Schrems Cases: Are Rules Clarified?

Ke Xu

Master's Thesis in European and International Trade Law

HARN63

2022

LUND UNIVERSITY

SCHOOL OF ECONOMICS AND MANAGEMENT

Table of Contents

Abstract

According to General Data Protection Regulation (GDPR), there are “equivalent adequate” (Article 45), “appropriate safeguards” (Article 46), “derogations” (Article 49) as options to perform the cross-border data transfer. Privacy Shield, together with its predecessor Safe Harbor, was introduced with the purpose to facilitate the data transfer between EU and the United States in compliance with EU laws. The data transfers made under the Safe Harbor and Privacy Shield were deemed to meet the “equivalent adequate” requirements, and thus relied by business organizations as the legal basis. The Edward Snowden leaks put the surveillance programs of the United States under the focusing light and such trigger point finally led to the invalidation of Safe Harbor and Privacy Shield by the Courts of Justice of the European Union (CJEU) in Schrems I and II respectively in 2015 and 2020.

In the absence of “equivalent adequate” protection, the most commonly used legal mechanism is Standard Contractual Clauses (SCCs) as “appropriate safeguards”. Originally the data exporter only attached the SCCs in the agreement with importer without need to make further assessment of the legal regime and data protection in the country of importer. After Schrems, Although SCCs were not invalidated by CJEU, but they were decided as insufficient by themselves and thus must have “supplementary safeguards” to reach the level of “equivalent adequate” protection. However, the CJEU did not further clarify what are “supplementary safeguards”, which brought legal uncertainty to the EU-U.S. cross-border data transfer and was arguably by critics to obscure the differences between “equivalent adequate” and “appropriate safeguards”.

The two main “derogation” are consent and necessity. Although the CJEU pointed out that there would be no “legal vacuum” in the absence of adequacy and safeguards, the strictly necessary application conditions have made such “derogation” applied only in limited circumstances.

Abbreviations

BCR	Binding Corporate Rules
CJEU	The Courts of Justice of the European Union
Charter	Charter of Fundamental Rights of the European Union
DPD	Data Protection Directive
DOT	Department of Transportation
EDPB	European Data Protection Board
E.O. 12333	Executive Order 12333
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FTC	Federal Trade Commission
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
NSA	National Security Agency
PCLOB	Privacy and Civil Liberties Oversight Board
PPD-28	Presidential Policy Directive 28
PRISM	Surveillance Program
UPSTREAM	Surveillance Program
SCCs	Standard Contractual Clauses
SMEs	Small and Medium size Enterprises

1. Introduction

1.1 Background

"Cross-border data flows" refers to the movement or transfer of information between computer servers across national borders. Such data flows underlie today's globally connected world and are essential to conducting international trade and commerce. Cross-border data flows enable people and companies to transmit information for online communication, track global supply chains, share research, provide cross-border services, and support technological innovation.[1] The General Data Protection Regulation (GDPR) entered into force on 24 May 2016, replaced the 1995 Data Protection Directive (DPD) and applies since 25 May 2018, which is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. A single law will also do away with the current fragmentation in different national systems and unnecessary administrative burdens.[2]

The United States and the European Union (EU) share an extensive trade and investment relationship and are each other's most important commercial partners for digitally-enabled services. Cross-border data flows between the United States and EU are the highest in the world and are integral to much of the U.S.-EU economic relationship.[3] According to the U.S. Bureau of Economic Analysis, U.S.-EU trade in information and communications technology (ICT) services and potentially ICT-enabled services was estimated to be over $264 billion in 2020.[4] Two of the top five e-commerce retailers in Europe in 2020 were U.S. firms Amazon and Apple.[5] One report stated that a loss of cross-border data flows on exports from the EU's data-reliant sectors would lead to an annual reduction in the EU's gross domestic product (GDP) worth at least €330 billion (roughly $388 billion), or around 2.5% of total EU GDP.[6] A total ban on such data transfers could lead to a 31% decline in digital service imports from the United States.[7]

There are fundamental differences in the U.S. and EU approaches to data privacy and protection. EU

[1] Kristin Archick, Rachel F. Fefer, U.S.-EU Privacy Shield and Transatlantic Data Flows, 22 September 2021, Congressional Research Service, R46917 p. 4.
[2] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en accessed 27 May 2022.
[3] Archick, p. 5.
[4] U.S. Bureau of Economic Analysis, Table 3.3. U.S. Trade in ICT and Potentially ICT-Enabled Services, by Country or Affiliation.
[5] Retail-Index, Top 100 E-Commerce Retailers in Europe, https://www.retail-index.com/E-commerceretail.aspx accessed 17 April 2022.
[6] Frontier Economics, "The Value of Cross-Border Data Flows to Europe: Risks and Opportunities," June 2021.
[7] European Centre for International Political Economy and Kearney Global Business Policy Council, "The Economic Costs of Restricting the Cross-border Flow of Data," July 2021.

concerns about how the United States handles personal data have posed challenges in U.S.-EU economic and security relations and, at times, have disrupted U.S.-EU data flows. At the same time, many U.S. stakeholders describe the EU's data privacy and protection regime as overly restrictive for efficient cross-border data flows.[8] With the purpose to prevent the disruption of the cross-border data flow, the United States and EU negotiated and reached the Safe Harbor Privacy Principles (Safe Harbor) in 2000 and its successor agreement the Privacy Shield in 2016, however, both were invalidated by the Court of Justice of the European Union (CJEU) in 2015 and 2020 respectively. The invalidation of the Privacy Shield framework may result in a 5% to 6% reduction in imports and exports of digital services and lead to €19-31 billion ($22-36 billion) in lost EU economic output annually.[9] The Privacy Shield had 5,380 participants, 75% of which were Small and Medium size Enterprises (SMEs). The participants include U.S. businesses and other organizations, U.S. subsidiaries in Europe, and 250 entities headquartered in Europe. By June 2021, about a year after the Schrems II decision, many sought alternatives or opted to exit the EU market.[10]

The Biden Administration is negotiating with the EU on an enhanced successor accord to Privacy Shield and have expressed hope that a new agreement will help bolster U.S.-EU relations and address U.S. business demands for durable, protected transatlantic data flows.[11]

1.2 Purpose and Research Question

As the background section above indicates, the transatlantic data flows play key role in international trade. According to GDPR chapter V, which regulates the cross-border data flow, there are some options could be used as legal basis for business organizations to transfer data out of EU. The purpose of this paper is to describe and analyze some options, "equivalent adequate" protection, SCCs and BCRs as "appropriate safeguards", and "consent or necessity derogations" as the most used and fundamental options for legal mechanisms of transatlantic data flows from EU to the United States.

To fulfill such purpose, the CJEU judgments in Schrems cases should not be neglected and maybe are the most decisive cases until now, which provide the opportunity to understand how these transatlantic data flow legal mechanisms interpreted by the CJEU. In general, the CJEU invalidated the Safe Harbor and Privacy Shield for the reason that both frameworks did not provide "equivalent

[8] Archick, Supra 1, p. 2.
[9] European Centre for International Political Economy and Kearney Global Business Policy Council, "The Economic Costs of Restricting the Cross-border Flow of Data" July 2021.
[10] Privacy Shield list, data pulled on 10 June 2021, https://www.privacyshield.gov/list accessed 18 April 2022.
[11] Archick, Supra 1, p. 1.

adequate" protection. Although SCCs were not invalidated by the CJEU, they were decided as insufficient by themselves and thus must have "supplementary safeguards" to reach the level of "equivalent adequate" protection. The CJEU also held there would be no "legal vacuum" even in the absence of adequacy and safeguards. Therefore, the research question of this paper would be: under what conditions can personal data be transferred from the EU to the U.S. in accordance with EU data protection law as interpreted in the CJEU Schrems cases?

1.3 Delimitation

There are other legal options under GDPR to transfer data such as approved codes of conduct and accredited third-party certifications, "derogations" for the purpose of performance of a contract or important reasons of public interest, legitimate interests of a company, etc. For some companies, data localization is also one of the choices to avoid the risks of legal uncertainty and burden of compliance especially after Schrems. International organizations are also negotiating multilateral agreement and framework. Due to the limited size, this paper only focuses on the CJEU interpretations regarding "equivalent adequate" protection, SCCs and BCRs as "appropriate safeguards", and "consent or necessity derogations" in Schrems cases, there is no intention to exhaust all cross-border data transfer theories or practices.

1.4 Method and Materials

As mentioned in purpose and research question, in order to describe and analyze the "equivalent adequate" protection, SCCs and BCRs as "appropriate safeguards", and "consent or necessity derogations" under GFPR chapter V, this paper uses method of legal-dogmatic research. To begin with descriptions of the relevant EU statues, DPD, GDPR and Charter of Fundamental Rights of the European Union, and brief introduction of the U.S. surveillance rules which are the main obstacles and reasons for the CJEU's judgments invalidating the Safe Harbor and Privacy Shield, this paper goes on to the key cases, Schrems I and II, and summaries the rationales and decisions of the CJEU. After providing the necessary information about statues and cases, this paper makes analyses from several perspectives regarding the judgments, including the relationship between adequate protection and supplementary safeguards, the unchanged national security challenges read in the context of the Charter, the EDPB and EU commission's efforts by updated SCCs and guidelines, and the limited application of derogations. During such analyses, this paper consults and collects information from the official publications, scholar comments and literatures, law journals and websites as inspirations and supporting materials to draw final conclusions.

1.5 Outline

Chapter 2 reviews the CJEU decisions in Schrems I and II invalidating the Safe Harbor and the Privacy Shield respectively. Chapter 3 discusses the “equivalent adequate”, “supplementary safeguards” and “derogations”. Chapter 4 reaches the conclusions.

2. From Schrems I to Schrems II, the invalidation of Safe Harbor and Privacy Shield

2.1 EU Data Protection Rules on Cross-border Data Flow

2.1.1 Data Protection Directive (DPD)

The Data Protection Directive (DPD) provides "The Member States shall provide that the transfer to a third country of personal data … may take place only if…the third country in question ensures an adequate level of protection…The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding…Member State may authorize…transfers of personal data to a third country which does not ensure an adequate level of protection…where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals…such safeguards may in particular result from appropriate contractual clauses".

2.1.2 General Data Protection Regulation (GDPR)

Although DPD was repealed and replaced by the General Data Protection Regulation (GDPR), which took effect in 2018, the rules on cross-border data flow were in essence reproduced and references to DPD shall be construed as references to GDPR. There are "equivalent adequate" (Article 45), "appropriate safeguards" (Article 46), "derogations" (Article 49) as options to perform the cross-border data transfer. GDPR provides "A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country…ensures an adequate level of protection…When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the rule of law, respect for human rights and fundamental freedoms, relevant legislation…effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects...the existence and effective functioning of one or more independent supervisory authorities…with responsibility for ensuring and enforcing compliance with the data protection rules…In the absence of a decision pursuant to Article 45(3) (adequate level of protection), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available…The appropriate safeguards may be provided for…standard

data protection clauses adopted by a supervisory authority and approved by the Commission…In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, a transfer or a set of transfers of personal data to a third country or an international organization shall take place only on one of the following conditions: (a) the data subject has explicitly consented to the proposed transfer…(b) the transfer is necessary for the performance of a contract…"

The contractual clauses ensuring appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries. This includes model contract clauses – so-called standard contractual clauses (SCCs) – that have been "pre-approved" by the European Commission. The most popular tool for third-country data transfers is reported to be SCCs. In order to rely on SCCs, data exporters must include the data protection clauses in their contracts with relevant data importers in order to impose legal obligations on both parties.[12]

2.1.3 Charter of Fundamental Rights of the European Union

The EU considers the privacy of communications and the protection of personal data to be fundamental rights. These rights are contained in Articles 7 and 8 of the 2000 Charter of Fundamental Rights of the European Union (Charter) and made binding on all EU members through the 2009 Treaty of Lisbon (the EU's most recent institutional reform treaty). Furthermore, Article 52 of the Charter holds that any limitations on such rights must be subject to the principle of proportionality, while Article 47 provides the right to judicial redress for infringements.[13]

2.2 U.S. Surveillance Rules

Under the U.S. Constitution, ensuring national security falls within the President's authority. The President may direct the activities of the U.S. Intelligence Community, in particular through Executive Orders or Presidential Directives, the two central legal instruments in this regard are Executive Order 12333 (E.O. 12333) and Presidential Policy Directive 28 (PPD-28). PPD-28 imposes a number of limitations for intelligence operations with binding force on U.S. intelligence authorities. E.O. 12333 allows the National Security Agency (NSA) to access data 'in transit' to the

[12] Maria Helen Murphy, Assessing the Implications of Schrems II for EU–US Data Flow, International and Comparative Law Quarterly, Cambridge University Press, 2021, p. 249.
[13] Archick, Supra 1, p. 2.

United States, by accessing underwater cables on the floor of the Atlantic, and to collect and retain such data before arriving in the United States.[14]

Section 702 of the Foreign Intelligence Surveillance Act (FISA) permits the Attorney General and the Director of National Intelligence to authorize jointly, following Foreign Intelligence Surveillance Court (FISC) approval, the surveillance of individuals who are not United States citizens located outside the United States in order to obtain 'foreign intelligence information'. It does not authorize individual surveillance measures but surveillance programs like PRISM and UPSTREAM on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence. The certifications to be approved by the FISC contain no information about the individual persons to be targeted but rather identify categories of foreign intelligence information.[15]

In the context of the PRISM programme, Internet service providers are required, according to the findings of that court, to supply the NSA with all communications to and from a 'selector', some of which are also transmitted to the FBI and the Central Intelligence Agency (CIA). As regards the UPSTREAM programme, telecommunications undertakings, as the network of cables, switches, and routers, are required to allow the NSA to copy and filter Internet traffic flows in order to acquire communications from, to or about a non-US national associated with a 'selector'. Under that programme, the NSA has access both to the metadata and to the content of the communications concerned.[16]

2.3 Safe Harbor

The EU has never recognized the U.S. data protection system as adequate. This is partly because of the lack of comprehensive, federal privacy legislation. European DPAs argued that "the current patchwork of U.S. laws and self-regulation is not adequate".[17] However, driven by the economic importance of EU-U.S. digital trade, and the data flows which underpin this, the European Commission has been flexible and pragmatic in finding ways to maintain unhindered EU-U.S. data flows.[18] In 2000, after two years of negotiation with the U.S., the European Commission issued the Decision 2000/520 (Safe Harbor).[19] A U.S. company or organization could self-certify annually to

[14] 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, recital 68.
[15] Ibid recital 109.
[16] CJEU Judgement of 16 July 2020 in Case C-311/18, *Facebook Ireland and Schrems,* ECLI:EU:C:2020:559, para 61-63.
[17] Paul Schwartz and Karl-Nikoloaus Peifer, "Transatlantic Data Privacy" (2017) The Georgetown Law Journal, p. 118.
[18] Paul Schwartz, "Global Data Privacy: The EU Way" (2019) NYU Law Review, p. 786.
[19] Commission Decision 2000/520/EC of 26 July 2000, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce.

the Department of Commerce that it was in compliance with seven basic privacy principles (notice, choice, onward data transfer, security, data integrity, access, and enforcement) and related requirements deemed necessary to meet the EU's data protection adequacy standards.[20] This policy innovation meant that certified U.S. companies, and even entire sectors, could enjoy the de facto benefits of an adequacy decision, without there being a full adequacy decision in place.[21] Safe Harbor was of tremendous economic benefit to U.S. technology firms, which developed lucrative business models tapping into European markets – predicated on unrestricted EU-U.S. data flows.[22]

2.4 Schrems I

The Edward Snowden leaks of May 2013 represented a pivotal moment in the history of EU-U.S. data flows. Edward Snowden revealed the mass surveillance programmes of the U.S. National Security Agency (NSA), many of which directly implicated EU citizens.[23] Mr. Schrems, as a user of Facebook, made a complaint that his personal data was transferred to Facebook Inc located in the United States. He contended the law and practice in force in U.S. did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities. Mr. Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, in particular those of NSA.[24] The High Court (Ireland), before which Mr. Schrems had brought judicial review proceedings against the rejection of his complaint, made a request to the CJEU for a preliminary ruling, known as Schrems I, on the interpretation and validity of Safe Harbor.

In the CJEU's ruling, the Court found that when assessing whether the data protection regime of a third country meets the requirements for adequacy, the level of protection required should be 'essentially equivalent'.[25] However, since Decision 2000/520 did not state that the United States 'ensures' an adequate level of protection, there was no need to examine the content of the Safe Harbor principles.[26] The Court found that the European Commission failed to examine U.S. domestic laws or international commitments (as required by the DPD) prior to issuing its determination that the Safe

[20] Archick, Supra 1, p. 7.
[21] Oliver Patel and Dr. Nathan Lea, EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows, UCL European Institute, May 2020, p. 10.
[22] Henry Farrell and Abraham Newman, "Of Privacy and Power: The Transatlantic Struggle over Freedom and Security" (2019) Princeton University Press, p. 135.
[23] Ibid.
[24] CJEU Judgement of 6 October 2015 in Case C-362/14 Schrems, ECLI:EU:C:2015:650, para 27-28.
[25] Ibid para 73.
[26] Ibid para 97-98.

Harbor principles provided an adequate level of protection for EU citizens' personal data.[27] The Court invalidated the Safe Harbor with the rationales: "United States public authorities are not required to comply with the Safe Harbor…The national security, public interest, or law enforcement requirements have primacy over the Safe Harbor principles…As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter…the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data…as enshrined in Article 47 of the Charter"[28]

At the time of the CJEU's Schrems I decision, approximately 4,500 companies and organizations were participating in Safe Harbor. U.S. officials and business leaders were disappointed by the CJEU's ruling and concerned that it could disrupt data flows from the EU, with significant negative implications for U.S.-EU trade and economic relations.[29] Beyond invalidating Safe Harbor, the Schrems I judgement was significant for several reasons:

- It was the first time an EU data adequacy decision was invalidated.
- It formally established the CJEU as the ultimate arbiter of EU data adequacy decisions.
- It settled questions on the meaning of adequacy, i.e., that the third country's data protection system must be 'essentially equivalent' to the EU's.
- It meant that the European Commission would now assess national security and mass surveillance legislation, frameworks and practices when undertaking adequacy assessments.
- It instructed national DPAs (Data Protection Authorities), like the Irish Data Protection Commission, to investigate issues and complaints even if they concerned 'adequate' countries.[30]

EU data protection authorities, however, announced a four-month grace period during which they agreed to not enforce the Schrems I decision while U.S. and EU officials continued negotiations on a new agreement.[31] The U.S. was generally against restricting data flows, and it pushed for unrestricted data flows when negotiating trade agreements. The European Commission also agreed that EU-U.S. data flows were important, which was why it worked hard after Safe Harbor's invalidation to ensure a new arrangement was quickly put in place.[32] Also, the Commission's Digital

[27] Archick, Supra 1, p. 8.
[28] Supra 19, para 79-98, Also see, Court of Justice of the European Union, "The Court of Justice Declares that the Commission's US Safe Harbor Decision Is Invalid," press release, 6 October 2015.
[29] Archick, Supra 1, p. 8.
[30] Schwartz, Supra 17.
[31] Article 29 Working Party, "Statement of the Article 29 Working Party," press release, 16 October 2015.
[32] Schwartz, Supra 17.

Single Market strategy emphasized the importance of free data flows for trade.[33] Furthermore, the pursuit of harmonized data protection standards via the 1995 Data Protection Directive was in part driven by the Commission's desire to facilitate free flow of data between member states and strengthen the single market.[34]

2.5 Privacy Shield

In February 2016, U.S. and EU officials announced an agreement on a replacement for Safe Harbor—the EU-U.S. Privacy Shield. Similar to the former Safe Harbor accord, the Privacy Shield Framework required compliance with seven basic privacy principles. In contrast to Safe Harbor, however, Privacy Shield sought to address the concerns raised by the CJEU in Schrems I. In July 2016, the European Commission adopted an adequacy decision for Privacy Shield, formally designating the new program as a valid mechanism for transferring personal data for commercial purposes to the United States.[35] The European Commission noted in particular its confidence that "The Commission has assessed the limitations and safeguards available in U.S. law as regards access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities for national security, law enforcement and other public interest purposes. By letter signed by the Secretary of State…the U.S. government has also committed to create a new oversight mechanism for national security interference, the Privacy Shield Ombudsperson, who is independent from the Intelligence Community…any interference by U.S. public authorities with the fundamental rights of the persons whose data are transferred...will be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective [U.S.] legal protection against such interference."[36]

The U.S. government, European Commission and most member states were extremely keen for Privacy Shield to be upheld, considering it a highly useful mechanism.[37] The volume of cross-border data flows between the EU and the U.S. is the highest in the world.[38] Examples like video conferencing tools as Zoom, Skype, Google Hangouts and Cisco Webex routinely transfer EU customer data to U.S. servers for processing and analysis using Privacy Shield. This potentially includes personal data generated by European government and EU officials, who have increasingly

[33] European Commission, "A Digital Single Market Strategy for Europe" (2015).
[34] Lee Bygrave, "Transatlantic Tensions on Data Privacy" (2013) Transworld Working Paper, p. 5.
[35] Ibid p. 9.
[36] 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.
[37] Schwartz, Supra 17, p. 11.
[38] Congressional Research Service, "Digital Trade and U.S. Trade Policy" (2017), p. 20.

used such tools since COVID-19, which has prompted privacy concerns and even calls to use European-headquartered video conferencing companies.[39]

The European Commission and the Department of Commerce conduct annual joint reviews of the program and invite U.S. national intelligence experts and European DPAs to participate. The Federal Trade Commission (FTC) and the Department of Transportation (DOT) enforced compliance.[40] In June 2020, the FTC reported enforcement actions against dozens of companies that made false or deceptive representations about their Privacy Shield participation.[41] The FTC's $5 billion penalty against Facebook included holding executives accountable for privacy-related decisions and prohibiting misrepresentations related to Privacy Shield.[42] The U.S. Department of State Under Secretary of State for Economic Growth, Energy, and the Environment currently serves as the independent Privacy Shield Ombudsperson to handle complaints regarding U.S. government access to personal data.[43] The U.S. Privacy and Civil Liberties Oversight Board (PCLOB), while not formally part of the Privacy Shield arrangement, is responsible for oversight of the implementation of executive branch counterterrorism efforts, including surveillance practices and policies, to ensure that privacy and civil liberties are protected.[44]

2.6 Schrems II

Following the CJEU's Schrems I ruling in 2015 invalidating Safe Harbor, Facebook Ireland said it was transferring most data to its U.S. servers using standard contractual clauses (SCCs). Mr. Schrems was then asked to reformulate his complaint in light of this.[45] Mr. Schrems claimed, inter alia, that United States law required Facebook Inc. to make the personal data transferred to it available to certain United States authorities, such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) and the data was used in the context of various monitoring programmes in a manner incompatible with Articles 7, 8 and 47 of the Charter. He claimed the SCCs Decision cannot justify the transfer of that data to the United States and asked the Commissioner to prohibit or suspend

[39] Vincent Manancourt, "EU Zooms ahead, despite worries over app" (2020) Politico.
[40] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield accessed 20 April 2022.
[41] Lesley Fair, "FTC Settlement Focuses on those Other Privacy Shield Framework Requirements," Federal Trade Commission, 30 June 2020.
[42] "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," Federal Trade Commission 24 July 2019.
[43] https://www.state.gov/privacy-shield-ombudsperson accessed 20 April 2022.
[44] https://www.pclob.gov accessed 20 April 2022.
[45] https://noyb.eu/en/project/eu-us-transfer accessed 21 April 2022.

the transfer of his personal data to Facebook Inc.[46] In 2017 the Irish High Court referred the case, known as 'Schrems II', to the CJEU for a preliminary ruling.

In this Schrems II case, the CJEU held that: "the appropriate safeguards, enforceable rights, and effective legal remedies…must ensure that data subjects…pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union, read in the light of the Charter of Fundamental Rights of the European Union. The assessment of the level of protection must take into consideration both the contractual clauses…and the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.[47]

To answer the question whether the SCCs Decision is capable of ensuring an adequate level of protection given that the standard data protection clauses provided for in that decision do not bind the supervisory authorities of those third countries, the CJEU said "those clauses are not capable of binding the authorities of that third country, since they are not party to the contract… Therefore, the content of those standard clauses might not constitute a sufficient means of ensuring the effective protection of personal data transferred…Article 46(1) of the GDPR provides that, in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. According to Article 46(2)(c) of the GDPR, those safeguards may be provided by standard data protection clauses drawn up by the Commission. However, those provisions do not state that all safeguards must necessarily be provided for in a Commission decision such as the SCC Decision…such a standard clauses decision differs from an adequacy decision…the controller 'should be encouraged to provide additional safeguards … that supplement standard [data] protection clauses'…controller or processor to verify, on a case-by-case basis…whether the law of the third country of destination ensures adequate protection…by providing, where necessary, additional safeguards to those offered by those clauses…the mere fact…SCC Decision, do not bind the authorities of third countries to which personal data may be transferred…cannot affect the validity of that decision."[48]

The next question the CJEU needed to answer was about "the Privacy Shield Decision enables interference based on national security and public interest requirements or on domestic legislation of

[46] CJEU Judgement of 16 July 2020 in Case C-311/18, Facebook Ireland and Schrems, ECLI:EU:C:2020:559, para 61-63.
[47] Ibid para 105.
[48] Ibid para 123-136.

the United States, with the fundamental rights of the persons…More particularly…by US public authorities through the PRISM and UPSTREAM surveillance programmes under Section 702 of the Foreign Intelligence and Surveillance Act (FISA) and E.O. 12333…in order to satisfy the requirement of proportionality… the limitations on the protection of personal data must apply only in so far as is strictly necessary…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…Therefore, the Privacy Shield Decision cannot ensure a level of protection essentially equivalent to that arising from the Charter, contrary to the requirement in Article 45(2)(a) of the GDPR…the Ombudsperson is appointed by the Secretary of State and is an integral part of the US State Department…nothing in that decision to indicate that the dismissal or revocation of the appointment of the Ombudsperson is accompanied by any particular guarantees, which is such as to undermine the Ombudsman's independence from the executive…it is to be concluded that the Privacy Shield Decision is invalid".[49]

[49] Ibid para 150-201.

3. Analysis

3.1 "Unchanged Melody"

The result of Schrems may not be a big surprise. When EU and U.S. officials held their third annual review of the administration and enforcement of Privacy Shield in 2019, the EU cited progress in U.S. oversight and enforcement actions but noted concern about a "lack of oversight in substance" and the need for more checks for onward transfers, issues similar to those cited by the CJEU.[50] Questions even existed at the time of its approval about whether Privacy Shield would go far enough in addressing broader EU concerns about U.S. data protection standards, and whether it would be able to stand up to future legal challenges to it at the CJEU.[51] The Privacy Shield framework did not entail or require any change to U.S. national security, surveillance or data privacy legislation, or stopped the NSA or other U.S. intelligence agencies from conducting surveillance on EU citizens in a way which violated EU law. The fundamental problem of U.S. government access to EU citizens' data has thus not been fully resolved.[52]

The focus on how government agencies access data for national security purposes has always been the key barrier to data flows between the EU and the U.S. for a long time. In both Schrems cases, the issue was U.S. government access to personal data for national security purposes and the rights of EU citizens in the U.S. to judicial review and redress, the CJEU found that the U.S. fell short in that the U.S. was not according EU personal data the protection and rights of redress available in the EU.[53] Article 23 of GDPR provides "Union or Member State law…may restrict by way of a legislative measure the scope of the obligations and rights…when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard (a) national security…". In effect, national security policy remains the sole responsibility of the Member States, each EU Member State is afforded discretion to balance national security needs with data privacy rights, yet the EU is not according to a similar discretion to third countries.[54] One example could be the United Kingdom (UK) Investigatory Powers Act 2016 before Brexit. Such extensive surveillance regime was already the subject of repeated references to the Court of Justice and characterized by a similarly broad surveillance approach to that criticized by the Court

[50] European Data Protection Board, EU-U.S. Privacy Shield - Third Annual Joint Review, 12 November 2019.
[51] Natasha Lomas,"Europe and U.S. Seal Privacy Shield Data Transfer Deal to Replace Safe Harbor," Techcrunch.com, 2 February 2016.
[52] Oliver Patel and Dr. Nathan Lea, EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows, p. 19.
[53] Joshua P. Meltzer, "The Court of Justice of the European Union in Schrems II: The Impact of the GDPR on data flows and national security, Brookings Report", August 2020.
[54] Ibid.

in Schrems II.[55] U.S. government argued that many E.U. Member States had even less intelligence oversight protections than did the United States. In particular, the U.S. government highlighted how European Union Member States afforded individuals more limited judicial review and provided less stringent regulation of both domestic and international clandestine intelligence collection than did the United States.[56] EU countries themselves are not averse to similar surveillance practices, which could potentially target U.S. citizens.[57] As some scholars commented, the European Union has been engaging in exporting a system of rights protections with the purpose to set EU standard as global standard as "Brussels Effect"[58] and the impact of this pattern beyond the borders of EU has become an "effective sovereign" of data protection and privacy.[59] The EU efforts are branded as protectionist and contrary to the worldwide trend for global trade liberalization,[60] which creates unfair trade barriers and limits U.S. firms' access to the EU market, and has the potential to become the de-facto privacy standard of the world.[61]

3.2 "2 Become 1"

Schrems II introduced a new and significant degree of uncertainty into this field of law and the question of what is now necessary to legally continue cross-border data transfers of data.[62] The CJEU appeared to have collapsed the adequacy pathway of Article 45 and the appropriate safeguards test of Article 46 into a single question, that effect of this move has been to reduce all the Chapter V mechanisms into a single adequacy test that is unworkable in practice.[63] According to GDPR, the EU commission determines whether a country outside the EU offers an essentially equivalent level of data protection under adequate test. When assessing whether a third country's law and practice are adequate under the GDPR, the commission has also taken into account a number of other considerations, including the significance of a trading partner, both commercially and in terms of cultural ties to the EU, and strategic objectives in continuing data flows and encouraging legal

[55] A.D. Murray, Data Transfers between the EU and the UK post Brexit? International Data Privacy Law, 2017, p. 158-163.
[56] Dept. of Comm., Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II, Sep 2020, p. 15-17.
[57] Mark Scott, "Privacy Shield Is Stuck" Politico Digital Bridge, 15 July 2021.
[58] A. BRADFORD, The Brussels Effect, in North-Western University Law Review, 2012, p. 107.
[59] T. WU, J. GOLDSMITH, Who Controls the Internet?: Illusions of a Borderless World, Oxford: Oxford University Press, 2006, p. 176.
[60] M Huie, S Laribee and S Hogan, "The Right to Privacy in Personal Data: The EU Prods the US and Controversy Continues" (2002) 9 Tulsa Journal of Comparative and International Law 391, 401.
[61] House Of Representatives, "The EU Data Protection Directive: Implications For The US Privacy Debate: Hearing before the Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce" (8 March 2001) Serial No 107-19.
[62] Marcelo Corrales Compagnucci, Mark Fenwick, Mateo Aboy and Timo Minssen, Supplementary Measures and Appropriate Safeguards for International Transfers of Personal Data after Schrems II, p. 11.
[63] Laura Bradford, Mateo Aboy and Kathleen Liddell, "Standard Contractual Clauses for Cross-Border Transfers of Health Data After Schrems II" (2021) 8(1) Journal of Law and the Bioscience 1.

reform.[64] The CJEU reviewed the provisions of US national security law and concluded that these laws were deficient and inconsistent with the EU Charter of Fundamental Rights, an important effect of this change is to undermine other existing Article 45 adequacy rulings.[65] It seems highly unlikely that Israel, for example, or Argentina or Japan would meet Schrems II's new threshold for law enforcement surveillance.[66] The focus in Schrems II on compatibility with the EU Charter for Article 45 adequacy seems to exclude different approaches to privacy in other countries and restricts the scope for Article 45 adequacy findings more generally.[67] Article 46(1) of the GDPR allows appropriate safeguards to be taken by the controller or processor that "compensate for the lack of data protection in a third country." The CJEU interpreted the word "compensate" in Recital 108 more narrowly to mean capable of ensuring "a level of protection essentially equivalent to that which is guaranteed within the EU.[68] Schrems II could be read as a prohibition on any transfer, whether under Article 45, 46 or another provision of Chapter V, unless the legal rights of EU citizens in third countries are equivalent on every point to those available under EU law. The effect of this approach is to collapse all of Chapter V into a narrowly constructed legal adequacy determination, rather than treat them as a series of different options. All pre-Schrems II adequacy decisions are now suspect since they could be invalidated on the same grounds as the EU-US Privacy Shield adequacy.[69]

3.3 "Don't Stop Till You Get Enough"

Historically as the most commonly used legal mechanism to transfer data from EU to U.S., SCCs were entered by EU-based data exporters with data importers without performing further analysis into the legal regime and data protection principles of the third country to which data are transferred.[70] The SCCs were widely used because, prior to Schrems II, it were seen as an effective and convenient solution that could be used between individual entities and characterized as a "straight forward tick box solution" that is "simple and quick to execute".[71] After Schrems II, SCCs were held not capable of ensuring an adequate level of protection of the personal data transferred to third countries given that the standard data protection clauses do not bind the supervisory authorities of those third countries. Although the CJEU did not invalidated SCCs but held that additional safeguards might be

[64] European Commission Memo/17/15, "Digital Single Market – Communication on exchanging and protecting personal data in a globalized world" (10 January 2017).
[65] Compagnucci, Supra 62, p. 14.
[66] Meltzer, Supra 53.
[67] Meltzer, Supra 53.
[68] Compagnucci, Supra 62, p. 14.
[69] Compagnucci, Supra 62, p. 15.
[70] Joseph Liss, David Peloquin, Mark Barnes, Barbara E. Bierer, Demystifying Schrems II for the cross-border transfer of clinical research data, Journal of Law and the Biosciences, 1–14, p. 4.
[71] Compagnucci, Supra 62, p. 10.

provided by supplementary measures on a case-by-case basis, there is still legal uncertainty as to what specific measures may be adequate enough. As SCCs become "mini adequacy decisions", the complexity of this process may well lead companies, especially smaller ones, to avoid this route entirely. While large firms will be able to afford the expensive legal advice reviewing a foreign nation's surveillance law for compatibility with EU law, smaller firms will not.[72]

In June 2021, the EU Commission updated the SCCs to better reflect GDPR requirements and, in light of the Schrems II decision, to ensure that personal data transferred using SCCs receive a level of protection equivalent to that under EU law.[73] Compared with the prior SCCs, the new one has certain changes including: adds "processor to processor" and "processor to controller" to existing "controller to controller" and "controller to processor" model, permits multiple exporter, allows additional third parties to be added to existing agreement, etc. As the result of Schrems II, a compulsory transfer impact assessment is introduced to evaluate the third country's legal system, and non-exhaustive examples of technical measures as encryption and pseudonymization are suggested.

At the same time, the European Data Protection Board (EDPB) issued recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data with the aim to help exporters assess third countries and identify appropriate supplementary measures where needed. The recommendations provide a non-exhaustive list of examples of supplementary measures like contractual, technical, or organizational in nature. For example, EDPB considers that the encryption performed provides an effective supplementary measure under the conditions including, inter alia, the encryption algorithm conforms to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities; the strength of the encryption and key length takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved; the encryption algorithm is implemented correctly; the keys are reliably managed and retained solely under the control of the data exporter.[74]

Another popular technical supplementary measure is pseudonymization, which means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept

[72] Anupam Chander, Is Data Localization a Solution for Schrems II? Georgetown University Law Center, Journal of International Economic Law, Sep 2020, p. 4.
[73] Standard Contractual Clauses (SCC), European Commission.
[74] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, June 2021, para 84.

separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[75] EDPB considers that the pseudonymization performed provides an effective supplementary measure under the conditions including, inter alia, the additional information is held exclusively by the data exporter and kept separately in a Member State or trusted jurisdiction; disclosure or unauthorized use of that additional information is prevented by appropriate technical and organizational safeguards, it is ensured that the data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information.[76]

Meanwhile, depending on what contractual measures are already included in the Article 46 GDPR transfer tool that is relied on, additional contractual measures may also be helpful to allow EU-based data exporters to become aware of new developments affecting the protection of the data transferred to third countries.[77] The contract may need to provide that for transfers to take place, specific technical measures would have to be implemented.[78] It may also underscore the obligation of the importer to assist the exporter to provide sufficiently detailed information on all requests of access to personal data by public authorities.[79] The exporter could also add clauses whereby the importer certifies that it has not purposefully created back doors, and national law or government policy does not require the importer to create or maintain back doors.[80] In the event the legislations of third countries prohibit the importer to notify controller of the disclosure and access request by a law enforcement authority, such as a prohibition under criminal law the aim of which is to preserve the confidentiality of a law enforcement investigation, the importer is required to inform the exporter of inability to comply with the transparency obligations under contractual clauses.[81]

Despite all the endeavors above, even the EDPB itself recognized the supplementary measures are not necessarily effective in all third countries or in all circumstances, the data exporters shall be responsible for assessing their effectiveness in the context of the transfer. And it is still possible that no supplementary measure can ensure an essentially equivalent level of protection for specific transfer, in that case, the transfer must be avoided, suspended, or terminated. For example, contractual and organizational measures alone will generally not overcome access to personal data by public authorities of the third country based on problematic legislation, where only appropriately

[75] Article 4(5) of GDPR.
[76] EDPB, supra 74, para 85.
[77] Ibid para 100.
[78] Ibid para 103.
[79] Ibid para 106.
[80] Ibid para 109.
[81] Schrems II, para 139.

implemented technical measures, like pseudonymized or encrypted data, might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes. If the law of the third country prohibits the supplementary measures (e.g., prohibits the use of encryption) or otherwise prevents their effectiveness, the exporter must not start transferring personal data to this country, or must stop ongoing existing transfers to this country.[82] As one example of encryption prohibition, in November 2011, the China State Encryption Management Bureau issued public statements, indicating concern over the import/use of TPM integration and use in China. The Trusted Platform Module (TPM) is a specialized chip installed on commercial PCs that is used for the purpose of the hardware authentication or PC applications that require a level of trust. TPM contains hardware based cryptography used for authentication and key management systems. PC companies had to shut down TPM function in order to comply with local laws.[83] Pseudonymisation also has limited effect due to that physical, physiological, genetic, mental, economic, cultural, or social identity of a natural person, their physical location or interaction with an internet based service at specific points in time may allow the identification of that person even if their name, address, or other plain identifiers are omitted. Certain cloud service provider also requires the personal data cannot be pseudonymized or encrypted because the processing requires accessing data in the clear in order to execute the task assigned.[84]

Binding Corporate Rules (BCRs) are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. Such rules must include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. They must be legally binding and enforced by every member concerned of the group. Companies must submit binding corporate rules for approval to the competent data protection authority in the EU. The authority will approve the BCRs in accordance with the consistency mechanism set out in Article 63 GDPR.[85] BCRs are considered the "gold standard" for international data transfers, as they provide the only tailor made data transfer regulatory approval. As all concerned supervisory authorities have participated in the review and approval process, it seems unlikely that a supervisory authority would initiate an enforcement action against a data transfer that takes place on this basis.[86] Many companies criticized BCRs as exceedingly complex, costly, and risky because the EU data protection authority in every EU member state where

[82] Schrems II, para 50-58.
[83] TPM policy, HP Commercial PCs Customer Support, https://support.hp.com/us-en/document/ish_5031710-5031755-16 accessed 27 April 2022.
[84] EDPB, Supra 74, para 94.
[85] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en accessed 28 April 2022.
[86] Lukas Feiler, Wouter Seinen, BCRs as a robust alternative to Privacy Shield and SCCs, IAPP, July 2020.

the entity is located needs to approve them.[87] Although BCRs were not covered in Schrems cases, they are one of the "appropriate safeguards" under Article 46 as SCCs and cannot be used against U.S. government surveillance. The good news is the data transfer approval was made by supervisory authorities and based on case by case evaluation, which is the difference from the SCCs. Whether the supplementary safeguards are needed as SCCs is still pending for CJEU's further clarification.

3.4 "One More Try"

At the end of the Schrems II Judgment, the CJEU notes that "in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR". Although Schrems II did not affect specific derogations identified in the GDPR that allow for the transfer of personal data outside of the EU, the CJEU repeatedly underlined that "the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary"[88] Article 49 offers two main paths for what it calls "derogations" that permit transfer despite a lack of an adequate data protection law: consent or necessity.[89]

The EDPB issued the Guidelines on derogations of Article 49 and Guidelines on consent under GDPR, which says "According to Article 4 (11) of the GDPR, any consent should be freely given, specific, informed and unambiguous…Article 49 (1) (a) is stricter as it requires 'explicit' consent.[90] Explicit consent requires 'an express statement of consent', such as a written statement and 'consent for data transfers that occur periodically or on an on-going basis is inappropriate.[91] "The data exporter must make sure to obtain specific consent before the transfer is put in place…this provision requires data subjects to be also informed of the specific risks resulting from the fact that their data will be transferred to a country that does not provide adequate protection and that no adequate safeguards aimed at providing protection for the data are being implemented…The provision of this information is essential in order to enable the data subject to consent with full knowledge of these specific facts of the transfer and therefore if it is not supplied, the derogation will not apply…the GDPR sets a high

[87] Archick, Supra 1, p. 16.
[88] Schrems I, para 92.
[89] Anupam Chander, Is Data Localization a Solution for Schrems II? Georgetown University Law Center, Journal of International Economic Law, Sep 2020, p. 5.
[90] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, May 2018, p. 6-8.
[91] EDPB Guidelines 05/2020 on Consent under Regulation 2016/679, May 2020, para 91-93.

threshold for the use the derogation of consent. This high threshold, combined with the fact that the consent provided by a data subject can be withdrawn at any time, means that consent might prove not to be a feasible long term solution for transfers to third countries". Necessity is also narrowly construed as "data transfers on the grounds of derogation Article 49 (1) (b) may take place 'where the transfer is occasional and necessary in relation to a contract'…The 'necessity test' limits the number of cases in which recourse can be made to Article 49 (1) (b). It requires a close and substantial connection between the data transfer and the purposes of the contract…Personal data may only be transferred under this derogation when this transfer is occasional. It would have to be established on a case by case basis whether data transfers would be determined as 'occasional' or 'non-occasional'".[92]

3.5 "Where do we go from here"

The economic importance of transatlantic data flow has led to some calls for a third attempt to develop a new mechanism specifically for EU–US data transfers.[93] The US Department of Commerce and the European Commission released a statement committing to intensifying negotiations on an enhanced EU–US Privacy Shield framework to comply with the Schrems II ruling.[94] One argument in favor of returning to the negotiation table is that the CJEU judgment in Schrems II appeared to leave scope for the formulation of a data transfer agreement that could withstand CJEU scrutiny. As opposed to Schrems I—which included harsh criticism of generalized surveillance measures as compromising 'the essence' of Article 7 of the Charter—the CJEU in Schrems II focused on the absence of adequate safeguards.[95] Others doubt whether this remains a fruitful path forward as the CJEU invalidation of EU–US data transfer agreement for the second time in just five years demonstrated that the unwillingness of the CJEU to compromise on the matter of fundamental rights for economic expedience.[96] On the U.S. side, legislative action may be necessary to limit U.S. national security agency access to EU citizens' personal data and/or make it easier for EU citizens to challenge alleged infringements in U.S. courts.[97] Many experts, however, regard U.S. statutory changes to surveillance authorities or providing greater access to U.S. courts for EU citizens via legislation as unlikely in the

[92] EDPB, Supra 90, p. 8-9.
[93] J Meltzer, "The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security", Brookings, 5 August 2020.
[94] Intensifying Negotiations on Transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and US Secretary of Commerce Gina Raimondo, European Commission, 25 March 2021.
[95] T Christakis, "After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe" European Law Blog, 21 July 2020.
[96] Murphy, Supra 12, p. 247.
[97] Archick, Supra 1, p. 17.

short term given the political challenges and complexities involved.[98] U.S. officials express the hope for a "quick resolution" in the negotiations on an enhanced Privacy Shield, but assert that the United States also wants to ensure that a successor accord is "legally defensible because we certainly don't wish this to fall to another legal challenge" at the CJEU.[99]

A broad digital trade agreement covering cross-border data flows as U.S.-Japan Digital Trade Agreement could be an option. Several international organizations, including the Organization for Economic Co-operation and Development (OECD), the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and World Trade Organization (WTO) also aim to establish a regional and global framework to enable digital trade in a nondiscriminatory and less trade restrictive manner regarding personal data protection and cross-border data flows, which could be another try to resolve the challenges of cross-border data flows.

[98] Kenneth Propp, "Progress on Transatlantic Data Transfers? The Picture After the US-EU Summit," Lawfare, 25 June 2021.
[99] Doug Palmer, "U.S. Wants 'Legally Defensible' Privacy Shield Pact, Commerce Negotiator Says," Politico Pro, July 20, 2021.

4 Summary and Conclusion

Prior to Schrems cases, Chapter V of GDPR provided “equivalent adequate” protection, “appropriate safeguards” and “derogation” as different layers and options to make cross-border data flows in different circumstances. However, after Schrems II, it is argued that the CJEU collapsed all of Chapter V into a narrowly constructed legal adequacy determination, rather than treat them as a series of different options, which even brought uncertainty to the adequacy decisions made before Schrems since they could be invalidated on the same grounds as the EU-US Safe Harbor and Privacy Shield adequacy.

Meanwhile, the involvement of surveillance by governments under national security exception even raised the difficult level to resolve the problem. As the CJEU interpreted the “equivalent adequate” in the context of the Charter of Fundamental Rights of EU, the problem of U.S. government access to EU citizens’ data has been the key barrier to data flows. Neither satisfied the rule of proportionality nor provided the effective judicial redress against the government interference of data, U.S. did not provide “equivalent adequate” protection in the eyes of the CJEU leading to the invalidation of Safe Harbor and Privacy Shield in Schrems cases. It may not be practical to expect U.S. to modify their surveillance rules enduring CJEU scrutiny. Unless both parties may find an innovative breakthrough, the potential Schrems III may be inevitable.

Although the CJEU added at the final part of the Schrems II that in the absence of “equivalent adequate” protection and “appropriate safeguards”, “derogations” could be relied on to avoid legal vacuum, the CJEU itself also underlined in Schrems I that the protection of the fundamental right at EU level requires that derogations should apply only in so far as is strictly necessary. How could the “derogations” endure the same scrutiny under the Charter when the adequacy test already failed? Does that mean the “derogations” could cure the defects of inadequacy or being exceptions? Then why cannot the SCCs?

In the absence of further clarification by CJEU as to what are the supplementary measures, EU commission and EDPB had to make patchworks by new SCCs and guidelines to try to fix the problem and provide more legal certainty. The purpose of EU-U.S. data transfer frameworks, both Safe Harbor and Privacy Shield, was to provide an efficient and reliable tool for business operations in practice and reduce the cost and burden. Now it is becoming an unbearable burden, legally and economically, especially for small and middle size enterprises to make case by case evaluation of “equivalent adequate” protection of third country.

Moreover, without the protection by ex-ante authority approval by SCCs or BCRs, the business organizations have to take the risks of suspension or calling off the cross-border data flows, even the 4% annual global turnover penalty in the breach of GDPR, the huge legal uncertainty as the Sword of Damocles intimidates certain amount of business organizations to consider other solutions including data localization, which is obviously the last choice and would, even worse, open the Pandora's Box as new type of trade barrier with the disguise of data protection.

In summary, the CJEU decisions in Schrems cases left more questions to be answered further. The enhanced EU-U.S. transatlantic data flows framework and multilateral agreements by international organizations are in negotiation, the waiting time for clarification would not be long.

Bibliography

Official Publications

- Article 29 Working Party, (2015) “Statement of the Article 29 Working Party”.
- Commission Decision 2000/520/EC (2000), pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce.
- Commission Implementing Decision (EU) 2016/1250 (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.
- Congressional Research Service, (2017) “Digital Trade and U.S. Trade Policy”.
- Dept. of Comm., (2020) Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II.
- European Centre for International Political Economy and Kearney Global Business Policy Council, (2021) “The Economic Costs of Restricting the Cross-border Flow of Data”.
- European Commission Memo/17/15, (2017) “Digital Single Market – Communication on exchanging and protecting personal data in a globalized world”.
- European Commission, (2015) “A Digital Single Market Strategy for Europe”.
- European Data Protection Board, (2019) EU-U.S. Privacy Shield - Third Annual Joint Review.
- Frontier Economics, (2021) “The Value of Cross-Border Data Flows to Europe: Risks and Opportunities”.
- House Of Representatives, (2001) The EU Data Protection Directive: Implications For The US Privacy Debate: Hearing before the Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce, Serial No 107-19.
- European Commission, (2021) Intensifying Negotiations on Transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and US Secretary of Commerce Gina Raimondo.
- U.S. Bureau of Economic Analysis, Table 3.3. U.S. Trade in ICT and Potentially ICT-Enabled Services, by Country or Affiliation.

Literature

- Kristin A., Rachel F., U.S.-EU Privacy Shield and Transatlantic Data Flows, Congressional Research Service, 22 September 2021.
- Anu B., The Brussels Effect, in North-Western University Law Review, 2012.
- Laura B., Mateo A., and Kathleen L., Standard Contractual Clauses for Cross-Border Transfers of Health Data After Schrems II, Journal of Law and the Bioscience 1, 2021 8(1).
- Lee B., "Transatlantic Tensions on Data Privacy" Transworld Working Paper, 2013.
- Anupam C., Is Data Localization a Solution for Schrems II? Georgetown University Law Center, Journal of International Economic Law, Sep 2020.
- Theodore C., "After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe" European Law Blog, 21 July 2020.
- Marcelo C., Mark F., Mateo A. and Timo M., Supplementary Measures and Appropriate Safeguards for International Transfers of Personal Data after Schrems II.
- Lesley F., "FTC Settlement Focuses on those Other Privacy Shield Framework Requirements," Federal Trade Commission, 30 June 2020.
- Henry F. and Abraham N., "Of Privacy and Power: The Transatlantic Struggle over Freedom and Security" Princeton University Press, 2019.
- Lukas F., Wouter S., BCRs as a robust alternative to Privacy Shield and SCCs, IAPP, July 2020.
- Marsha H., Stephen L., and Stephen H., "The Right to Privacy in Personal Data: The EU Prods the US and Controversy Continues" 9 Tulsa Journal of Comparative and International Law, 2002.
- Joseph L., David P., Mark B., Barbara E. B., Demystifying Schrems II for the cross-border transfer of clinical research data, Journal of Law and the Biosciences.
- Natasha L., "Europe and U.S. Seal Privacy Shield Data Transfer Deal to Replace Safe Harbor," Techcrunch.com, 2 February 2016.
- Vincent M., "EU Zooms ahead, despite worries over app" Politico, 2020.
- Joshua M., "The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security", Brookings, 5 August 2020.
- Maria M., Assessing the Implications of Schrems II for EU–US Data Flow, International and Comparative Law Quarterly, Cambridge University Press, 2021.
- Doug P., "U.S. Wants 'Legally Defensible' Privacy Shield Pact, Commerce Negotiator Says," Politico Pro, 20 July 2021.
- Oliver P. and Dr. Nathan L., EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows, UCL European Institute, May 2020.

- Kenneth P., “Progress on Transatlantic Data Transfers? The Picture After the US-EU Summit,” Lawfare, 25 June 2021.
- Paul S. and Karl P., “Transatlantic Data Privacy” The Georgetown Law Journal, 2017.
- Paul S., “Global Data Privacy: The EU Way”, NYU Law Review, 2019.
- Mark S., “Privacy Shield Is Stuck” Politico Digital Bridge, 15 July 2021.
- Tim W., Jack G., Who Controls the Internet?: Illusions of a Borderless World, Oxford: Oxford University Press, 2006.

Online sources

- https://www.retail-index.com/E-commerceretail.aspx accessed 17 April 2022
- https://www.privacyshield.gov/list accessed 18 April 2022
- https://www.retail-index.com/E-commerceretail.aspx accessed 17 April 2022
- https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield accessed 20 April 2022
- https://www.state.gov/privacy-shield-ombudsperson accessed 20 April 2022
- https://www.pclob.gov accessed 20 April 2022
- https://noyb.eu/en/project/eu-us-transfer accessed 21 April 2022
- https://support.hp.com/us-en/document/ish_5031710-5031755-16 accessed 27 April 2022
- https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en accessed 28 April 2022
- https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en accessed 27 May 2022