiated by the fact that many companies do not rely on it as the only safeguards they provide for their clients[89]. At least confidence is lost in the particular case of adequacy decision for data transfer to the US when the Commission has already failed twice. More importantly, the third country is in its capacity to make any changes regarding its data protection rules with no obligation under the adequacy decision to maintain compliance with European standards and accordingly, the Commission under the GDPR must suspend the data flows to that third country if the adequacy findings are adversely altered due to those changes from that country. Such suspension can also result from the periodic review of the Commission whose conclusion comes to the opposite of the adequacy finding. Either way it has been proven that adequacy decisions never intend or are fit to be relied upon for longer periods, creating inconvenience for whoever relies on it and even more barriers to cross-border data transfer.

Many have successfully predicted the fate of Privacy Shield Decision as the same of Safe Harbour Decision[90]. While it is not the intention of this paper to pass the sentence for this instrument, it will be inspiring to find out if the adequacy decision that the Commission adopted regarding data transfer to Japan can survive the examination of the kind in *Schrems* judgements and if there exists any possibility for the adequacy decision about Japan to fail.

[89] Julie Brill, Assuring Customers About Cross-Border Data Flows (*Microsoft Blogs*, 16 July 2020) < https://blogs.microsoft.com/eupolicy/2020/07/16/assuring-customers-about-cross-border-data-flows/> accessed 12 May 2021.
[90] Kuner (n 79) 913.

4 Adequacy decision—Japan

On 23 January 2019 the Commission adopted Decision 2019/419[91] and found the adequate level of protection of personal data by Japan. It was the first adequacy decision adopted after the enter into force of the GDPR. The case with Japan differs in a lot of ways with the case with the US. The purpose of exploring Decision 2019/419 is to compare these two cases and find out if as an instrument it is being made better use of or if it is further exposing its inefficiencies in governing cross-border data transfer. This section starts with the general introduction to Decision 2019/419 and its flaws after examination by the requirements similar to those in the *Schrems* judgements, and also the implications about the future of adequacy decision as an instrument to govern cross-border data transfer.

4.1 Decision 2019/419

The exploration can start from the assessment the Commission made in Decision 2019/419. In that decision the Commission found that privacy and data protection in Japan had its root in the Constitution and were recognized as a constitutional right.[92] The most relevant law for data protection was the Act on the Protection of Personal Information (APPI), passed in 2003 and latest amended in 2017. An independent supervisory authority, the Personal Information Protection Commission (PPC) was established according to APPI, responsible for the oversight and enforcement of that legislation.[93] The PPC adopted "Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision" (The "Supplementary Rules"), in order to enhance the protection of personal data transferred from the EU to Japan and also, to ensure the adequacy based on Decision 2019/419.[94] The Commission also asserted in the decision that guidelines from the PPC are binding on business operators.[95]

The processing of personal data in Japan is also subject to purpose limitation set by Article 15 and 16 of the APPI, where personal data should be processed for a specific purpose and used in a way compatible with such purpose. The Supplementary Rules also strengthens the protection of personal data transferred from the EU to Japan by requiring that the recipient of personal data from the EU should also be bound by the purpose for which the data was previously collected.[96] A number of individual rights

[91] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L76/1.
[92] Decision 2019/419, recital 6-8.
[93] Decision 2019/419, recital 11.
[94] Decision 2019/419, recital 15.
[95] Decision 2019/419, recital 16.
[96] Decision 2019/419, recital 39-43.

are granted by the APPI, including the right to access, ratification and erasure of personal data and the right to object.[97]

The grounds upon which public authorities in Japan can rely to gain access and use of personal data are mainly criminal law enforcement and national security purposes.[98] For criminal law enforcement purpose, the collection of electronic information is permissible based on a court warrant or a request of voluntary disclosure. The warrant requirements are guaranteed by the Constitution and the Code of Criminal Procedure and applies to both the collection of electronic information and the interception of electronic communications. These compulsory measures are subject to an examination of the existence of necessity to achieve its objective.

For national security purposes, the Commission found that there was no law in Japan permitting compulsory requests or "wiretapping" outside criminal investigation. Business operators receiving a request for voluntary cooperation are under no legal obligation to comply with such request. Government access to personal data on national security grounds will all be subject to limitation of voluntary investigation and conform with the requirements of necessity and proportionality. The Commission thus excluded the possibility of Japan conducting mass and indiscriminate collection or access to personal information for national security reasons.

For investigation on both purposes, a special mechanism was created to facilitate individual redress for European data subjects whose data has been transferred to Japan, under which they can submit a complaint to the PPC and the PPC is under obligation to handle the complaint and intervene with other competent public authorities. A confirmation of the outcome will be made by the competent public authorities and may be helpful "in seeking judicial redress".[99]

4.2 The flaws

It is, of course, obvious that due to the fact that public authorities in Japan are not granted arbitrary or a wide range of powers in terms of conducting intelligence gathering and information collection, it is likely that the flaws in the Privacy Shield Decision such as the uncircumscribed access by public authorities to personal data without the consent of data subjects on national security grounds, are not seen in Decision 2019/419.

However, after a closer look into Decision 2019/419, a number of flaws can still exist, which could show its incompatibility with some of the legal requirements under the GDPR in light of recent case-law and the Charter.

[97] Decision 2019/419, recital 81.
[98] Decision 2019/419, recital 113.
[99] Decision 2019/419, recital 144.

Although there might not seem to be any problem with the limitations of power delegated to Japan's public authorities to conduct national security activities, some of requirements which are assessed and approved by the Commission may still suggest that the Japanese standards are not up to the European ones. In the first place, the data retention requirements are not clear enough to implicate adequate limitations to the processing of personal data for the purposes of criminal law enforcement and national security. In Opinion 1/15, the Court has held that the data retention requirements should "satisfy objective criteria that establish a connection between the personal data to be retained and the objective pursued"[100] and decided that data retention which is longer than justified by the objective of the measure itself would mean that the continued storage of personal data failed to be limited to what is strictly necessary[101]. And indeed, even in Annex VI of the Privacy Shield Decision, the US Department of Commerce stressed that personal data of non-US persons gathered through US intelligence activity will be limited to be retained for more than five years unless otherwise determined by the Director of National Intelligence to continue within the national interests of the US[102]. The Japanese law does not seem to restrict the period of retention of personal data except providing that personal information should only be retained "to the extent necessary for carrying out the duties of public authorities".

In the second place, the special mechanism created for the individual redress seems to resemble the "Ombudsperson Mechanism" in the Privacy Shield Decision in that they both function as liaison for the EU individual applicants of complaints with the public authorities responsible for handling the complaints and that they do not guarantee the judicial redress against the public authorities in court. The Commission used very vague language in implying only a possibility of such[103].

Also in the third place, in Annex 2 of Decision 2019/419, there seems to be no mentioning of actionable rights before a court in the area of national security except an administrative appeal for the review of the non-disclosure decision made by the authorities against the request of individuals.[104] In the Commission's assessment about the individual redress for access to personal data by public authorities, it mainly focused on the administrative review to the handling of complaints from individuals by the Administrative Organ and judicial redress was presented only as a possibility to challenge the decision of the Administrative Organ and also briefly mentioned in the form of a damage action.[105] Again, there lies the possibility of violation of the

---

[100] Opinion 1/15, para 191.
[101] Opinion 1/15, para 204-06.
[102] Privacy Shield Decision, annex VI I(C).
[103] Decision 2019/419, recital 144. The text used was "the possibility of receiving such a confirmation……may be of assistance to the individual in taking any further steps, including when seeking judicial redress."
[104] Decision 2019/419 Annex 2 II.C.
[105] Decision 2019/419, recital 165-70.

right to effective remedies enshrined by the Article 47 of the Charter, as the Court found in the *Schrems II* judgement.

Besides the above, there were also problems which exists generally and are deep-rooted in the distinction of the data protection regimes between EU and Japan.

The EU and Japan have different concepts of data privacy. The scope of APPI is limited to information relating to a living individual while the GDPR defines personal data to be "any information relating to an identified or identifiable natural person that potentially identifies the individual". The difference of the approaches to definition of personal data was clearly exhibited. Moreover, Japan seems to view personal data as an economic commodity and emphasizes more frequently about its contributions to the industry and economy.[106]

The enforceability of PPC guidelines can also cause confusion, although the Commission has acknowledged that PPC guidelines are binding on business operators[107]. In Japan guidelines play a unique and important role in the regulatory framework, particularly in data protection, in that they constitute no law but guide both the actions of private activities on a voluntary basis and the interpretation by the Japanese courts when applying APPI/PPC rules. And guidelines are the main enforcement mechanism of the PPC.[108]

It was also pointed out that the enforcement in Japan works primarily through cultural value and social norms, meaning that guidelines are followed due to the businesses' fear of loss of social trust and reputation. The trust of customers is valued as of vital importance and damage of that is more serious than damage of money. Such an enforcement was of course very different from the one in GDPR, which is based on the enforcement of punishment, regulatory body and law enforcement.[109]

4.3 Implications

The case of Japan can provide a lot of implications. Among them the first is that Decision 2019/419 was adopted upon a mutual adequacy agreement. Japan also acknowledged after that decision that EU provides an adequate level of protection under the APPI. While this proved the attraction of EU standards and that countries like Japan are adopting an EU-style data protection regime, it also reveals the limitations of the harmonizing effects of adequacy decision. For countries like the US where its businesses are in most cases, relied upon by other countries, it is not very much motivated to move towards a standard resembling the EU one.

---

[106] Flora Y. Wang, 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement' (2020) 33(2) HJLT 661, 669.
[107] Decision 2019/419, recital 16.
[108] Wang (n 100) 674-77.
[109] ibid 679-81.

Such limitations were also substantiated by the fact that Japan set up separate rules (Supplementary Rules) for data transfer from the EU. While these rules definitely contributed to the accomplishment of guaranteeing the level of protection to EU data subjects, such a supra-national treatment from Japan for cross-border data transfer can only be described as exceptional and uncopiable and in some way, deviates from the initial objective of using adequacy decisions as an instrument to regulate cross-border data transfer. It seems to strengthen the argument made by Kuner that adequacy requirements are a "formality over substance"[110]. It could also be explained by Japan's desire to reach adequacy agreements so as to facilitate trade with the EU and develop economic interests, so that it made such big an effort to fulfill this "formality".

More importantly, whilst more stricter rules are stipulated, the cultural and political difference add more doubts as to whether the enforcement would be effective as imagined. If the objective of appropriating third countries' laws to a way towards EU standards was circumvented by the supra-national treatment offered by Japan, would Japan's competent public authorities be willing and also experienced enough to enforce rules which are not even applicable to its own nationals? What is sure is that this in turn exposes more inconsistency with the Commission's approach of adopting adequacy decisions.

However, the case of Japan was after all an example of GDPR's extraterritorial effects—Japan has reformed its data protection regime to one that has a lot in common with the EU data protection regime. Before the amendment of APPI, the major discrepancy between Japan's data protection regime and the EU one includes, from the Japan side, the absence of an independent data protection authority, a provision on sensitive information and the rules on cross-border transfer of personal data.[111] Japan caught up with EU standards through the amendment. It even adopted a similar provision as the Article 45 of GDPR, requiring that data transfer to a foreign country without the consent of individuals to be conditional upon the existence of equivalent standards of data protection in that country to that in Japan. Indeed, Decision 2019/419 was adopted based on the conclusion of a mutual adequacy agreement, whereby Japan later also recognized the adequacy of EU's data protection standards. As the leading trade partners all over the world, the leaning of EU and Japan in the area of data protection standards has further raised the question whether the US will join.[112] And this is probably where the limitation of adequacy decision as an instrument surface—it cannot bind other countries and the most important player in data regulation is not willing to accept the rules set by the EU once and for all.

---

[110] Kuner (n 81).
[111] Yuko Suda, 'Japan's Personal Information Protection Policy Under Pressure: The Japan-EU Data Transfer Dialogue and Beyond' (2020) 60(3) Asian Survey 510, 514-16.
[112] ibid 528.

5 International Agreement as An Alternative Instrument

Both *Schrems* judgements showed that the unilateral assertion of EU values, instead of reaching reasonable common ground with other countries about the data protection standards, cannot succeed in delivering a sustainable and universally applicable solution for international data transfer. It is therefore necessary to consider whether international agreement could be an alternative instrument that functions better than adequacy decision.

5.1 An instrument already in use

5.1.1 Use by the EU

The regime for regulating cross-border data transfer in the EU is obviously a fragmented one. Article 16 of TFEU provides an independent legal basis for the EU to adopt and enforce data protection rules. More importantly, the Charter has stipulated the right to privacy and the right to data protection as fundamental rights in the EU. Thus, protection for the personal data transferred to third countries need not to be dependent upon any other cause. Any cross-border activities which involves such data transfer have to comply with the requirements stemming from the GDPR, the Charter or the Treaties, causing the fragmentation of the regulatory regime.

Rules on international data transfer differentiates among different sectors and areas of data transfer. For example, Directive 2016/680 ("Law Enforcement Directive")[113] applies to cross-border data movement for the purpose of criminal law enforcement which falls outside the scope of the GDPR according to Article 2(2)(d) of the GDPR. Chapter V of that directive provides rules for international transfer of personal data for law enforcement purposes, which also includes data transfer based on adequacy. However, so far, no adequacy decision based on Law Enforcement Directive has been adopted[114] and the Commission in February 2021 launched the procedure for adopting such an adequacy decision under Law Enforcement Directive with regard to data transfer to the United Kingdom after Brexit[115].

---

[113] 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 L119/89.

[114] Laura Drechsler, 'Comparing LED and GDPR Adequacy: One Standard Two Systems' (2020) 1(2) GPLR 93 .

[115] Draft decision on the adequate protection of personal data by the United Kingdom: Law Enforcement Directive <https://ec.europa.eu/info/sites/default/files/draft_decision_on_the_adequate_protection_of

Instead, international agreements have been used by the EU to regulate international data transfer in the area of law enforcement. The Umbrella Agreement[116] was reached by the EU and the US to ensure "a high level of protection to EU citizens' personal data transferred to judicial and police authorities across the Atlantic"[117].

Passenger Name Records[118] and Terrorist Financing Tracking Programme[119] are the two areas where international agreements have been concluded for the protection of personal data transferred within those areas.

The GDPR governs the data transfer in other areas to the extent which falls within the scope of that regulation. The Commission has listed adequacy decision, standard contractual clauses, binding corporate rules, certification mechanism, codes of conduct and derogations (Article 49 of the GDPR) as the toolkits of mechanisms for the legal transfer of personal data from the EU to third countries.[120] International agreement, however, has not been explicitly included as one of the toolkits.

5.1.2 Use around the globe

It would be incorrect, instead, to assert that international agreements cannot be used for global data governance. Right now, a number of international instruments are used to regulate cross-border data transfer. These instruments include guidelines or frameworks from international organisations, such as the *OECD Privacy Guidelines* and the *APEC Cross-Border Privacy Rules (CBPR) System*. Among those instruments, there is also the internationally binding document—*The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)*, to which 53 states have signed. The EU and many

---

_personal_data_by_the_united_kingdom_law_enforcement_directive_19_feb_2020.pdf> accessed on 6 May 2021.

[116] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences [2016] OJ L336/3

[117] Statement by Commissioner Věra Jourová on the European Parliament consent vote on the conclusion of the EU-U.S. data protection "Umbrella Agreement", <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_4182> accessed 6th May 2021.

[118] Existing international PNR agreements are the ones with Australia and the US, and there are still ongoing negotiations with Canada and Japan.

[119] EU-US Terrorist Finance Tracking Programme (TFTP) Agreement: Council Decision 2010/412/ of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program [2010] OJ L195/3.

[120] Rules on international data transfers (*website of the European Commission*) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en> accessed 12 May 2021.

of the member states are parties to the *OECD Privacy Guidelines* and *Convention 108*. Therefore, international agreements have been used specifically to tackle the challenges about data protection, while also promoting and upholding the free flow of cross-border transfer of personal data.[121]

5.2 Trade Agreements

Besides international agreements specifically singed for the purpose of data protection, many have put forward the inquiry of whether there exists such possibility as to include data protection rules in the trade agreements. Trade agreements mostly entail trade aspects of the data exchange crossing the borders, and so they should only involve the protection of personal data the transfer of which incurred as a result of trade. The protection of personal data transferred internationally under other purposes such as law enforcement purposes is thus not the topic under this section.

First of all, the close relationship between data protection and trade in the digital area is not a novel topic. The Commission in multiple occasions has explicitly agreed with and supported this relationship. In a press release after the Commission launched the adoption of adequacy decision regarding data transfer to Japan, not only did the Commission agreed that such an arrangement would complement the EU-Japan Economic Partnership Agreement, but it affirmed with Japan that "in the digital era, promoting high privacy and personal data protection standards and facilitating international trade must and can go hand in hand."[122] Similar words were also said in a joint statement from the Commission and South Korean data protection authorities after adequacy dialogues with that country.[123]

5.2.1 Benifits

The inclusion of rules governing cross-border data transfer in the trade agreements would offer benefits which adequacy decisions cannot provide.

As mentioned in *Section 2*, the *per se* nature of adequacy decision made it only a unilateral finding by the EU regarding the level of protection in third countries and thus, impossible to establish international obligations as the international agreements can do. While under adequacy decisions it depends

---

[121] See Article 16, 17 &18 of the OECD Privacy Guidelines and Article 12 of Convention 108.

[122] International data flows: Commission launches the adoption of its adequacy decision on Japan (*Press release of the European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5433> accessed 8th May 2021.

[123] Joint Statement by Commissioner Reynders and Yoon Jong In, Chairperson of the Personal Information Protection Commission of the Republic of Korea (*Press release of the European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1506> accessed 8th May 2021.

totally on the EU side to bear the risk and the result of policy changes in the third countries, international agreements undoubtedly give more pressure on other countries to maintain the standards and level of protection of personal data transferred there as breaking the international obligations under them would induce legal responsibilities and damages which are actionable under international law. They also provide the EU with unambiguous directions of remedies and responses in the case where that third country breaches its international obligations. The superiority of international agreements over the wholly domestic instrument to govern cross-border data transfer, which inevitably involves different jurisdictions and international relations, is thus enormous.

The adequacy decision can only be said to open the door from the EU side, but international agreements would create a channel for the data exchange to take place. Such a channel can thus also overcome the inefficiencies of adequacy decision due to its relatively short period of validity or its uncertainty about the length of the validity period. In this sense, the legal certainty and the reliability of the instrument to govern cross-border data transfer are greatly increased.

The legal certainty is also strengthened by the involvement of more EU institution in the conclusion of international agreements. The conclusion of international agreements brings more decision-making institutions into the process—such as the Council, the European Parliament and the CJEU. With more opinions and involvements from these institutions, different interests affected by such agreements and concerns over the issued covered there can be put forward, discussed and balanced. Thus, conformity with EU law can be better guaranteed with the conclusion of an international agreement.

Moreover, trade agreement better reflects and acknowledges the relationship of data flows and trade. With the development of trade and especially the rapid growth of digital trade, data flows multiply, raising concerns over the protection of privacy and personal data as a result of such flows. It also fits in better with the perception of some countries regarding the position of data in world's trade. Many countries such as Japan and the US see data as a business commodity or an essential booster of economy. They are better motivated in negotiating a deal for both trade interests and privacy issues to be guaranteed than solely tackling the issue of protection of personal data of other countries' data subjects transferred to them. And the fact that protection of data flows was already included in the digital trade title in some draft FTA agreements to which the EU was a party, has proved that the EU to some extent is also bringing itself in line with that kind of rhetoric. To enforce the protection of personal data transferred internationally incurred by trade under trade agreement is therefore a both viable and reasonable option.

5.2.2 Difficulties

However, as the Commission has noted, "the EU data protection rules cannot be the subject of negotiations in a free trade agreement"[124]. Under the existing adequacy regime, the adoption of a unilateral decision which falls wholly within the internal aspect of EU law obviously cannot be subject to negotiations in an international agreement. But even without being bound by the adequacy instrument, difficulties remain with the use of trade agreements as an instrument to regulate cross-border data transfer.

Although there is no doubt that the EU has competence and legal personality to conclude international agreements with other countries and inter-governmental organizations, it is nevertheless hard to fit the negotiation and conclusion of data protection rules into the EU's competence of external relations. If the EU were to approach the regulation of cross-border data transfer through trade agreements, the legal basis should usually be Common Commercial Policy or the implied powers of internal market.[125] As have been emphasized, data protection constitutes an independent legal basis stemming from Article 16 of TFEU. Neither the Common Commercial Policy nor the implied powers of Internal Market were explicitly found to cover the competence of EU to negotiate international rules regarding cross-border data transfer, especially under the perspective of protection the fundamental rights to privacy and data protection.

They also would not rightly categorize the position of data protection in the EU legal system. As illustrated in Section 2, data protection is not a "by-product" of Common Commercial Policy or Internal Market. The negotiation of data transfer rules under the competence of them would have the implication that data protection is dependent upon or secondary to them. Even if the data transfer rules reached through trade agreements would only involve the transfer of personal data incurred as a result of trade, this is not the case of how data protection is viewed under EU law. Such kind of negotiation will have the possibility of contradicting Article 16 of the TFEU and the Charter.

As regards the possibility of regulating cross-border data transfer through WTO law, the rules and mechanisms under WTO law seem not to be ready to fully address digital trade, despite they constitute comprehensive and enforceable rules and provide effective dispute settlement. According to Burri, while some rules are particularly designed to "allow WTO members to tailor their commitments", many issues such as the classification of certain online games, the applicability of WTO rules and commitments to electronically traded services and the finding of "likeness" for the

---

[124] 2017 Communication (n 39) 9 & fn 42.
[125] Case 22/70 *Commission of the European Communities v Council of the European Communities* [1971] ECLI:EU:C:1971:32; Opinion 1/03 of the Court (Full Court) of 7 February 2006 [2006] ECLI:EU:C:2006:81; Opinion1/94 of the Court of 15 November 1994 [1994] ECLI:EU:C:1994:384.

application of Most Favored Nation obligations and national treatment commitments for E-Commerce, have been left unanswered.[126] The lack of political consensus on the substantial issues of digital trade impedes the adaptation of WTO law to the new development in trade.

Some regional trade agreements also seek to approach cross-border data transfer. The Trans-Pacific Partnership Agreement requires that parties of TTP should "adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce", but no standards or benchmark for such a legal framework other than "principle or guidelines of relevant international bodies" are referred to[127]. TTP also "encourage the development of mechanisms to promote compatibility" between different regimes of personal information protection and call on parties to "endeavour to exchange information on any such mechanism applied in their jurisdictions and explore ways to promote compatibility"[128]. These provisions, as Burri noted, are "essentially treating lower standards as equivalent" and "prioritizing trade over privacy rights"[129].

Indeed, seen from the texts of EU's proposal of data protection clauses under the digital trade title for trade agreements[130], the EU seems to take a rather loose approach in that it only asks that each party can "adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy". It avoids going beyond that to reach a common standard of safeguards recognized by both parties. This likely relates to the difficulties of reaching common grounds with countries that have a different kind of regulatory regime of data protection and the fact that privacy and personal data are perceived differently in different countries. The inclusion of data protection provisions in a trade agreement will therefore always involve a balance between the need for trade facilitation, on the one hand, and privacy and data protection on the other hand. Such a balance in a trade agreement seems to be unable to avoid the fate of prioritizing trade.

Further complicacy arises in that there exists no effective mechanism for the balance of human rights and international trade law. For example, trade dispute resolution bodies are bound by their limited competence, which do not include coordination on human rights issues. Even if international human rights could constitute customary law which WTO adjudicating bodies are allowed to apply, customary law are applied "only to the extent that it does not conflict or is not inconsistent with WTO agreements"[131]. In

---

[126] Mira Burri, 'The Regulation of Data Flows Through Trade Agreements' (2017) GJIL 408, 413-17.
[127] TTP art 14.8(2) <https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf> accessed 12 May 2021.
[128] TTP Agreement, art 14.8(5).
[129] Burri (n 121) 434.
[130] See n 35.
[131] Svetlana Yakovleva, 'Should fundamental rights to privacy and data protection be a part of the EU's international trade "deals"?' (2018) 17(3) WTR 477, 490.

the end, not only did solution-finding become hard and time-consuming due to the divergence between trade partners (especially the EU and the US[132]) over multiple ground issues in the area of digital trade, but the international trade system might not be able to be adaptive enough to undertake the task of balancing trade and human rights.

5.3 Going forward with hesitancy

Convention 108 is signed mostly by European countries and several non-EU countries. It was signed to protect individuals against the processing of personal data and seeks to regulate cross-border data flow. No other binding international agreement is in negotiation or signed to pursue the same objective. Adequacy decision is still the main instrument the Commission is actively trying to utilize to approach cross-border data transfer in order to protect the rights of EU data subjects.[133]

However, provisions about the protection of personal data from cross-border data flows incurred by digital trade have been included in the proposal of free trade agreements from the EU side. Although the EU did not intend to pursue an ultimate mutual solution for cross-border data flows in those provisions, the possibility to regulate data flows under trade agreements has been opened. It is nevertheless difficult to reconcile the autonomy of data protection in the EU legal system with the trade objectives pursued in the trade agreements.

Article 16 of TFEU obliges the EU to protect personal data and the Charter has stipulated the rights to privacy and data protection as fundamental rights in the EU. The level of protection to personal data in the EU is thus very high and that kind of protection given is not conditional upon any other legal basis. It can never be secondary to other interests such as trade. The balance between fundamental rights and the need to facilitate trade is also very hard to make. With the EU holding data protection as fundamental rights, there is not much leeway to bargain and even, for the EU to make compromises, as usually needed in trade negotiations. This perhaps explains why the EU, in the proposal for data protection provisions in FTAs, did not go a little further than reiterating each Party's power to adopt and maintain safeguards for cross-border data transfer. It is probably not easy to strike a bilateral deal when other third countries do not regard data protection as a fundamental right. The fact that EU also lacked explicit competence in enforcing human rights also makes it more complicated when it comes to negotiating deals involving them.

---

[132] Burri (n 121) 413-35.

[133] On 30 March 2021, adequacy talks were concluded with South Korea and the Commission will soon launch the decision-making procedure to adopt the adequacy decision. See Joint Statement by Commissioner Reynders and Yoon Jong In, Chairperson of the Personal Information Protection Commission of the Republic of Korea. <https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1506> accessed 10 May of 2021.

Large amounts of personal data cross borders as a result of the stark development of digital trade. However, to put the individual rights of data subjects at the same level with trade interests for these two to be balanced in a trade agreement, is nevertheless still imaginary. On the one hand, the third countries would lack the will and legal connotation from their legal regimes to do so. There is also no international consensus in this respect. On the other hand, to waive or compromise the fundamental right of data protection and to subject such right to the balance against trade interests according to a standard not totally European, are not really an option.

It is understandable, therefore, that the EU has chosen adequacy decision—an imperfect but practicable tool with extraterritorial effect. At this stage, adequacy decision may have the effect of formulating international consensus and setting standards for data protection while fulfilling its primary job to safeguard the rights of EU data subjects. It is still possible that trade agreements could become a useful tool in asserting necessary safeguards for data transferred as a result of digital trade, the need of which is real and strong. The EU will certainly approach cross-border data transfer through trade agreements with hesitancy—the high standard of data protection as a fundamental right is unique.

6 Conclusion

The need for trade translates into the need for cross-border data transfer in the era of digital trade. While enforcement of data protection measures may restrict the free flows of personal data, more trust on privacy and protection of personal data and the increase of interoperability of regulatory frameworks with regard to cross-border data transfer can in turn contribute to growth of cross-border trade.[134]

The EU has been a supporter for the free movement of information.[135] But the EU also recognizes privacy and protection of personal data as fundamental rights in the EU. The protection afforded to the data subjects whose personal data is transferred to third countries should not be undermined. This is an important principle established by the EU's data protection regime[136] and necessary to keep the integrity and the uniform standard of data protection in the EU.

Adequacy decision is designed to guarantee the level of protection for EU data subjects but also to promote EU standards of data protection globally. Such an instrument exposed its deficiencies and inconsistency when approached by the Commission after two adequacy decisions authorising data transfer to the US have failed to comply with the GDPR and the Charter, rejected by the CJEU on the interference to fundamental rights on national security grounds. The comparison needed to find adequacy is difficult to operate and application of EU standards to third countries cannot always result in equivalence. With the US having rather distinct concepts and regime of data protection, the extraterritorial effect of adequacy decision is stranded, and risks being downgraded to a "formality".

Adequacy decision is being made through dialogue and negotiation with third countries. The push behind the engagement of third countries in making commitments to fulfil the requirements of adequacy nevertheless includes at least the interests of trade facilitation. The adequacy decision regarding the data transfer to Japan was an example of a third country actively moving towards EU standards and reforming its data protection regime under the influence of the GDPR. However, it was also an example where trade interests pushed the making of a mutual adequacy deal. This decision might be exceptional since Japan set up special rules for the personal data of EU data subjects transferred there. And there are flaws and thus possibilities that this decision may not fully comply with the legal

---

[134] Vincenzo Spiezia and Jan Tscheke, 'International Agreements on Cross-Border Data Flows And International Trade: A Statistical Analysis' (2020) OECD Science, Technology and Industry Working Papers, 6 < https://dx.doi.org/10.1787/b9be6cbf-en> accessed 12 May 2021.

[135] 2016 OECD Ministerial Declaration on the Digital Economy. <https://www.oecd.org/sti/ieconomy/Digital-Economy-Ministerial-Declaration-2016.pdf> accessed 12 May 2021.

[136] GDPR, art 44.

requirements under the GDPR and the Charter. Moreover, with the US not willing to join the EU standards and adequacy decision not being able to bind anyone other than the EU, adequacy decision may not fulfil its fundamental task of guaranteeing the level of protection given to EU data subjects after the transfer of personal data to third countries. Therefore, the limitations of adequacy decision as an instrument to regulate cross-border data transfer have been exposed and are reconcilable due to its *per se* nature.

Article 3(2) of TFEU stipulated that "the Union shall also have exclusive competence for the conclusion of an international agreement when its conclusion is provided for in a legislative act of the Union or is necessary to enable the Union to exercise its internal competence, or in so far as its conclusion may affect common rules or alter their scope". Article 50 of the GDPR right now has not included the conclusion of an international agreement for the cooperation of data protection into one of the steps it shall take for international cooperation as defined by that article. Therefore, it is not provided for by the GDPR to conclude such an agreement with other third countries. Neither is there an international consensus for a common and universally applicable standards and concepts of data protection.

However, it remains to be seen whether one day there will be a need urgent enough for the EU to determine that the protection of personal data transferred from the EU to the outside world is necessary to the exercise of EU's internal competence of enforcing common rules of data protection, due to the large amount of data transfers taking place as a result of the development of digital trade. The link between the internal and external spheres of the protection of personal data from the EU is not difficult to establish[137] whilst the international standard of data protection is. As for the major obstacle exposed by the Court of Justice—which is the national security concern due to the government access to data, multilateral cooperation on legal controls of surveillance measures is desired but a deal is not expected to be made in the near future.[138]

The close relationship of trade and data protection also provides the possibility to enforce rules for the protection of personal data transferred internationally through trade agreements. Although such an approach would provide a steady and bilaterally binding channel and more legal certainty, the priority of trade interests inherent in such an approach seems to be incompatible with the autonomy of data protection regime in EU's legal system and the principles enshrined by the fundamental rights. It is also

---

[137] Data transfer rules aims to maintain the level of protection based on EU standards by applying to data processing taking place outside the EU in order to prevent the circumvention of EU data protection standards. See Christopher Kuner, 'Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection' (2021) University of Cambridge Faculty of Law Research Paper No. 20/2021, 23 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850> accessed 20 May 2021.

[138] Propp (n 81).

difficult for the EU to negotiate and make compromise as trade negotiations usually require, with its view of privacy and data protection as fundamental rights in the EU. In reality, the EU has not gone too far with this approach.

It is wise for the EU to adopt adequacy decisions to globalise the EU standards. However, the appropriation of global standards cannot be realized as the US are not willing to join. The attempts of the Commission made in finding adequacy of data protection in the US failed in front of the CJEU and further exposed the potential of making adequacy decision a "formality" by the insistence of the Commission on such an approach to EU-US data transfer, pushed by the force of trade.[139] Such insistence would endanger the integrity of the fundamental rights of data subjects in the EU and thus the uniformity of rules and enforcement of data protection within the Internal Market. The EU must have a consistent approach to cross-border data transfer. Whichever instruments the EU decides to make use of in approaching EU-US data transfer, the principle that the level of protection of personal data of the data subjects in the EU should not be undermined, must be upheld.

[139] Discussion of successor arrangement to Privacy Shield Framework has started between the EU and the US. See 'Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo' (*Press release of the European Commission* 25 March 2021) <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443> accessed 13 May 2021.

Bibliography

Books

Hijmans H, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (Law, Governance and Technology Series vol31, Springer 2016)

Jay R, *Guide to The General Data Protection Regulation: A Companion to The Data Protection Law and Practice* (Sweet and Maxwell 2017)

Kuner C, *Transborder data flows and data privacy law* (OUP 2013)

Lynskey O, *The Foundations of EU Data Protection Law* (OUP 2015)

Articles

Bignami F, 'European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining' (2007) 48(3) BCLR 609

Bradford A, 'The Brussels Effect' (2012) 107(1) NULR 1

Burri M, 'The Regulation of Data Flows Through Trade Agreements' (2017) GJIL 408

Chander A, 'Is Data Localization a Solution for *Schrems II*?' (2020) 23(3) JIEL 771

Dai L, 'A Survey of Cross-Border Data Transfer Regulations Through the Lens of The International Trade Law Regime' (2020) 52(3) NYUJILP 955

Dimitrova A and Brkan M, 'Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair' (2018) 56(4) JCMS 751

Drechsler L, 'Comparing LED and GDPR Adequacy: One Standard Two Systems' (2020) 1(2) GPLR 93

Goldstein D and others, 'Understanding the EU–US "Privacy Shield" Data Transfer Framework' (2016) 20(5) JIL 17

Guamán D, Del Alamo J and Caiza J, 'GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps' (2021) 9 IEEE Access 15961 < https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9328756> accessed 24 February 2021

Kazzi H, 'Digital Trade and Data Protection: The Need for a Global Approach Balancing Policy Objectives' (2020) 4(2) EJELS 42

Kuner C, ‘Reality and Illusion in EU Data Transfer Regulation Post *Schrems*’ (2017) 18(4) GLJ 881

——‘Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU’s Ambition of Borderless Data Protection’ (2021) University of Cambridge Faculty of Law Research Paper No. 20/2021 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850> accessed 20 May 2021

——‘Developing an Adequate Legal Framework for International Data Transfers’ (2009) 263 in: S.Gutwirth and others, *Reinventing Data Protection?*(Springer 2019)

Mitchell A and Mishra N, ‘Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute’ (2019) 22 Journal of International Economic Law 389

Pfisterer V, ‘The Right to Privacy - A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy’ (2019) 20 German LJ 722

Philouze A, ‘The EU-US Privacy Shield: Has Trust Been Restored?’ (2017) 3(4) EDPL 463

Richards N, ‘The Dangers of Surveillance’ (2013) 126 (7) HLR

Rustad M and Kulevska S, ‘Reconceptualizing The Right to Be Forgotten to Enable Transatlantic Data Flow’ (2015) 28(2) Harvard Journal of Law & Technology 349

Schröder C and others, ‘German DPAs Add Further Pressure to E.U.-U.S. Data Transfers’ (2016) 28(1) IPTLJ 17

Spiezia V and Tscheke J, ‘International agreements on cross-border data flows and international trade’ (2020) OECD Science, Technology and Industry Working Papers < https://doi.org/10.1787/b9be6cbf-en> accessed 24 February 2021

Stoddart J, Chan B and Joly Y, ‘The European Union’s Adequacy Approach to Privacy and International Data Sharing in Health Research’ (2016) 44(1) Journal of Law, Medicine & Ethics, Spring 143

Suda Y, ‘Japan’s Personal Information Protection Policy Under Pressure: The Japan-EU Data Transfer Dialogue and Beyond’ (2020) 60(3) Asian Survey 510

Voss W, ‘Cross-Border Data Flows, the GDPR, and Data Governance’ (2020) 29 Wash Int'l LJ 485

Wang F, ‘Cooperative Data Privacy: The Japanese Model of Data Privacy and The EU-Japan GDPR Adequacy Agreement’ (2020) 33(2) HJLT 661

Yakovleva S, ‘Should fundamental rights to privacy and data protection be a part of the EU's international trade "deals"?’ (2018) 17(3) WTR 477

Zalnieriute M, ‘Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU ‑ Canada PNR Agreement’ (2018) 81(6) MLR 1046

Newspapers

——‘The world’s most valuable resource is no longer oil, but data’ *The Economist* (London, 6 May 2017) < https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 27 March 2021

Chee F, ‘New EU-U.S. data transfer pact? Not any time soon, says EU privacy watchdog’ *Reuters* (4 December 2020) <https://www.reuters.com/article/eu-privacy-idUSKBN28E2JQ> accessed 20 May 2021

Confessore N, ‘Cambridge Analytica and Facebook: The Scandal and the Fallout So Far’ New York Times (New York, 4 April 2018) < https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html> accessed 19 May 2021

Wong J and Paul K, ‘Twitter hack: accounts of prominent figures, including Biden, Musk, Obama, Gates and Kanye compromised’ The Guardian (London, 16 July 2020) < https://www.theguardian.com/technology/2020/jul/15/twitter-elon-musk-joe-biden-hacked-bitcoin> accessed 19 May 2021

Official publications

—— 2016 OECD Ministerial Declaration on the Digital Economy. <https://www.oecd.org/sti/ieconomy/Digital-Economy-Ministerial-Declaration-2016.pdf> accessed 12 May 2021

—— Bundesverfassungsgericht, ‘In their current form, the Federal Intelligence Service’s powers to conduct surveillance of foreign telecommunications violate fundamental rights of the Basic Law’ (Press Release No. 37/2020, 19 May 2020) <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html> accessed 26 May 2021

—— Congressional Research Service, ‘Digital Trade and U.S. Trade Policy’ (2017), 20 < https://epic.org/crs/R44565.pdf> accessed on 26 March 2021

—— OECD, ‘Trade in the Digital Era’ (2019) OECD Going Digital Policy Note <www.oecd.org/going-digital/trade-in-the-digitalera.pdf.> accessed 12 May 2021

—— OECD, OECD Privacy Guidelines < http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> Accessed 25 February 2021

Casalini F and González J, 'Trade and Cross-Border Data Flows' (2019) OECD Trade Policy Papers, 27 <https://doi.org/10.1787/b2023a47-en.> accessed 12 May 2021

Draft decision on the adequate protection of personal data by the United Kingdom: Law Enforcement Directive <https://ec.europa.eu/info/sites/default/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_19_feb_2020.pdf> accessed on 6 May 2021

Patel O and Lea N, 'EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows' (UCL European Institute Policy Paper 2020) <https://iapp.org/media/pdf/resource_center/eu_us_privacy_shield_brexit_data_flows_uclei_june_2020.pdf> accessed 26 March 2021

Spiezia V and Tscheke J, 'International Agreements on Cross-Border Data Flows And International Trade: A Statistical Analysis' (2020) OECD Science, Technology and Industry Working Papers, 6 < https://dx.doi.org/10.1787/b9be6cbf-en> accessed 12 May 2021

Weiss M and Archick K, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield' (2016) Congressional Research Service, 3 <https://fas.org/sgp/crs/misc/R44257.pdf> accessed 12 May 2021

Websites and blogs

—— Statcounter, 'Social media stats in Europe - April 2021' < https://gs.statcounter.com/social-media-stats/all/europe> accessed 26 March 2021

Brill J, Assuring Customers About Cross-Border Data Flows (*Microsoft Blogs*, 16 July 2020) < https://blogs.microsoft.com/eupolicy/2020/07/16/assuring-customers-about-cross-border-data-flows/> accessed 12 May 2021

Facebook, 'Facebook data policy' <https://www.facebook.com/about/privacy/update> accessed 25 March 2021

Google, 'Google privacy& terms' <https://policies.google.com/privacy/frameworks?hl=en> accessed 25 March 2021

Propp K, 'Transatlantic Data Transfers: The Slow-Motion Crisis' (*Council on Foreign Relations*, 13 January 2021) <https://www.cfr.org/report/transatlantic-data-transfers> accessed 20 May 2021

Table of Cases

CJEU

C-518/07 *Commission v Germany* [2010] ECLI:EU:C:2010:125

22/70 *Commission of the European Communities v Council of the European Communities* [1971] ECLI:EU:C:1971:32

C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd* [2020] ECLI:EU:C:2020:559

C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications* [2014] ECLI:EU:C:2014:238

C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317

C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* [2020] ECLI:EU:C:2020:791

C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650

C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2020] ECLI:EU:C:2020:790

C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016] ECLI:EU:C:2016:970

C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECLI:EU:C:2003:294

Opinion1/94 of the Court of 15 November 1994 [1994] ECLI:EU:C:1994:384

Opinion 1/03 of the Court (Full Court) of 7 February 2006 [2006] ECLI:EU:C:2006:81

Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017 [2017] ECLI:EU:C:2017:592

European Court of Human Rights

Association '21 December 1989' and Others v Romania App no 33810/07 (ECtHR 24 May 2011)

Klass and Others v Germany App no 5029/71 (ECtHR, judgment of 6 Sep 1978)

Rotaru v Romania App no 28341/95 (ECtHR, 4 May 2000)

Segerstedt-Wiberg and Others v Sweden App no 62332/00 (ECtHR 6 June 2006)

United States

Katz v. United States, 389 U.S. 347 (1967)

United States v United States District Court for the Eastern District of Michigan, 407 U.S. 297 (1972)

United States v Truong Dinh Hung, US Court of Appeals for the Fourth Circuit, 629F.2nd 908 (4th Cir. 1980)

Table of legislation

Regulations

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 [2016] OJ L119/1

Directives

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

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11

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 L119/89

Decisions

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7

Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [2001] OJ L181/19

Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries [2004] OJ L385/74

Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council [2010] OJ L39/5

Council Decision 2010/412/ of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program [2010] OJ L195/3

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 [2016] OJ L207/1

Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information [2019] OJ L76/1

Table of international treaties, conventions, official papers and policy documents

International treaties and conventions

Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences [2016] OJ L336/3

Charter of Fundamental Rights of the European Union [2012] OJ C326/391

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

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

Treaty establishing the European Economic Community [1957] available at < https://ec.europa.eu/romania/sites/default/files/tratatul_de_la_roma.pdf>

Official papers and policy documents

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

Communication from The Commission to The European Parliament and The Council Exchanging and Protecting Personal Data in a Globalised World COM (2017) 7 final

EU Proposal for a Digital Trade Title, explanatory note-January 2019, Negotiations on a Deep and Comprehensive Free Trade Agreement (DCFTA) between the European Union and Tunisia. <https://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157646.01.24%20-%20Factsheet%20-%20Digital%20Trade%20EN%20.pdf> accessed 21 April 2021

EU proposal for provisions on Cross-border data flows and protection of personal data and privacy <https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf> accessed 21 April 2021

EU provisions on Cross-border data flows and protection of personal data and privacy in the Digital Trade Title of EU trade agreements, explanatory note-July 2018, 5th Round of Trade Negotiations between the European Union and Indonesia.

<https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157129.pdf> accessed 21 April 2021

Report from The Commission To The European Parliament And The Council on the third annual review of the functioning of the EU-U.S. Privacy Shield COM(2019) 495 final <https://ec.europa.eu/info/sites/default/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf> accessed 13 May 2021