Santa Clara Journal of International Law

Volume 19 | Issue 2 Article 1

5-1-2021

Cross-Border Data Transfers Between the EU and the U.S.: A Transatlantic Dispute

Jiménez-Gómez, Briseida Sofía

Cross-Border Data Transfers Between the EU and the U.S.: A Transatlantic Dispute

By: Briseida Sofía Jiménez-Gómez*

This article deals with the clash between the European and American approach to transborder data flows. In the last decades, the discourse has been that the U.S. offers a market-dominated approach while the EU was embedded in a right-dominated policy. General Data Protection Regulation (GDPR) restricts data transfers outside the EU. An analysis of the meaning of the level of adequate protection of a non-EU country is necessary to transfer data beyond the EU. The Court of Justice of the European Union has invalidated the Privacy Shield agreement to transfer commercial data from the European Union to the United States, leaving transatlantic data transfers in a current predicament. Safe Harbour Principles previously and Privacy Shield recently have been read according to EU data protection law, in particular the General Data Protection Regulation in combination with the European Charter of Fundamental Rights. The landmark Schrems II judgement is assessed to point out current available options to transfer data from the European Union to the United States and also several implications on cross-border data flows beyond the EU-U.S. relationship.

Keywords: data protection – privacy – international commerce – surveillance – fundamental rights – international data transfers

* RCC Postdoctoral Fellow at the Harvard Law School Institute for Global Law and Policy. PhD in Law Complutense University (Madrid). LL.M. College of Europe (Brugge).

TABLE OF CONTENTS

I. A CONFLICT OF CULTURES: A CONFLICT OF VALUES

A. Dependence on Personal Data

All industries depend on data flows, from traditional industries to cutting edge technologies. Economic growth is determined by industries development and business growth, for which free data flow is a fundamental support.[1] The European Union was aware that the digital economy within the EU itself relies on data transfers.

The transatlantic economic relationship between the EU and the United States is the largest in the world, valued at $7.1 trillion.[2] The Data Protection Directive (Directive 45/95, today repealed)[3] was viewed as "[t]he most significant potential barrier to transatlantic data flows."[4] Compatibility between divergent frameworks does not sound an easy task. Too much protection can overly restrict business activities and trade, but too little protection can create negative market effects affecting consumer trust.

The process of harmonization inside the EU was based on free flow of personal data to foster growth, but at the same time the level of protection of personal data increased with the adoption of Directive 45/95, as many Member States did not previously have a data protection regime. Within the framework of the aim of creating a market Union, data flows could not be an impediment within the EU. EU legal regimes have crossed European borders when third states decided to regulate data protection considering the EU legal regime as a model.[5] Recital 10 of the General Data Protection Regulation (GDPR) specifically refers to ensure a high level of protection of natural

---

[1] *See* Daniel Castro & Alan Mcquinn, *Cross-Border Data Flows Enable Growth in All Industries*, INFO. TECH. & INNOVATION FOUND. (Feb. 2015), http://www2.itif.org/2015-cross-border-data-flows.pdf.

[2] *See* Press Release, Department of Commerce, U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows (July 16, 2020), https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.

[3] 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, O.J. (L 281) [hereinafter Data Protection Directive].

[4] *See* Joshua P. Meltzer, *Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows*, BROOKINGS INST. (Nov. 3, 2015), https://www.brookings.edu/testimonies/examining-the-eu-safe-harbor-decision-and-impacts-for-transatlantic-data-flows/.

[5] *See* Graham Greenleaf, *'European' Data Privacy Standards Implemented in Laws Outside Europe,* 149 PRIVACY LAWS & BUS. INT'L REP. 1 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3096314 (14 of 20 GDPR countries selected outside Europe have restrictions on data exports based at least in part on the laws of the recipient country).

persons plus to remove obstacles of data flows throughout the EU.[6] Therefore, the GDPR establishes free flow of personal data in the geographical space of the EU (and EEA).[7] Some scholars even go further suggesting that data flows should be the fifth freedom of the internal market.[8] The GDPR model is within the framework of a particular international organization with aims of political union.

However, the external dimension of data flows is uneven. The EU regime proposes restrictions of data flows to third States to ensure that the level of protection of natural persons is not undermined.[9] Article 44 of the Regulation prohibits the transfer of personal data to countries outside EU borders, unless the recipient country can provide evidence of an adequate level of data protection equivalent to the EU.

By contrast, U.S. law does not require a national regulator to approve a data transfer agreement.[10] This has practical implications, considering the market power of U.S. companies in online services. For example, tech giants, like Google and Facebook admitted access to personal information.[11] The United States is one of the non-European countries in the G20 that does not have data privacy laws meeting this minimum international standard referring to the OECD standards.[12] As Professor Lessig highlighted, "[t]he problem

---

[6] 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 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[7] *See* General Data Protection Regulation art. 1(3) [hereinafter GDPR]. The principle of free movement of data within the Union for non-personal is established in Regulation (EU) 2018/1807, subject to restrictions on public security reasons. *See* Regulation (EU) 2018/1807, of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union, 2018 O.J. (L 303) 59; *see also* PEDRO A. DE MIGUEL ASENSIO, CONFLICTS OF LAWS AND THE INTERNET 128 (2020).

[8] *See* OLIVIER LINDEN & ERIK DAHLBERG, KOMMERSKOLLEGIUM NAT'L BD. OF TRADE SWEDEN, DATA FLOWS – A FIFTH FREEDOM FOR THE INTERNAL MARKET?, 25-29 (2016), https://www.kommerskollegium.se/globalassets/publikationer/ rapporter/2016/publ-data-flows.pdf.

[9] *See* GDPR, *supra* note 7, arts. 44-50.

[10] There are no specifications in the Gramm-Leach-Bliley Act. The California Security Breach Notifications Law and the California Online Privacy Protection Act does not address the use of data transfer agreement. Although a regulator may have audit powers to ensure compliance with the Health Insurance Portability and Accountability Act, there is no need to approve a data transfer agreement.

[11] Samuel Gibbs, *Gmail Does Scan All Emails, New Google Terms Clarify*, THE GUARDIAN (Apr. 15, 2014), https://www.theguardian.com/technology/2014/apr/15/gm ail-scans-all-emails-new-google-terms-clarify.

[12] Greenleaf, *supra* note 5, at 2. (China, Brasil and Saudi Arabia are part of the G-20 that do not have privacy laws meeting OECD standards. Only 4 countries of the 13 non-European countries in the G20 are in this category).

with privacy is that private data flows too easily–that it too easily falls out of the control of the individual."[13] According to the property perspective, privacy tools will be more developed if users would pay for protecting privacy. In a comparison with copyright, copyright holders (such as Hollywood industry in the U.S.) pay to get protection.[14] Privacy may not be as well as protected as copyright because the American society does not "invoke the rhetoric of property to defend incursions into privacy."[15]

Protecting data privacy means not only limiting access to personal information, so that citizens maintain the right to information they want to display about themselves, data protection cares about that data flows appropriately.[16] How is the level of appropriateness regulated? This article deals with the clash between the European and American approach to transborder data flows. In the last decades, the discourse has been that the U.S. offers a market-dominated approach while the EU was embedded in a right-dominated policy.[17] Both systems are converging, maybe at a slow pace, and mutual regulatory influences are acknowledged at least at a substantive level. The California Consumer Privacy Act (CCPA)[18] was influenced by the GDPR, but the GDPR has also been inspired by the California law on data notification breaches (see arts. 32-34 GDPR).[19] The EU Commission encouraged the National Telecommunication and Information Administration of the U.S. Department of Commerce to consider reporting data breaches for harmonization at a federal level, instead only at state level.[20] This was also recognized in the "Data Protection and Privacy Agreement" or "DPPA" for law enforcement purposes in criminal matters (Article 10).[21]

In the last years we have observed an increase in people's concern related to global phenomena, such as Snowden revelations (2013) or

---

[13] Lawrence Lessig, *Privacy as Property*, 69 SOCIAL RESEARCH 247, 250 (2002).
[14] *Id.* at 252.
[15] *Id.* at 255.
[16] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE, 2-3 (Stanford Univ. Press 2010), https://crypto.stanford.edu/portia/papers/privacy_in_context.pdf.
[17] Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1318 (1999-2000).
[18] California Consumer Privacy Act of 2018, Assembly Bill No. 375 (2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.
[19] *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771 (2019); Lee A. Bygrave, *Transatlantic Tensions on Data Privacy*, TRANSWORLD 9 (2013).
[20] *See* Letter from Bruno Gencarelli to Secretary Redl, (Nov. 9, 2018) (Request for public comments on a proposed approach to consumer privacy [Docket No. 180821780-8780-01]).
[21] *See* 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 O.J. (L. 336) (in the EU referred to as "Umbrella Agreement").

Cambridge Analytica scandal (2018).[22] The US CONSENT Act,[23] the Privacy Bill of Rights Act,[24] and the New Consumer Online Privacy Rights Act (COPRA)[25] were enacted after the Cambridge Analytica scandal. Recently, the US Public Health Emergency Privacy Act has come into force after the pandemic of COVID-19.[26] The criticism of stuck U.S. privacy law does not seem to be any more the case. Eleven privacy bills were introduced in the U.S. Congress and several states are enacting broad legislation.[27]

Transfer of personal data abroad is not only a technical problem, it is rather a legal issue and like every legal issue implicates economic and societal values. Therefore, a technical solution does not make disappear the problem of understanding between two different legal viewpoints. Code may solve the problem of identifiability, but the issue of citizen redress and the ability to public enforcement when use of data is not in compliance with the law may only be solved by a legal solution. Diplomats usually work in reaching agreements with foreign countries and cultures. A political solution may be a good step to reach a common understanding, however, without a legal framework where individuals can base their data privacy claims, without the option of clear (public and private) enforcement, consumers and citizens or netizens completely lose their rights they had in the off-line world.

Part I explores the different perspectives surrounding data privacy between the United States and the European Union. The ideology on data protection (EU terminology) and privacy (U.S. terminology) expands with regard to international data flows. The extensive jurisdiction of the GDPR is considered under the effects doctrine. This part also briefly examines the liberal governance model created under the Organisation for Economic Cooperation and Development Guidelines. The OECD model reflects a mixed approach regarding international data flows. Meanwhile it adopts a free flow data approach in line with the self-regulation and voluntary U.S. model, it also permits restrictions of international data flows when the recipient country does not provide equivalent protection.

---

[22] *See* Julie Carrie Wong, *The Cambridge Analytica Scandal Changed the World- But it Didn't Change Facebook,* THE GUARDIAN (Mar. 18, 2019), https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook ("It took five full days for the founder and CEO of Facebook – the man with total control over the world's largest communications platform – to emerge from his Menlo Park cloisters and address the public. When he finally did, he did so with gusto, taking a new set of talking points").

[23] CONSENT Act, S. 2639, 115th Cong. § 2 (2018).

[24] Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019).

[25] Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019).

[26] Public Health Emergency Privacy Act, S. 3749, 116th Cong. (2020).

[27] See Anupan Chander, Margot E. Kaminski, & William McGeveran, *Catalyzing Privacy Law*, MINN. L. REV. (Apr. 16, 2021), https://minnesotalawreview.org/article/catalyzing-privacy-law/.

Part II turns to the options that the General Data Protection Regulation allows to transfer data to a non-EU country. Chapter V of the GDPR together with the first case on *Schrems v. Facebook* is analyzed. It broadens the lens to the first jurisprudence from the Court of Justice of the European Union, considering the particular challenges of adequacy decisions issued by the European Commission. Moreover, it assesses the importance of international commitments by the example of the Council of Europe Modernized Convention 108, to which non-European countries have committed. A consideration of the meaning between the EU equivalent level of protection and an appropriate level of protection is necessary to think about the situation of the United States in the aftermath of the *Schrems II* decision by the Court of Justice of the European Union on July 16, 2020. This part remembers the Commission warnings on the Safe Harbour Principles, predecessor mechanism of the Privacy Shield to transfer data from the European Union to the United States. An in-depth analysis of the Court of Justice of the European Union in *Schrems I* on 6 October 2015 reveals that the causes for Safe Harbour Principles invalidation were not commercial, but related to surveillance matters, which was not assessed by the European Commission during the negotiations of the first agreement. The study of provisions of the European Charter of Fundamental Rights in previous cases is key to understanding the development of the Court of Justice of the European Union reasoning. Furthermore, the common contractual alternative of standard contractual clauses is explained, considering the clarifications of the most recent case *Schrems II*.

Part III examines the issues of the invalidation of the Privacy Shield in detail. It contrasts different previous opinions on the compatibility between the U.S. and EU law. It explains the absence of compatibility between the United States and the European Union law, considering the specific U.S. laws which are problematic from a fundamental rights approach, with special attention to surveillance programmes and their underlying legal basis. The proportionality principle is expanded to consider non-legal reasons such as the intelligence collaboration between the United States and the Member States of the European Union. Specific risks regarding cross border transfers to the U.S. arise for non-U.S. citizens, in particular the absence of means of effective redress, despite the improvements of U.S. laws like the FREEDOM Act and the Judicial Redress Act. Moreover, it also analyzes the significance of independence of the Privacy Shield Ombudsperson in relation to the European legal context and previous case. This part includes an explanation of the current available options to transfer data from the European Union to the United States and pointing out further consequences for international agreements beyond the EU-U.S. relationship.

The article concludes with some remarks on why an international framework is more necessary than ever, considering the surveillance society in which we are immersed in most parts of the world.

B. The United States Model

The U.S. perspective considers regulation of data flows inappropriate. The last decade of the twentieth century saw the bursting of e-commerce. Regulation could hamper the economic prospects of corporations which were benefiting from the common use of the internet by consumers. The decision of the U.S. administration seems to balance a set of priorities and tilt to a flexible and tailored self-regulation. Self-regulation seems a better option than a comprehensive regulation by the legislature.[28] It exists an intrinsic belief that companies will provide meaningful and consumer-friendly regimes on its own.[29] The U.S. government publicly supports the private sector initiative on incorporating privacy safeguards.[30] Regulation of privacy is viewed as risky, costly and burdensome. The "religion of self-regulation" was also criticized by American scholars.[31]

However, the concept of companies towards privacy has changed substantially.[32] Google CEO Sundar Pinchai has stated that Google believes privacy is a human right at a remote hearing before the U.S. Congress on July 30, 2020.[33] The CCPA in California obliges companies to establish new rights for residents in California. In practical terms, differences between California law and the rest of the United States are reflected in the privacy policies of companies operating throughout the United States. An example of the current legislative fragmentation for a U.S. citizen is the company's warning that even if someone uninstalls the app from your device, it will still have the unique

[28] *See* Henry Farrell, *Negotiating Privacy Across Arenas: The EU-U.S. "Safe Harbor" Discussions*, *in* COMMON GOODS: REINVENTING EUROPEAN AND INTERNATIONAL GOVERNANCE 101, 105–26 (Adrienne Héritier ed., 2002).
[29] THE WHITE HOUSE, *A Framework for Global Electronic Commerce*, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html (last updated 1997).
[30] *Id*.
[31] *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999); Joel R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 113–14 (1995).
[32] *Compare* 1997 Vice President of American Express, "We believe that government regulation of privacy on the Internet and other online areas is very risky given the rapid changes in this new technology." Peggy H. Haney, *Case Study of American Express' Privacy Principles: Why and How They Were Adopted, the Choices Involved and a Cost-Benefit Analysis*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE 209, 213 (U.S. Dep't of Commerce ed., 1997), https://www.ntia.doc.gov/page/chapter-6-corporate-experiences-privacy-self-regulation.
[33] Tony Romm, *Amazon, Apple, Facebook and Google Grilled on Capitol Hill over Their Market Power*, THE WASHINGTON POST (July 29, 2020), https://www.washingtonpost.com/technology/2020/07/29/apple-google-facebook-amazon-congress-hearing/.

associated identifier for the device. However, if U.S. are California residents, they enjoy some rights, like the right of deletion under the CCPA.

Some privacy policy clauses only warn the user that by using our websites and mobile applications, you consent to the transfer to, the processing and storage of your information in, countries outside of your country of residence, which may have different data protection laws than those in the country in which you reside.[34] The residence of the user does not seem the only factor to take into account. Therefore, data gathered by these websites do not offer the option to consent or opt-out, basically they are unilateral provisions not able to negotiate by users or consumers with the handicap that it is not clear at all which law is applicable to the personal data of the user. It may be absent in the privacy policy the destination of personal data and any further guidance to the user.

Consequently, self-regulation does not seem an effective way for transborder data flows. If the policy option is free personal data flows, users are lost to vindicate their rights because it appears that there is no right to defend. The last approach contrasts with the protective approach of citizens endorsed by EU law.

In the past, data protection standards were not in a prominent position in international negotiation. For example, when discussing free trade agreements or privacy was not seen a very serious matter compared to other human rights. However, technology has made the focus on data protection more significant. The EU-led agreements related to international trade usually contemplates as a mandatory requirement that international data flows between both areas are subject to privacy standards forward by the GDPR.[35] By contrast, the U.S. furthers its policy of limitless flow of data across borders through trade agreements where only a public policy reason can be a limit to transborder data flows.[36]

C. The Effects Doctrine: The European Union Model

The connecting factors for the application of the GDPR are offering goods or services to data subjects in the EU or monitoring their behavior in

[34] *See e.g.*, Target privacy policy before July 1, 2020 said: "We are based in the United States. When we obtain information about you, we may transfer, process, and store such information in the United States and other countries. By using our websites and mobile applications, you consent to the transfer to, and to the processing and storage of your information in, countries outside of your country of residence, which may have different data protection laws than those in the country in which you reside." The last up-to-date has deleted this information (last visited Aug. 16, 2020), https://www.target.com/c/target-privacy-policy/-/N-4sr7p?Nao=0#ContactTarget.

[35] *See* Adil Nussipov, *How America and Europe Deal with Data*, CMDS (Jan. 7, 2020), https://cmds.ceu.edu/article/2020-01-07/how-america-and-europe-deal-data.

[36] *Id.*

the EU, irrespective of location of processing personal data.[37] The targeting of residents in the EU has been considered an example of the effects doctrine that permits a State to assert jurisdiction where a regulated conduct produces significant effects on a territory.[38] Data protection is a protective law similar to consumer protection laws whose objective is preventing negative effects of conduct targeted to citizens or residents in the European Union. The effects doctrine could be considered similar to the objective territoriality principle.[39]

However, personal data located in the territory of the EU seems to dictate control, in particular because the GDPR restricts transfer of data outside the EU without finding appropriate safeguards.[40] The GDPR broadens its territorial scope beyond the EU under the idea that protecting privacy is a fundamental right that must continue, disregarding where personal data are processed. In fact, the legal protection follows the data which has been included under the personality principle.[41] One of the goals of regulating cross-border data flows is furthering social and economic values,[42] despite this, the EU Charter of Fundamental Rights does not mention regulation of cross-border data flows while refers to the "essence" of fundamental rights and freedoms.

The CJEU has confirmed that the high level of protection of natural persons guaranteed by the GDPR is not undermined abroad,[43] in particular, protection of personal data concerning natural persons that are citizens or residents in the EU.

If social and economic values in the U.S. and the EU are different (liberal approach and social protection), we should ask ourselves how

---

[37] Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 127), Article 3(2).

[38] The effect test comes from competition law, *see* Julia Hörnle, *Juggling More than Three Balls at Once: Multilevel Jurisdictional Challenges in EU Data Protection Regulatio*n, 27 INT'L J. L. & INFO. TECH. 142, 164 (2019).

[39] *Id.* at 165.

[40] *See* Jennifer Daskal, *Transnational Government Hacking*, 10 J. L. NAT'L SEC. L. & POLICY 677, 682 (2020) ("In restricting the transfers of data outside the EU absent a finding of adequate data protection safeguards, the EU, for example, presumes that location of data (whether in or out of the EU) dictates control.").

[41] *See* CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 123 (2013).

[42] *Id.* at 160.

[43] *See* Case C-362/14 *Maximilien Schrems v. Data Protection Commissioner* [2015] EU:C:2015:650 [hereinafter *Schrems I*]; Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Ltd, Maximilien Schrems* [2020] EU:C:2020:559 [hereinafter *Schrems II*]. *See also* CJEU, Opinion 1/15, Draft Agreement Between Canada and the European Union, (July 26, 2017) EU:C:2017:592 (invalidating the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data).

different they are and if it would be possible to further them without conflict. We should recognize that culture influences on both sides of the Atlantic, and admit legal pluralism as a viable solution, having taken into account there is not an international aspiration of becoming a political union. We need to consider the basis of philosophical values in common such as democracy, the rule of law, liberty, justice and solidarity in order to propose a more realistic and effective approach to data flows.

D. The Liberal Governance Model

The liberal governance model has its representation at international level with the Organisation for Economic Co-operation and Development Guidelines (OECD Guidelines).[44] The OECD Guidelines governing the protection of privacy and transborder flows of personal data are voluntary and focus on "consumers" and "users" instead of "citizens."[45] OECD recommends to remove or avoid creating unjustified obstacles to transborder flows of personal data.[46] However, the OECD Guidelines explicitly allows to restrain data flows where the State does not observe the OECD Guidelines or where "the re-export of such data would circumvent its domestic privacy regulations."[47] Moreover, restrictions are allowed with respect to certain categories of personal data if specific regulations exist in a Member country and the recipient country does not provide equivalent protection.[48] It is true that the OECD guidelines support self-regulation,[49] but also encourage countries to provide for "reasonable means" for individuals to exercise their rights.[50] Likewise, Member States should endeavor to develop principles to govern the applicable law in the case of transborder flows of personal data.[51] These principles could have a domestic or international approach.

Therefore, the OECD model could be considered a mixed model under sources of inspirations from both transatlantic approaches. A question that arises is the following: What is the advantage of having the basic principles recognized at international level if later, nationally, sectoral regulation or another type of self-regulation ignores key elements of the principles? Thus, it seems *a priori* that the U.S. data protection system does not comply with

[44] Organization for Economic Co-operation and Development: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Sept. 23, 1980, OECD Doc. C (80) 58 *reprinted in* 20 I.L.M. 422 (1981) [hereinafter OECD, *Guidelines*].
[45] Reidenberg, *supra* note 17, at 1353.
[46] OECD, *Guidelines*, *supra* note 44, at Preface.
[47] *See* OECD, *Guidelines, supra* note 44, §17.
[48] *See* OECD, *Guidelines*, *supra* note 44, §17.
[49] *See* OECD, *Guidelines, supra* note 44, §19(b).
[50] *See* OECD *Guidelines*, *supra* note 44, §19(c).
[51] *See* OECD Guidelines, *supra* note 44, §22.

international principles.[52] Consequently, a systemic legal conflict between EU law and U.S. law would exist.

II. GDPR OPTIONS

The GDPR provides a set of options to legalize cross-border data transfer in Chapter V (articles 44-50). The most advantageous is obtaining an adequacy decision from the European Commission (art. 45 GDPR). In the absence of an adequacy decision, appropriate safeguards are needed for transfers beyond the EU (art. 46 GDPR). The first section will analyze the problems regarding an adequacy decision of the United States. The second section will assess the option of appropriate safeguards, in particular the use of standard contractual clauses.

A. Obtaining an Adequacy Decision

Obtaining an adequacy decision by a third country has the benefit that no further requirements exist to transfer personal data from the EU. The official webpage of the EU Commission assimilates the U.S. limited to the Privacy Shield framework to other countries adequacy decisions (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay).[53] Consequently, international data transfers are assimilated to intra-EU transfers. An adequacy decision usually covers all personal data towards a third country. Article 45 (1) of the GDPR allows finding adequacy for a "territory or one or more specified sectors within that third country." An example of a specific sector where the EU has reached an agreement with the U.S. concerns the airline Passenger Name Records transfers.[54]

The requirements for a third country to comply with are the core principles of data privacy: purpose limitation principle, data quality principle, proportionality principle, transparency principle and security principle.[55] In addition, onward transfers from the third country must also comply with the

[52] Reidenberg, *supra* note 17, at 1337 ("In the absence of comprehensive data protection legislation, the full range of internationally-recognized principles for fair information practice may be hard to satisfy; narrow, sectoral laws, policies, ad hoc protections and practices typically ignore key elements of the First Principles.").
[53] EU Commission, *Adequacy Decisions*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited June 15, 2020) (Adequacy talks are ongoing with South Korea).
[54] *See* Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, EU-U.S., Dec. 14, 2011, T.I.A.S. No. 12-701.
[55] *See* Data Protection Working Party, Working Document (WP 12) of 24 July 1998 on transfers of personal data to third a country. (DG XV D/5025/98).

principles.[56] Moreover, the data subject should have the right to access all data concerning him and the right to rectification and opposition.

i. International Commitments

In export data transactions the reference to international commitments in Article 45 (2)(c) of the GDPR would include the Council of Europe Convention 108 (CoE 108) plus the amending Protocol (2018) in order to assess the adequacy of a third country's data protection regime.[57] However, the United States is not a member of the CoE 108 whilst eight non-Members of Council of Europe signed the CoE 108.[58]

One difference in language exists to assess the data protection regime of a third country as a recipient of personal data. The yardstick of the original CoE 108 (1981) refers to an "equivalent protection" meanwhile the Modernised Convention (2018) refers to an appropriate level of protection.[59] The criteria to evaluate an appropriate level of protection are (i) the law of a third country State or international organisations, including the applicable international treaties or agreements; or (ii) *ad hoc* or approved standardized safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.[60] Modernised Convention 108 aligns with GDPR as there are grounds to allow personal data transfers even when not "appropriate level of protection exists." In particular, consent of the data subject, specific interests of the data subject or legitimate public interests when these interests are established by law and such transfer constitutes a necessary and proportionate measure in a democratic society, including freedom of expression. The first and last derogations, data subject's consent and freedom of expression in a democratic society are both novelties comparing the original with the Modernised Convention. However, the explicit reference to freedom of expression explicitly goes beyond the GDPR derogations.[61]

---

[56] *See* GDPR, arts. 44, 45 (2)(a).

[57] Council of Europe, Modernised Convention for the protection of individuals with regard to the processing of personal data, 2018, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 [hereinafter Modernised Convention 108]; Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018), Ad hoc Committee on Data Protection (CAHDATA), https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e.

[58] Eight non-members of Council of Europe signed the CoE 108 (Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, Uruguay), *see* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures (last visited July 16, 2020).

[59] *See* Modernised Convention 108, *supra* note 57, at 10.

[60] *See id*. art. 14(3).

[61] *See* GDPR, art. 49.

If the United States would accede to the Modernised Convention, it would be easier to conclude that the United States regime and the European Union regime are equivalent. Some commentators consider that the CoE 108 offers a level of protection lower that the European regime.[62] However, the amending Protocol enhances and clarifies data protection flows taken into account the GDPR, which means that when the Modernised Convention would be approved by every member of the Council of Europe, more convergence between both regimes would exist.[63] Therefore, a third country that overcomes the test of an appropriate level of protection via the Modernised Convention would facilitate the GDPR test of an equivalent level of protection. One of the advances of the Protocol is the broad application to public and private sectors, without the option to exclude national security activities.[64] Likewise, the powers of supervisory authorities are clarified.

ii. Adequacy Decisions are not Immune to Legal Challenges

Adequacy decisions issued by the EU Commission are not immune to be challenged under a court proceeding. Data protection authorities are in charge of monitoring and enforcing the GDPR.[65] Their tasks are detailed, including to handle complaints lodged by data subjects or organisations that represent data subjects[66] and conduct investigations on the application of the GDPR.[67] Thus, *ex parte* or *ex officio* data protection authorities can challenge the validity of an EU Commission adequate decision in legal proceedings (art. 57(5) of the GDPR). Data protection authorities may be obliged to suspend an administrative procedure in order to request authorization from the judicial body to declare if a Commission decision regarding international data transfers is valid.[68]

---

[62] *See* Julian Wagner, *The Transfer of Personal Data to Third Countries Under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?*, 8 INT'L DATA PRIVACY L. 318, 327 (2018).

[63] *See generally* Graham Greenleaf, *A World Data Privacy Treaty? Globalisation and Modernisation of Council of Europe Convention 108,* in EMERGING CHALLENGES IN PRIVACY LAW 101 (Normann Witzleb et al. eds., 2014).

[64] *See* Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data art. 3, Sep. 28, 1981, European Treaty Series - No. 108 [hereinafter Modernised Convention 108]; *see also* Proposal for a Council Decision authorizing Member States to sign, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) COM/2018/449 final - 2018/0237 (NLE), Brussels, 5.6.2018.

[65] GDPR, art. 57 (1)(a).

[66] GDPR, art. 57 (1)(f).

[67] GDPR, art. 57 (1)(h).

[68] *See Disposición adicional quinta. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, (Spanish Law of Data Protection, (B.O.E. n. 294, December 6, 2018)).

The Court of Justice of the European Union (CJEU) has exclusive jurisdiction to declare invalid a Commission decision adopted to consider if a third country ensures an adequate level of protection by reason of its domestic law or regarding the international commitments it has entered.[69] National courts can assess the validity of an EU act, but they cannot declare invalid themselves, as they are not endowed with the necessary power.[70] The CJEU uses *a fortiori* reasoning, considering that if national courts do not have competence, neither the national supervisory authorities. A Commission decision adopted pursuant to the article 25(6) of the Data Protection Directive is an EU act. Therefore, the protection of privacy and fundamental rights concerning transfer of personal data to third countries in the framework of a Commission decision under article 45 of the GDPR can only be declared invalid by the CJEU.

On the contrary, in the light of Article 8(3) of the Charter and article 28(3) of the Data Protection Directive where the national supervisory authority considers that the person claim is well founded, the supervisory authority must be able to engage in legal proceedings.[71] As a result, supervisory authorities must have legal capacity to be part of legal proceedings and bring the well-founded objections before national courts to enable them to ask the CJEU for a preliminary ruling if required.

The consequences are crucial because when the claimant contends that the law and practices in force in the third country do not ensure an adequate level of protection and brings a claim before the national supervisory authority, the supervisory authority must examine the claim, irrespectively of the existence of a Commission decision regarding the compatibility with the data transfers from the EU to a third country.[72] The right to private life, the right to data protection and the right to an effective remedy are fundamental rights under the EU Charter, enlightening the interpretation of personal data rules. In the *Schrems* I case, the repealed Directive on data protection was read together with articles 7, 8 and 47 of the EU Charter. This jurisprudence is alive and applicable in regard to the section of the GDPR concerning data transfer beyond the EU.[73]

iii. The Safe Harbour Principles

U.S. privacy law was defined as a "patchwork of narrowly-focused sectoral laws and voluntary self- regulation," that could not be relied upon to

[69] *See* Schrems v. Data Protection Comm'r*,* C-362/14, ¶ 61 (Oct. 6, 2015).
[70] *Id.* ¶ 62 (citing judgments in *Foto-Frost*, 314/85, (EU:C:1987:452), ¶¶ 15-20, and *IATA and ELFAA*, C-344/04, (EU:C:2006:10), ¶ 27).
[71] *See id.* ¶ 65.
[72] *See Schrems I*, *supra* note 43, ¶ 66.
[73] *See Schrems II*, *supra* note 43, ¶¶ 156-58.

provide adequate protection for data transferred from the EU in 1999.[74] However, the famous Safe Harbour Principles (SH) were an arrangement negotiated by the European Commission and the Federal Trade Commission to allow organisations to transfer personal data from the European Union to the United States provided they were self-certified.[75] Decision 2000/520 described seven SH Principles: notice, choice, onward transfer, security, data integrity, access and enforcement.[76] SH scheme was voluntary and entered into force in 2000.

Under the SH only companies subject to the jurisdiction of the Federal Trade Commission (FTC) could self-certificate and a proceeding against unfair and deceptive practices could be brought against the company who failed to comply with their promises.[77] For example, financial services would not fall within the FTC powers.[78]

The European Parliament in 2013 adopted several resolutions to urge the EU Commission to take actions to renegotiate the agreement granting EU citizens the right to information when their data is processed in the U.S.; ensuring that EU citizens' access to the U.S. judicial system is equal to that enjoyed by U.S. citizens, and that the right to redress is granted.[79]

The three issues declared by the EU Commission in 2013 were the following.[80] First, the privacy policies of companies benefited from the SH

[74] Opinion 1/99 of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the United States Government (Jan. 26, 1999); https://ec.europa.eu/justice/article29/documentatio n/ opinion-recommendation/files/1999/wp15_en.pdf.

[75] Without *ex-ante* verification from the FTC. *See* FAQ 6, Commission Decision 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, 2000/520/EC, OJ, L 215/7 (Jul. 25, 2000).

[76] Commission Decision 2000/520, annex I, 2000 O.J. (EC).

[77] Shara Monteleone & Laura Puccio, *From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU-US Data Transfer Rules*, at 6 (Jan. 2017). Other enforcement is undertaken by the US Department of Transportation for members who are subject to its jurisdiction. *See* Damon Greer, *Safe Harbour—a framework that works*, 1 INTERNATIONAL DATA PRIVACY LAW, 143, 146 (2011).

[78] *See* Article 29 Data Protection Working Party, Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles," adopted on May 16, 2000, CA07/434/00/EN WP 32.

[79] Resolution of 4 July 2013 on the US National Security Agency Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Privacy, 2016 O.J.(C 075) 14.

[80] Communication from the Commission to the European Parliament and the Council on Rebuilding Trust in EU-US Data Flows, 2013 O.J. (C 846); Communication from the

were opaque, which affected the enforceability by the FTC. Second, there was not a follow-up of the validity of the SH certification by the U.S. Department of Commerce. Third, the mechanism lacked means of redress for European citizens once the data were transferred to the U.S. Interestingly, the first implementation report of the functioning of SH by the European Commission on 20 October 2014, also identified that the concerned privacy policies were not publicly accessible, there was a lack of FTC enforcement and questioned third party dispute resolution mechanisms. The justification for not renewing the certification of 20% of companies was that "employees responsible for managing Safe Harbour compliance have left the organization without a transfer of duties to new personnel."[81] What type of commitment with privacy have organizations that do not continue with the self-certification method based on self-assessment?[82] Considering that if cost of non-complying with privacy law was larger than complying with data protection law,[83] it seems rare that companies do not train their employees to comply with privacy law. Some first skepticism regarding the attitude of U.S. companies about how global businesses operate with privacy laws arose.[84]

Safe Harbour defenders considered that its success was measured in terms of raising the level of privacy compliance in the U.S.[85] This sort of statements brings to light hat the level of privacy protection in the United States was lower than in Europe, precisely because the United States never asked for approval of an adequate decision by the Commission, since they sensed that the response by the European Commission would be negative.[86] That is why the SH was reached as a compromise. However, the CJEU ruled that the SH framework did not satisfy the "essentially equivalent" data protection under EU law.[87] *Schrems I* invalidated the Commission decision underlying SH. The rights of European citizens had been unprotected since

---

Commission to the European Parliament and the Council on the Functioning of the SH From the Perspective of EU Citizens and Companies Established in the EU, 2013 O.J. (C 847).

[81] Greer, *supra* note 77, at 147.

[82] *See* FAQ 7, Commission Decision 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, 2000/520/EC, OJ, L 215/7 (Jul. 25, 2000).

[83] *See* Ponenom Institute, *Cost of Compliance: Benchmark Study of Multinational Organizations* 2 (Jan. 2011), https://www.ponemon.org/local/upload/file/True_Cost_of_Compliance_Report_copy.pdf ($9.4 million versus $3.5 million).

[84] *See* Mary E. McIntire, *How a Law Seminar Inspired a Student to Bring a Case to Europe's Top Court*, THE CHRONICLE OF HIGHER EDUCATION (Oct. 7, 2015), https://www.chronicle.com/article/How-a-Law-Seminar-Inspired-a/233682.

[85] Greer, *supra* note 77, at 145.

[86] *See* Greer, *supra* note 77, at 144.

[87] *Schrems I, supra* note 43, ¶ 96.

the conception of the political commitment between the United States Government and the European Commission.[88]

From the legal-political point of view, on both sides of the Atlantic it was known that the SH failed to meet European standards on data privacy, despite designed to be complied to it.[89] The SH was active from its inception until it was struck down by the CJEU. But was this invalidation surprising? The legal battle simply granted European citizens the rights that they already have in their laws before 2015. American scholars warned the U.S. authorities, in particular the U.S. Department of Commerce, that the SH Principles did not meet European standards. Professor Schwartz expressly stated "the safe harbor principles largely track the worst aspects of the industry codes of conduct."[90] The European Parliament also warned the EU Commission before and after the SH Principles were enforced[91]. Hence, during 15 years European citizens' rights have been infringed. Only when the press and media focus on a particular event, this event gets on the public eye and the political discourse incorporates the claims of citizens, users and consumers.

iv. The EU Charter Significance

It is noteworthy that the rules of the Directive 45/95 continue in the GDPR, although its enforcement had been doubtful in the past.[92] Different reasons could justify such result: DPAs did not have sufficient means;[93] Member States in the transposition of the Directive did not agree on the limitation of data transfers because it was considered a limitation on the prospects for trade, as different regulation of exemptions shows;[94] or because simply verifying compliance with EU law beyond borders is very difficult, especially if there is no collaboration with foreign government entities. Weak implementation of Articles 25 and 26 of the Data Protection Directive was considered a "litmus test" for the Directive's international credibility and

---

[88] Joe McNamee, *Fifteen Years Late, Safe Harbor Hits the Rocks*, EUROPEAN DIGITAL RIGHTS (Oct. 6, 2015), https://edri.org/safeharbor-the-end/ ("In reality, however, the case is much deeper than 'just' mass surveillance. The European Commission has never had the political courage to recognize that Safe Harbor was never safe.").

[89] *See* Letter from Fred H. Cate, Robert E. Litan, Joel R. Reidenberg, Paul M. Schwartz & Peter P. Swire to David L. Aaron, Undersecretary for International Trade, U.S. Dep't of Com. (Nov. 17, 1998), https://cseweb.ucsd.edu/~goguen/courses/268D/agre.safe.html.

[90] Schwartz, *supra* note 31, at 1699.

[91] *See* European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), OJ 2017, C 378/104, (Nov. 2017).

[92] EUROPEAN COMM'N, FIRST REPORT ON THE IMPLEMENTATION OF THE DATA PROTECTION DIRECTIVE (95/46/EC) 18-19 (May 15, 2003).

[93] Lee A. Bygrave, *Privacy Protection in a Global Context: A Comparative Overview*, 47 SCANDINAVIAN STUDIES IN LAW 319, 346 (2004).

[94] *See* EUROPEAN COMM'N, *supra* note 92, at 11.

success.[95] However, strong implementation would also be accused of creating a bureaucratic procedure that could hamper trade, so avoidance was a logical scape.

This debate is linked to the scope of extraterritorial application of EU data protection rules, which has been founded on the protection of fundamental rights of EU residents beyond their situs of residence.[96] It could be argued that the essence of the fundamental right to data protection is enshrined in Article 8 of the EU Charter where a reference to cross-border data transfers is missing. Having jurisdiction and imposing limits when personal data have crossed borders and it is already located in a third country could be considered against the comity principle.

However, the CJEU held that satisfying an objective of general interest, namely against serious crime and public security was not exempt of limits and assessment of the secondary law in light of the fundamental rights needed to comply with the principle of proportionality.[97] Two mentions in the *Digital Rights Ireland* judgement could be key for data transfer abroad. Article 8 of the Charter was mentioned twice and can be considered the essential notion of data protection. First, Data Retention Directive did not provide for sufficient safeguards as the Directive did not ensure effective protection of the data "retained" against the risk of abuse and against any unlawful access and use of that data.[98] Second, a lack of reference to a prior review by a court or by an independent administrative body was missing in the Data Retention Directive, considering the access of competent national courts.[99] Article 8 (3) of the Charter was referred as an essential component of the protection of individuals with regard to the processing of personal data.[100]

Although the Data Retention Directive objective was to harmonize Member State law on retention of certain data on electronic communication, so within the EU borders, the same standards have been followed by the CJEU to assess the legality of data transfers abroad with EU fundamental rights.[101] The Privacy Shield did not pass muster at the proportionality test by virtue of analyzing the real powers of the Commission.[102] The discretion of the EU legislature must be also reduced, knowing in advance that personal data transferred to the U.S. is accessed by U.S. enforcement authorities.

---

[95] Bygrave, *supra* note 93, at 348.
[96] *See supra* Section I (C).
[97] *See* CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* (8 April 2014), (EU:C:2014:238), ¶ 54-60 [hereinafter CJEU, *Digital Rights Ireland*].
[98] CJEU, *Digital Rights Ireland*, ¶ 66.
[99] CJEU, *Digital Rights Ireland*, ¶ 68.
[100] CJEU, *Digital Rights Ireland*, ¶ 68, referring to Case C-614/10 *Commission v Austria* (EU:C:2012:631), ¶ 37.
[101] *See Schrems I*, *supra* note 43, ¶ 58.
[102] *Schrems II*, *supra* note 43, ¶ 201.

In *Digital Rights Ireland,* discretion of the EU legislature was curtailed because there was a wide interference with fundamental rights. Similarly, in *Schrems I* the CJEU held that the Commission's discretion is reduced when assessing the adequacy level ensured by a third country.[103] The key difference is that the high level of protection of personal data continues when data are transferred to a third country, following AG Yves Bot.[104] However, AG Bot called for a global assessment of law and practice in the third country,[105] but the CJEU only refers to law, following the literal wording of the article 25 (6) of the Data Protection Directive, domestic law and international commitments.[106] Indeed, article 25 (2) of the Data Protection Directive was more specific: "the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country." Moreover, this list is non-exhaustive.[107]

The determining factor in Bot's opinion is that "adequate" must be interpreted within the objective of the Data Protection Directive. Therefore, it discards the linguistic meaning of "sufficient protection" and it is closer to the meaning of "appropriate," insisting on data transfer to third countries should not be given a lower level of protection than processing within the EU.[108] According to AG Bot, "it must not be forgotten that the objective of Article 25 of Directive 95/46 is to prevent personal data from being transferred to a third country that does not ensure an adequate level of protection, in breach of the fundamental right to protection of personal data guaranteed by Article 8 of the Charter."[109]

The ratio of the adequacy requirements to such an extent are equivalent, since the adequate level of protection required by the GDPR corresponds to the level of data protection required by the EU Charter. However, the EU Charter was neither binding when the Directive entered into force nor when the SH Principles were approved by the EU Commission. With the GDPR in force, clearly the EU Charter has the same weight that the Foundational Treaties,[110] so *a fortiori*, the level of adequate protection from the Charter must have the same expression in the GDPR. Privacy Shield, like

[103] *Schrems I*, *supra* note 43, ¶ 78.
[104] *See* Opinion of AG Bot, delivered on 23 September 2015, Case C-362/14; (EU:C:2015:627), ¶140 [hereinafter Schrems I Advocate General Opinion]. *See also Schrems I*, *supra* note 43, ¶72.
[105] Schrems I Advocate General Opinion*, supra* note 104, ¶ 141.
[106] *See Schrems I, supra* note 43, ¶ 73.
[107] *See Schrems I, supra* note 43, ¶ 70.
[108] Schrems I Advocate General Opinion*, supra* note 104, ¶ 144.
[109] *Schrems I, supra* note 43, ¶ 148.
[110] *See* 2012 O.J. (C. 326) 232.

Safe Harbour, intrinsically concerns processing of personal data under the meaning of GDPR (art. 4.2) because both are mechanisms to transfer commercial data to the United States. EU data protection law is applied indirectly to the United States, without any practical difference between direct application and indirect application of EU data protection law.[111]

Thus, the territorial scope of the Charter should be the same as the GDPR, as this is a European Regulation.[112]

v. The Surveillance Matter

The hegemony of the U.S. as a surveillance country is rooted in some economical and technical reasons. The Internet backbone location routes through the U.S., even foreign to foreign communication, and popular software and hardware companies are based in the U.S.[113]

According to the European Commission, "the large scale access by intelligence agencies to data transferred to the US in the context of commercial transactions was not foreseeable at the time of adopting the Safe Harbour."[114] In the same communication the European Commission acknowledged that U.S. law allows large-scale collection and processing of personal data that is stored or otherwise processed by companies based in the United States.[115] Data transferred under SH to companies certified was easily accessible by U.S. authorities and intelligence under espionage programs like PRISM and these interferences went beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in the Safe Harbour Decision.

The CJEU did not analyzed the SH principles, but the fact that they were only binding the self-certified private entities, and not public authorities was noted as a gap of the mechanism.[116] The adequate level of protection is measured only in relation to what was considered in the Decision 2000/520.[117] Thus, the CJEU did not consider any development in U.S. law. But, should the CJEU judge U.S. law, a conflict of jurisdiction starts, so judge Lenaerts is

---

[111] *See* Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, GERMAN L. J. 881, 893 (2017).
[112] *See* Violeta Moreno-Lax & Cathryn Costello, *The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territoriality to Facticity, the Effectiveness Model, in* THE EU CHARTER OF FUNDAMENTAL RIGHTS: A COMMENTARY 1657 (Steve Peers et al. eds., 2014); Case C-617/10, Åklagaren v Åkerberg Fransson, 2013 C.J.E.U. ¶ 21.
[113] BRUCE SCHNEIER, DATA AND GOLIATH 64 (2015).
[114] *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU,* at 16, COM (2013) 847 final (Nov. 27, 2013).
[115] *Id.* at 17.
[116] *Schrems I, supra* note 43, ¶ 82.
[117] *Schrems I, supra* note 43, ¶ 83.

right when states: "we are not judging the U.S. system here, we are judging the requirements of EU law in terms of conditions to transfer data to third countries, whatever they be."[118] However, the judgment recognizes that the Decision 2000/520 establishes a primacy of U.S. law over EU law, in particular national security, public interest, or law enforcement requirements, so self- certified United States organisations are "bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them."[119]

Decision 2000/520 did not establish any limits of interference by public authorities with fundamental rights,[120] when the EU Commission knew that U.S. authorities could access to personal data transferred and processing them in an incompatible manner.[121] The Commission did not ensure that U.S. governmental access was strictly necessary and proportional and noticed that data subjects did not have administrative or judicial redress.[122] However, the CJEU did not explicitly mention data protection as a fundamental right when dealing with the interference on public interest requirements, but only referred to establish the existence of an interference with article 7 of the Charter, the fundamental right to respect for private life.[123] *Digital Rights Ireland* case was referred, but in that case the CJEU considered an interference of both article 7 and article 8 of the EU Charter.[124]

In U.S. law there was a distinction between crime and espionage.[125] On the one hand, investigating crimes need to follow the procedures under Electronic Communications Privacy Act (ECPA).[126] ECPA is a federal law that requires court orders to start surveillance in order to uncover a crime. On the other hand, the Foreign Intelligence Surveillance Act (FISA)[127] regulates espionage and how U.S. agencies gather foreign intelligence information within the U.S.[128] Despite court orders are needed and they are granted by a special federal court, the Foreign Intelligence Surveillance Court (FISC)

---

[118] Valentina Pop, *ECJ President on EU Integration, Public Opinion, Safe Harbor, Antitrust*, WALL ST. J.: BRUSSELS BLOG (Oct. 14, 2015), https://blogs.wsj.com/brussels/2015/10/14/ecj-president-on-eu-integration-public-opinion-safe-harbor-antitrust/.

[119] *Schrems I, supra* note 43, ¶ 86.

[120] *Schrems I, supra* note 43, ¶ 88.

[121] *Schrems I, supra* note 43, ¶ 90.

[122] *Schrems I*, *supra* note 43, ¶ 90.

[123] *Schrems I*, *supra* note 43, ¶ 87.

[124] Joined Cases C-293/12 & C-594/12, Digit. Rts. Ireland v. Minister for Commc'ns, Marine and Nat. Res., EU:C:2014:238, ¶ 37 (Apr. 8, 2014).

[125] DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 71 (2011).

[126] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2522, 2701-2711, 3121-3127 (2002).

[127] Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801-11 (2015).

[128] Solove*, supra* note 124, at 73.

meetings of the court are secret and orders are issued without the need of suspicion of wrongdoing.[129] One significant difference in a trial is that defendants can access the documents justifying the surveillance under ECPA, but FISA only allow review in camera.[130] The order under ECPA can last longer periods that under FISA and up to 120 days when a non-U.S. person is the target.[131] During the Bush Administration FISA was expanding and the subtle line between crime and espionage investigation was eliminated with the introduction of one word. Instead of "the purpose" of the investigation was to gather foreign intelligence, the PATRIOT Act introduced "a significant purpose" of the investigation.[132] Moreover, the FISA Amendments Act of 2008 permit the Attorney General and the Director of National Intelligence to acquire foreign intelligence information by jointly authorizing surveillance of individuals who are not "United States persons" and are reasonably believed to be located outside the U.S. Finally, Section 702 FISA authorizes foreign surveillance programs by the NSA.

B. Standard Contractual Clauses

i. A Contractual Alternative

Contract tools are a widely used mechanism to transfer personal data from the EU to the US. International data transfers can use "appropriate safeguards" as a legal basis pursuant to Article 46 of the GDPR. Standard data protection clauses adopted by the Commission are referred to in art. 46 (2) (c) GDPR. The CJEU has clarified that Standard Contractual Clauses (SCCs) adopted by the Commission Decision 2010/87 are valid.[133]Two relevant Commission Decisions exist with regard to SCCs. One establishes SCCs for data transfers from data controllers in the EU to data controllers established outside the EU or European Economic Area (EEA) (Commission Decision 2001/497/EC of 15 June 2001, modified by 2004/915/EC of 27 December 2004).[134] Another set of contractual clauses, adopted by the Commission

[129] Solove*, supra* note 124, at 74.
[130] 18 U.S.C. § 2518(9); 50 U.S.C. § 1806(f).
[131] 18 U.S.C. § 2518(5); 50 U.S.C. § 1805(d).
[132] Solove*, supra* note 124, at 76; Moreover, Justice Breyer explains using the authority of § 1881(a), the Government can obtain court approval for its surveillance of electronic communications between places within the United States and targets in foreign territories by showing the court (1) that a significant purpose of the acquisition is to obtain foreign intelligence information, and (2) that it will use general targeting and privacy-intrusion minimization procedures of a kind that the court had previously approved, 50 U.S.C. § 1881(a)(g). Clapper v. Amnesty Int'l USA, 568 U.S. 398, 423 (2013) (Breyer, J., dissenting).
[133] *Schrems II*, *supra* note 43.
[134] Commission Decision 2001/497/EC of June 15, 2001, on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, Under Directive 95/46/EC (Text with EEA relevance) (Notified Under Document Number C(2001) 1539), 2001 O.J. (L 181) 19;

Decision 2010/87, are for data transfers from controllers in the EU to processors established outside the EU or EEA.[135] Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amends Decisions 2001/497/EC and 2010/87/EU to implements *Schrems I* judgment.[136] Data protection authorities' (DPAs) powers are provided on the GDPR[137] and cannot be restricted by any Commission Decision.[138]

On the other hand, SCCs can also be adopted by a DPA and approved by the Commission under art. 46(2)(d) of the GDPR.

From a terminological perspective, there is a change with regard to art. 25 (2) Data Protection Directive, which referred to "adequate safeguards." This word change could suggest that safeguards have to be high and not merely sufficient, as in English the meaning can be controversial.[139] However, these protections apply to a particular data transfer when there is no adequacy in a third country to which data are to be transferred.[140] This protection is a "middle protection," that should be differentiated from the standard of the highest protection, only under an adequacy decision issued by the European Commission. In principle, these standards are different and an invalidation of one legal basis does not affect another legal basis.[141]

Decision 2010/87 has the effect of preventing DPAs to refuse data transfers made under contracts that incorporate the standard contractual clauses approved by the Commission. Organisations can use standard contractual clauses approved by the Commission for transfers within and beyond the EU. In contrast, standard contractual clauses adopted by a data protection authority can only be used for international transfer from the

---

Commission Decision 2004/915/EC of Dec. 27, 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 (Notified under Document Number C(2004) 5271), 2004 O.J. (L 385) 74.

[135] Commission Decision 2010/87 of Feb. 5, 2010, on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC of the European Parliament and of the Council, Notified under Document C(2010) 593) (Text with EEA relevance), 2010 O.J. (L 39) 5.

[136] Commission Implementing Decision (EU) 2016/2297 of Dec. 16, 2016 Amending Decisions 2001/497/EC and 2010/87/EU on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries and to Processors Established in Such Countries, Under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2016) 8471), 2016 O.J. (L 344) 100.

[137] *See* GDPR, arts. 51-59.

[138] *Schrems I*, *supra* note 43, ¶ 103.

[139] *See* Schrems I Advocate General Opinion, *supra* note 104, ¶142.

[140] Kuner, *supra* note 111, at 904.

[141] Kuner, *supra* note 111, at 905.

jurisdiction of that authority (art. 28 (8) GDPR).[142] Pursuant to art. 46 (2)(c) GDPR if an organization used SCCs approved by the EU Commission, no requirement to obtain a DPAs' authorization is needed. This is a significant change in comparison to the repealed Data Protection Directive.[143] However, DPAs in Member States retain powers to prohibit or suspend data flows in exceptional circumstances (art. 37 (1) (j) GDPR).[144]

SCCs are a template agreement drafted by the EU Commission in order to speed negotiations and contracting between data exporters and importers outside the EEA. The main purpose of SCCs would be to compensate for any deficiencies in the protection afforded by the third country of destination. In AG Saugmandsgaard øe opinion, the SCCs could not depend on the level of protection guaranteed in the third country of destination.[145] This opinion in part has been reversed by the *Schrems II* judgment,[146] bringing SCCs in a comma.[147]
The EU Commission does not have an obligation to evaluate the level of data protection in countries to which data are transferred under SCC, because the object of a SCC Decision is not a third country, a territory or a specific sector.[148] The Irish Data Protection Court in May of 2016 considered that SCCs could not address the deficiency in U.S. law, which failed to provide legal remedies to EU citizens.

ii. Obligations on Private Parties

SCCs pursuant to the requirement of Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, incorporates effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law. Transfers of personal data under the clauses of such a decision are suspended or prohibited

[142] *See* European Data Protection Bd., Opinion 17/2020 on the draft Standard Contractual Clauses Submitted by the SI SA (Article 28(8) GDPR) (May 19, 2020), https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-172020-draft-standard-contractual-clauses_en.
[143] *See* Data Protection Directive, *supra* note 4, at 40.
[144] This power was in art. 28 (3) Data Protection Directive; *see* Data Protection Directive, *supra* note 4, at 43.
[145] *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ireland, ECLI:EU:C:2019:1145 (Dec. 19, 2019).
[146] *See* Opinion of Advocate General Saugmandsgaard øe Case C-311/18, Data Prot. Comm'r v. Facebook Ireland, (EU:C:2019:1145) (Dec. 19, 2019), [hereinafter Schrems II Advocate General Opinion].
[147] *See* Daniel J. Solove, *Schrems II: Reflections on the Decision and Next Steps*, PRIVACY AND SECURITY BLOG (July 23, 2020), https://teachprivacy.com/schrems-ii-reflections-on-the-decision-and-next-steps/.
[148] *Schrems II*, *supra* note 43, ¶ 130.

in the event of the breach of such clauses or it being impossible to honour them.[149]

According to Decision 2010/87, the applicable law to evaluate the protection of fundamental rights is the law of the Member State in which the data exporter is established.[150] Therefore, GDPR forms part of that legislation.[151] The CJEU does not mention any Member State law that could be used as comparator between surveillance law in an EU Member State and the U.S. EU data controllers or processors and the recipient of personal data are obliged in particular by Clause 4(a) and Clause 5(a)-(b) of Decision 2010/87 to ensure that the law of the third country of destination does not go beyond what is necessary in a democratic society to safeguard, *inter alia*, national security, defense and public security and are not in contradiction with those standard data protection clauses.[152] The verifications must be done prior to the transfer from the EU to the third country. Pursuant to Clause 5(b) of Decision 2010/87, the recipient is under an obligation to inform the controller of any inability to comply with those clauses, giving the power to suspend the transfer of data and/or to terminate the contract to the EU controller.[153]

Power becomes an obligation. The controller is under a special obligation to inform the data subject before the data transfer or as soon as possible after. This obligation seems to be triggered only when special categories of data are transferred under Clause 4 (f) of Decision 2010/87. The data subject enforced its rights against the data exporter as third-party beneficiary (Clause 3 Decision 2010/87). The importer of the data does not have the obligation of informing the data subject concerned, but informing the data exporter under Clause 5(d) Decision 2010/87. The data subject can bring legal action against the controller (the data exporter) and have the right to compensatory damages as a result of any breach of the obligations referred to in Clause 3 (Third-party beneficiary clause) or in Clause 11 (sub-processing) of Decision 2010/87.

Moreover, the data exporter liability could be claimed against the data importer, arising out of a breach by the data importer or by his sub-processor of any of their obligations when the data exporter has factually disappeared or ceased to exist in law or has become insolvent.[154]

---

[149] *Schrems II*, *supra* note 43, ¶ 137.
[150] Commission Decision 2010/87 of Feb. 5, 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, art. 3(f)), 2010 O.J. (L 39) 5.
[151] *Schrems II, supra* note 43, ¶ 138.
[152] *Schrems II*, *supra* note 43, ¶ 141.
[153] *Schrems II*, *supra* note 43, ¶ 142.
[154] Commission Decision 2010/87 of Feb. 5, 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, annex cl. 6(2), 2010 O.J. (L 39) 5.

In case of a change in the relevant legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the standard data protection clauses, the controller is obliged to suspend the data transfer or notifying to continue the transfer. The mechanism seems to be active by the call of the data importer or a sub-processor in the third country concerned. It is not clear how the competent supervisory authority would control whether the proposed transfer should be suspended or prohibited in order to ensure an adequate level of protection. According to Clause 4(g), the controller (data exporter) should receive the notification by the data importer and communicate to the supervisory authority afterwards.

Therefore, a private party is obliged to assess the law of the concerned third country to ascertain whether the proposed transfer should be suspended or prohibited in case it does not ensure an adequate level of protection. Besides, according to the CJEU, the competent supervisory authority has not only a "right" to conduct an audit of the recipient of personal data,[155] but it is also required "to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence."[156]

The GDPR is clear in article 58 (f) and (j) that the supervisory authority shall have corrective powers, such as impose a ban on processing or order the suspension of data flows to a recipient in a third country. The result is that the same proactive requirement is placed on supervisory authorities to analyze on a case-by-case basis when equivalent protection cannot be ensured. The new adding in *Schrems II* is that data controllers must stop data transfers without waiting from a supervisory authority intervention, having an independent duty. The door is open to disagreements between different EU nations and even controllers about whether a particular country's law is adequate.

As Schrems used similar arguments that causes the annulment of the Safe Harbour Principles to challenge SCCs, one could think that the mechanism used to transfer data to a third country does not affect the result if the third country's law is not essentially equivalent to EU law. The essence of the fundamental rights is not measured in the specific mechanism but according to the recipient country of data transfers (the importing country). Brussels effect[157] would translate in a *de facto* regulation of the recipient country data protection law, albeit indirectly by data transfer legislation of the exporting country.

It remains to be seen how an EU controller or processor can compensate for the lack of data protection in a third country by way of appropriate safeguards when the SCCs do not bind public authorities. A

[155] *Schrems II*, *supra* note 43, ¶ 145.
[156] *Schrems II*, *supra* note 43, ¶ 112.
[157] Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012).

contractual mechanism based on SCCs should apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country.[158] The CJEU suggests controllers or processors using "supplementary measures" to protect data under the SCCs[159], but does not specify what measures these could be when the third country law is contrary to the SCC. From the CJEU reasoning, it is inferred that private parties (EU controllers and processors) are under an obligation to provide contractual guarantee of an adequate level of protection against access by the public authorities of that third country in order to continue transferring personal data. One solution could be data encryption, but the issues concerning government surveillance laws cannot be solved by private parties.

III. PRIVACY SHIELD: SOLUTION TO A TRADE CONFLICT

Privacy Shield Decision is a mechanism for transferring commercial data from the EU to the U.S.[160] The Privacy Shield was called a "cosmetic" make-over of the Safe Harbour agreement.[161] The main concern is that U.S. authorities are accessing this data without adequate safeguards, in particular the NSA surveillance programs have been challenged. Personal data could be accessed for national security purposes in a nebulous in between detection of crime and espionage.

As of 20 July 2020, 5394 organizations were certified under the Privacy Shield[162].The Privacy Shield could be suspended, amended or repealed in three scenarios: when U.S. public authorities fail to comply with the commitments, when complaints by EU data subjects are not systematically effectively address or when the Privacy Shield Ombudsperson does not provide timely and appropriate responses to EU data subjects systematically.[163]

A. Surveillance Interference: A Problem Not Solved

[158] *Schrems II*, *supra* note 43, ¶ 133.
[159] *Schrems II*, *supra* note 43, ¶134.
[160] Commission Implementing Decision 2016/1250 of July 12, 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 O.J. (L207) 1.
[161] Monika Zalnieriute, *Developing a European Standard for International Data Transfer after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, 81 THE MOD. L. REV. 1046, 1061 (2018).
[162] Department of Commerce, "Privacy Shield List," DEP'T. of COMMERCE: PRIV. SHIELD FRAMEWORK (July 20, 2020), https://www.privacyshield.gov/list.
[163] Commission Implementing Decision 2016/1250 of July 12, 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 O.J. (L207) 1, 36.

The new techniques appearing in the '60 obligated a rebalance of privacy and surveillance due to the low cost of resources and the ease with which new technologies have been used for penetration of privacy. Today the surveillance problem is not different, but the surveillance state is more exhaustive than ever before because it is perpetrated by private means. It can be argued that legislation was already considered anachronistic in 1992.[164] Surveillance done by the intelligence community is facilitated by the existing corporate surveillance.[165] Scholars have coined the term "surveillance capitalism."[166] Consumers accept corporate surveillance because they want to use their products, which are convenient. We should ask ourselves if there is any option not to trade our privacy for convenience. No privacy seems the price citizens have to pay to enjoy apps and electronic services. Without data protection laws, no private rights are to be asserted, so when international cooperation reaches an agreement that does not comply with basic international data privacy principles, which is really the position of an individual citizen?

Predominantly consumers don't really have a choice to opt-out of corporate surveillance.[167] The business apparatus to exploit customers is used not only for law enforcement but to prevent any risks. Without business collaboration with national agencies, government surveillance would be not so easy. And more important, business privacy policies need to protect consumers, but without legal frameworks, enforcement is impossible. Sometimes, even with an apt legal framework, public enforcement does not repair the real damage.[168] Although privacy and security are not the same concept, they complement each other, because security defines which privacy choices should be implemented.[169] According to Westin, the weighing process is defined in five steps to balance competing interests: the seriousness of the need to conduct surveillance, if alternative methods to meet the end exist, the reliability of the instrument, the need to consent and the capacity for limitation and control the surveillance mechanism.[170] If pointing to a social problem and

---

[164] *See generally* Joel R. Reidenberg, *The Privacy Obstacle Course: Hurding Barriers to Transnational Financial Services*, 60 FORDHAM L. REV. S137, S146 (1992) (referring to the implications of the European Convention and to the OECD Guidelines for complex financial service information processing. For example, any information that relates to an identifiable person is covered under the two instruments.).

[165] Schneier, *supra* note 113, at 78.

[166] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019).

[167] Schneier, *supra* note 113, at 49.

[168] *See* Schneier, *supra* note 113, at 46 (describing a case of a company that misled consumer by its privacy policy but the Federal Trade Commission didn't fine the company, though, because the app was free, the remedy was forcing the company to clean up its deceptive practices and delete the data it had collected).

[169] Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 669 (2013).

[170] ALAN F. WESTIN, PRIVACY AND FREEDOM 370 (1967).

solving it through surveillance is the only alternative, we can affirm that it doesn't exist a balance between privacy and surveillance.

From another angle but with the same background, Trump administration planned to ban Chinese social media in the U.S., claiming that personal data are prone to data requests from the Chinese government.[171] Although it is not clear what will finally happen, the location of a parent social media in China threatens national security, foreign policy and economy of the United States according to the executive orders.

The CJEU shows consistency with its previous judgement invalidating the SH principles.[172] The EU Commission could have been more cautious when agreeing in the language used in the PS. The Privacy Shield recognizes primacy of U.S. law over PS Principles 'to the extent necessary to meet national security, public interest, or law enforcement requirements' (paragraph I.5. of Annex II, under the heading 'EU-U.S. Privacy Shield Framework Principles). The CJEU remembers that in case of conflict between the Privacy Shield Principles and requirements on U.S. law, organizations are not only bound by the PS Principles, but also bound to disregard the PS principles without limitation. This is a relevant interpretation of the PS decision that it was not obvious in the literal language used. Indeed, the PS decision states "adherence to these principles may be limited," not "should be limited." According to this interpretation, organizations had no choice in case of conflict between PS Principles and national security, public interest, or law enforcement requirements.

The CJEU is brave in signaling three U.S. legal acts where an interference with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States.[173] The likelihood of transferring data is enough to trigger an interference with fundamental rights. It was already held that "it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference."[174] This is a significant difference with U.S. law standing.[175]

PRISM and Upstream surveillance programmes under Section 702 of the FISA and E.O. 12333 are the focus of the ruling. The CJEU does not prohibit surveillance programs, the analysis is limited to verify if appropriate

[171] Kari Paul, *Can Trump Ban TikTok? What the Executive Order Means – Explained*, THE GUARDIAN (Aug. 7, 2020), https://www.theguardian.com/technology /2020/aug/07/donald-trump-tiktok-executive-order-explainer.
[172] *Schrems II*, *supra* note 43, ¶164.
[173] *Schrems II*, *supra* note 43, ¶¶ 165-66.
[174] *Schrems I*, *supra* note 43, ¶ 87.
[175] *See* Clapper, 568 U.S. 398.

safeguards exist in U.S. law to limit U.S. access authorities to personal data transferred for commercial purposes.

NSA can access to all communication through internet services providers with a "selector" under the PRISM program.[176] Moreover, under the Upstream programme telecommunications companies are also required to allow the NSA to copy and filter internet traffic flows of communications sent or received by a non-US national associated with a selector or when communications are about that person.[177] A case is pending before the United States Court of Appeals for the Fourth Circuit that will need to rule on the constitutionality with the Fourth Amendment of the Upstream surveillance.[178]

B. Absence of Compatibility Between U.S. and EU Law

i. Previous Uncertainty Concerning Compatibility

Three French non-profit organizations claimed that the Privacy Shield failed to take into consideration the generalized nature of the collections allowed and the lack of effective remedy provided for under the U.S. regulatory regime.[179] Therefore, according to them, the U.S. protection was not substantially equivalent to that guaranteed within the European Union. They claim an infringement of the essence of the fundamental right to respect for private life guaranteed by Article 7 of the Charter. The three arguments were that operations allowed under the U.S. regulatory regime are not limited to what is strictly necessary, that there is a lack of an effective remedy and that there is also a lack of a provision of independent monitoring under the U.S. law.

In contrast to that argument, Professor Swire considers that U.S. surveillance law is compatible with EU fundamental rights. His claims are based on a strict rule of law, separations of powers and judicial oversight by the Foreign Intelligence Surveillance Court (FISC) of national security surveillance[180]. The judges of the FISC are independent federal judges with a lifetime appointment.[181] He considers that the Advocate General in the *Schrems I* case was not correct when he described that the NSA accessed the

---

[176] *Schrems II*, *supra* note 43, ¶ 61.
[177] *Schrems II*, *supra* note 43, ¶ 62.
[178] *See Wikimedia v. NSA – Challenge to Upstream Surveillance Under the FISA Amendments Act*, ACLU (Sept. 6, 2018), https://www.aclu.org/cases/wikimedia-v-nsa-challenge-upstream-surveillance-under-fisa-amendments-act.
[179] Case T-738/16, La Quadrature du Net and Others v. Commission, 2017 EUR-Lex CELEX Lexis (Jan. 9, 2017), https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62016TN0738.
[180] Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013,* GEORGIA TECH SCHELLER COLLEGE OF BUSINESS RESEARCH PAPER NO. #36 (Dec. 18, 2015), at 3, http://dx.doi.org/10.2139/ssrn.2709619".
[181] *Id.* at 8.

data through Facebook in a generalized and comprehensive manner, what was "mass, indiscriminate."[182] Section 702 of Foreign Intelligence Surveillance Act was revised in 2008 to cover surveillance based on targeting purposes of non-US citizens located outside the U.S.[183] To do that it is needed a certification of the FISC and identifiers (email address or phone number), which are used to limit collections and queries.[184] NSA can access to the full contents of communications, but raw data is destroyed after a period of two to five years.[185] This information is disseminated with other intelligence agencies. Foreign to foreign communications that are stored on US data servers can only be accessed by a federal court order (FISC) and following Section 702 FISA. However, the fact that only a small fraction of global internet users are effective targets under the Section 702 FISA (in 2014 there were 92,707) seems the arguable hard reason.[186] According to a FISC opinion, "over 90% of the Internet communications obtained by the NSA in 2011 under Section 702 actually resulted from PRISM, with less than 10% coming from Upstream."[187] Professor Swire thinks that if PRISM is considered a target program, Upstream should also be considered target because the collection is carried out with the same selector process.[188] But that is not what we can read in the New York Times: "The collection is part of a broader program under a 2008 law that allows warrantless surveillance on domestic networks as long as it is targeted at noncitizens abroad."[189]

NSA collection activities conducted illegally after 9/11 were authorized retroactively under Section 702 of FISA.[190] There were minimal protections for U.S. citizens.[191] Americans and non-Americans are on the same boat, because data about innocent people are found in authorized

[182] Schrems I Advocate General Opinion, *supra* note 104, ¶¶ 198-200.
[183] Swire, *supra* note 180, at 12.
[184] Swire, *supra* note 180, at 13.
[185] Swire, *supra* note 180, at 13.
[186] Swire, *supra* note 180, at 17.
[187] Swire, *supra* note 180, at 17.
[188] Swire, *supra* note 180, at 17.
[189] Charlie Savage & Scott Shane, *Secret Court Rebuked N.S.A. on Surveillance,* N.Y. TIMES (Aug. 21, 2013), https://www.nytimes.com/2013/08/22/us/2011-ruling-found-an-nsa-program-unconstitutional.html.
[190] Schneier, *supra* note 113, at 65.
[191] Schneier, *supra* note 113, at 65.

intelligence targets.[192] However, people cannot prove they are under surveillance.[193]

The Five Eyes is a partnership of intelligence agencies of English-language-speaking countries: U.S., UK, Canada, Australia, and New Zealand. The Nine Eyes adds France, Denmark, the Netherlands, and Norway: and the Fourteen Eyes, includes, Germany, Spain, Italy, Belgium and Sweden.[194] The NSA captures the communications of citizens of one country when they transit another country, therefore, it can be considered in accordance with the intelligence agencies agreement.[195] But the U.S. also shares data with Israel,[196] Saudi Arabia, and Turkey.

Some voices consider that surveillance programs as PRISM make the U.S. and its allies safer. However, that is questionable in light of an Open memorandum submitted to President Obama by Former NSA Senior Executives in 2014. Former NSA officials acknowledged that the massive collection of data does not enhance the ability to prevent terrorism, as telephone records prevent zero terrorist plots.[197] They explained that a devised process called THINTHREAD was developed by a group of NSA mathematicians and computer technology before 9/11 for collection and rapid analysis of billions of electronic records relating to targets of intelligence interest.[198] THINTHREAD ensures automatic encryption of information about U.S. persons, complying with the standard of FISA and the Fourth Amendment.[199] Therefore, "data on U.S. citizens could be decrypted only if a judge approved it after a finding that there was probable cause to believe that the target was connected with terrorism or other crimes."[200] This open memorandum demonstrates that abuses have occurred at least in terms of the procedures used by the NSA. However, the focus is on U.S. persons, whose

---

[192] Schneier, *supra* note 112, at 67 ("Some of this reflects the nature of intelligence; even, minimized information about someone will contain all sort of communications with innocents, because literally every communication with a target that provides any interesting information whatsoever will be retained."); *see also Amicus curia in Irish High Court, Case Data Prot. Comm'r v. Facebook Ireland Limited* (Feb. 27, 2017) ("U.S. Privacy Law does not provide adequate safeguards for personal data and private communications of E.U. citizens and does not provide an effective means of redress for a breach of Charter Rights."), https://epic.org/privacy/intl/schrems/02272017-EPIC-Amended-Submissions.pdf.
[193] *See* Clapper, 568 U.S. 398.
[194] Schneier, *supra* note 112, at 77.
[195] Edward Snowden, *Statement to the European Parliament*, European Parliament (Mar. 7, 2014), https://www.europarl.europa.eu/document /activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.
[196] Schneier, *supra* note 112, at 76-77.
[197] *NSA Insiders Reveal What Went Wrong,* CONSORTIUM NEWS (Jan. 7, 2014), https://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong/.
[198] *Id.*
[199] *Id.*
[200] *Id.*

privacy has been abused. Nothing is said about foreign targets, but it would not be surprising a positive answer, as access was provided. According to these ex senior NSA executives, "[t]hat NSA's bulk collection is more hindrance than help in preventing terrorist attacks should be clear by now despite the false claims and dissembling."[201]

ii. The Schrems II Ruling: The Proportionality Principle

The absence of compatibility between U.S. and EU law does not focus on commercial privacy rights in the landmark *Schrems II* ruling on 16 July 2020. The CJEU's analysis focuses on the lack of proportionality and limitations in surveillance measures targeting non-American citizens. Limitation of fundamental rights are plausible, but pursuant to art. 52 (1) of the EU Charter only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.

The principle of proportionality is applied to PRISM and Upstream programs regulated under Section 702 FISA. The CJEU states that the FISC does not review if 'individuals are properly targeted to acquire foreign intelligence information' because the focus is checking whether those surveillance programmes relate to the objective of acquiring foreign intelligence information.[202] On the other hand, Presidential Policy Directive 28 (PPD-28) allows for bulk collection and limits on dissemination and retention, but does not grant data subjects actionable rights before the courts against the U.S. authorities.[203] Moreover, E.O. 12333 allows access to data overseas and in transit to the United States without that access being subject to any judicial review. Thus, in any event, E.O. 12333 does not delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data.[204] The CJEU wants to ensure that the persons whose data are transferred have sufficient guarantees to protect effectively their personal data against risk of abuse. The concerned legal basis must "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."[205] Furthermore, automated processing exacerbates the need for such safeguards.[206] The lack of proportionality refers to collection and use of personal data and the need of minimum safeguards of control over use and retention of personal data gathered by the government.

---

[201] *Id.*
[202] *Schrems II, supra* note 43, ¶ 179.
[203] *Schrems II*, *supra* note 43, ¶ 181.
[204] *Schrems II*, *supra* note 43, ¶ 183.
[205] *Schrems II*, *supra* note 43, ¶ 177.
[206] CJEU Opinion 1/15, Draft Agreement Between Canada and the European Union, ECLI:EU:C:2017:592, ¶¶ 140-41 (July 26, 2017).

Finally, the CJEU held in *Schrems II* that the U.S. did not provide an equivalent protection to the EU. The limitations on U.S. surveillance programs in Section 702 of the FISA and E.O. 12333, together with read PPD-28, "correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary."[207] Consequently, the PS Decision does not satisfy that the requirements on U.S. domestic law on access and use by public authorities of such data transferred from the EU to the U.S. are essentially equivalent to those required under article 52 (1) of the EU Charter.[208]

Schrems II judgment shows that different parts of a legal system are not watertight compartments. Trade may be affected as a consequence of lack of guarantees and limitations of the laws on surveillance, whose object is national security and public interest. The AG's opinion at *Schrems I* was criticized for its views on mass surveillance.[209] The CJEU did not mention that mass and undifferentiated accessing of personal data is clearly contrary to the principle of proportionality and the fundamental values, but that it was raised by the Irish High Court in relation to the compatibility with the Irish Constitution.[210]

The pivotal concern in *Schrems II* is not a transatlantic understanding of privacy principles in the private sector, which has always been a significant difference between the European and American approaches. The difference lies in the effects of data access by the government, an issue in which Americans have always been pioneers and have tended to fear their government more than companies. The fact that Europeans, specifically Schrems, brought to court the case of data could be accessed by American intelligence agencies implies to approach the problem from a completely different angle to the traditional opposition between Europe and the U.S. regarding privacy. The case has certainly made more accessible information about the U.S. surveillance review in comparison to other parts of the world.

However, it should not be forgotten that the EU benefits to some extent from the U.S. intelligence, if not as a whole, of course some of its Member States. That cooperation should not be compromised. The system must be improved, so that Europeans can bring a lawsuit in case of surveillance before the U.S. courts. Although everything seemed resolved with the principle of equality, when it was agreed that European citizens would have access to the same redress mechanisms as Americans[211] that promise is actually an empty shell, taking into account that even American citizens themselves have no

[207] *Schrems II*, *supra* note 43, ¶ 184
[208] *Schrems II*, *supra* note 43, ¶ 185.
[209] *See supra* Section III (B)(i).
[210] *See Schrems I*, *supra* note 43, ¶ 33.
[211] *See infra* Section III (C)(i).

such possibility in the event of surveillance. What is being asked is not equal rights but accommodation to the framework of fundamental rights that prevail in the EU. This framework may not be exactly the same as the one that binds the Member States by the European Convention on Human Rights (ECHR), since the EU Charter is only activated when EU law is applied or the Member States implement EU law.[212]

Furthermore, the establishment of a higher level in European law is also completely in accordance with the Charter. The wording of article 52 (3) of the Charter establishes that the meaning and scope of Charter rights shall be the same as those laid down by the ECHR, afterwards it clarifies "This provision shall not prevent Union law providing more extensive protection."

Given the current regulation with the GDPR, it is clear that the fundamental rights contained in the Charter cannot go unnoticed. The CJEU is right in not mentioning any article of the ECHR whilst the Advocate General considers that such regimes of interception of electronic communications, even on a mass scale, are compatible with Article 8 (2) of the ECHR provided that they are accompanied by a number of minimum guarantees.[213] Indeed, the leading interpretation was already held in *Schrems I*. The express obligation under EU law to protect personal data reading in light of Article 8 (1) of the EU Charter is intended to ensure that the high level of that protection continues where personal data is transferred to a third country.[214] The fear of the CJEU was that without demanding an essentially equivalent level of protection in the third country, EU law could be easily circumvented.[215]

The Commission's experience in negotiating the SH and the subsequent annulment by the CJEU could have prevented the outcome of *Schrems II*. Yet the crucial point at this moment is solving a debate on available remedies under surveillance laws.

The EU has been accused of being hypocritical under the premise that some Member States do not have such limitations and safeguards with regard to surveillance.[216] Nevertheless, the topic is different because EU membership presupposes that Member States comply with EU values and that makes them beneficiaries of internal data flows. This was one of the great handicaps that the EU faced long ago. However, it is not true that there is a double standard.

---

[212] *See Charter of Fundamental Rights of the European Union,* European Union, art. 51, § 1, 26 October 2012, 2012/C 326/02.
[213] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland, ECLI:EU:C:2019:1145 ¶ 282 (Dec. 19, 2019).
[214] *See Schrems I*, *supra* note 43, ¶ 72.
[215] *Schrems I*, *supra* note 43, ¶ 73.
[216] *See* David Bender, *Having Mishandled Safe Harbor, Will the CJEU Do Better with Privacy Shield? A US Perspective*, 6 INT'L DATA PRIVACY L. 117, 123 (2016).

What happens is that the CJEU focuses on the analysis of U.S. law because the specific case concerns the Commission decision to transfer data from the EU to the U.S. In the near future, this standard could be applied to any country without an adequacy decision by the Commission. In fact, the validated use of SCCs does not prevent this mechanism from being insufficient when the recipient of the data cannot guarantee the same level of protection that the data had in the EU.

Some DPAs have been quick to point out that data under the PS system should not be transferred to the U.S. and that all transfers using the Commission's SCCs should be reviewed.[217] In the short term, a ban on data from certain countries and specifically the U.S. could happen. It is not only a legitimate reason, but it is worthy that personal data continues in the EU to comply with legislation. However, the costs of implementing such a short-term solution must be studied. The question that arises is whether this answer is practical, considering that while large companies probably will not have problems in the implementation (since they often operate under transnational groups), small ones could face technical problems.

C. Lack of Effective Legal Remedies

i. U.S. Law Developments Does Not Affect Surveillance

The very existence of effective judicial review is inherent in the existence of the rule of law. The essence of Article 47 of the EU Charter is to provide individuals to pursue legal remedies when their fundamental rights are infringed. Recent U.S. developments concerning redress were not mentioned by the CJEU whilst invalidating the Privacy Shield.

First, the U.S. Judicial Redress Act (JRA)[218] extends to EU citizens the judicial redress provisions in the U.S. Privacy Act of 1974.[219] Second, the U.S. FREEDOM Act forbids bulk collection in national security matters[220]. It is claimed that the U.S. is the only country that has finished a bulk collection program.[221] However, these legal improvements only concern American citizens.[222]

---

[217] *See Berlin: Berlin Commissioner issues statement on Schrems II case, asks controllers to stop data transfers to the US* (July 17, 2020), https://www.dataguidance. com/news/berlin-berlin-commissioner-issues-statement-schrems-ii-case-asks-controllers-stop-data.
[218] Judicial Redress Act, Pub. L. 114-126, 130 Stat. 282 (2016).
[219] *See* The Privacy Act of 1974, 5 U.S.C. § 552a (2015).
[220] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 272 (2015).
[221] Fred H. Cate & James X. Dempsey, Introduction and Background to BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA xxviii (2017).
[222] Franziska Boehm, *Assessing the New Instruments in EU-US Data Protection Law for Law Enforcement and Surveillance Purposes*, 2 EUR. DATA PROT. L. REV. 178, 190 (2016).

Concerning the first legislative act, the JRA was considered a pre-condition to sign the U.S.-EU "umbrella" Data Privacy and Protection Agreement. In principle, it extends to all data subjects in the EU the right to enforce their data protection rights in U.S. courts, for instance, in case of unlawful disclosure of records or for unjustified refusal to access data.[223]

However, several exemptions make the JRA not useful for a surveillance context. Citizens of covered countries are permitted to bring civil actions against U.S. federal agencies and obtain civil remedies, but damages only when intentional or willful conduct is shown.[224] It excludes non-EU citizens, for example, any natural person that is not a citizen of a covered country, which is contrary to article 47 and 21 of the EU Charter.[225] Moreover, it only applies for certain violations of the Privacy Act and there is no right to restrict the collection of data, but rather a right to access, rectify and disclose personal data. As JRA does not establish a right to minimize the collection of surveillance data for U.S. citizens, they are not empowered to enforce it. In the same way, the extension of no right to Europeans does not solve the problem of redress in light of the EU Charter. Furthermore, in the case of the Privacy Shield, the Attorney General may require to certify that the policies for transferring personal data for commercial purposes of the country 'do not materially impede the national security interests' of the U.S.[226] The approval of the head of 'designated Federal agency or component is needed. Thus, if the head of the NSA does not concur, the NSA will not be a designated agency and the JRA will not apply to it.[227]

Second, the FREEDOM Act makes changes regarding bulk collection of phone records and the content of the FBI request. Stricter minimization conditions applied for FBI access, retention and dissemination of personal data.[228] Moreover, the *amicus curiae* mechanism makes it possible for experts to participate in the proceedings in front of the FISA court. However, the issue with the FREEDOM Act is that the new protections refers to U.S. persons.

The CJEU notes that the Commission erred on the assessment about judicial redress in the Privacy Shield Decision.[229] Concerning unlawful (electronic) surveillance for national security purposes, no effective judicial

---

[223] *See* MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RSCH. SERV., R44257, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 13 (2016), https://fas.org/sgp/crs/misc/R44257.pdf.

[224] *See* 5 U.S.C. § 552a(g)(4). S*ee also In re Jet Blue Airways Corp. Privacy Litig*., 379 F. Supp. 2d 299 (E.D.N.Y. 2005) (plaintiffs failed to prove damages for passenger records sharing with the government).

[225] In contrast, The Freedom of Information Act (FOIA) applies to "any person." *See* 5 U.S.C. § 552a(b).

[226] *See* Judicial Redress Act of 2015, H.R. 1428, 114th Cong. §2(d)(1)(C) (2016).

[227]*See* Bender, *supra* note 216, at 130.

[228] Boehm, *supra* note 222, at 184.

[229] *Schrems II*, *supra* note 43, ¶ 191.

redress is mentioned. Therefore, PRISM and Upstream programmes based on Section 702 of the FISA and those surveillance programs based on E.O. 1233 do not have an effective remedy because U.S. law does not grant individuals actionable rights in the courts against the U.S. authorities.[230] The Commission Decision violates Article 47 of the Charter as the United States law does not ensure a level of protection essentially equivalent to European law. Indeed, the US Supreme Court did not grant standing to a group of plaintiffs claiming that they were likely under surveillance and had to take expensive measures to avoid that surveillance.[231] The justification was they could only speculate as to whether they were under surveillance, but did not prove it.

ii. Lack of Independence of the Privacy Shield Ombudsperson

One of the essential elements of data protection is that requirements stemming from Article 8(1) and (2) of the EU Charter are subject to control by an independent authority.[232] For instance, the Proposed Agreement on the processing of Passenger Name Records between the EU and Canada did not ensure the independence of the supervisory authority, because the language used "an authority created by administrative means that exercises its functions in an impartial manner and that has a proven record of autonomy" seems to permit that the Canadian authority was subject to a subordinate relationship and was not free from any external influence on its decisions.[233]

The U.S. government created an Ombudsperson Mechanism as a contact point for foreign governments that wish to raise concerns regarding U.S. signals intelligence activities. According to Annex III to the Decision, the Privacy Shield Ombudsperson is independent from the Intelligence Community.[234]

However, the Privacy Shield Ombudsperson is not independent, as it is an integral part of the U.S. State Department. In particular, the Privacy Shield Ombudsperson is appointed by the Secretary of State and reports directly to him. The CJEU points out that no additional safeguards come along with the appointment, dismissal or revocation of the Privacy Shield Ombudsperson.[235] Additionally, the PS Ombudsperson does not have authority to adopt binding decisions, which does not guarantee the conditions

---

[230] *Schrems II*, *supra* note 43, ¶ 192.
[231] Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).
[232] *See* C-518/07, Comm'n v. Germany, ECLI:EU:C:2010:125, ¶ 25 (March 9, 2010); *See also* C-288/12, Comm'n v. Hungary, ECLI:EU:C:2014:237, ¶ 48 (April 8, 2014).
[233] CJEU, Opinion 1/15, (July 26, 2017), ¶ 230.
[234] *See* Annexes to the Commission Implementing Decision, Annex III, Letter from U.S. Secretary of State John Kerry, (July 7, 2016), https://www.ftc.gov/system/files/documents/plain-language/annexes_eu-us_privacy_shield_en1.pdf; Recital 116, Privacy Shield Decision.
[235] *Schrems II*, *supra* note 43, ¶ 195.

for an effective remedy in accordance with Article 47 of the Charter.[236] In conclusion, the created mechanism does not afford EU citizens a level of protection essentially equivalent to that guaranteed by the fundamental right of an effective remedy.

D. No Legal Vacuum: Reduced Alternatives

The validity *in abstracto* of the Commission Decision 2010/87 is separated from the inadequacy finding of a third country legal system. However, both are correlated because data transferred for commercial purposes between private companies that can be processed for the purposes of public security, defense and State security by the authorities of that third country remain under the scope of the GDPR.[237]

Binding corporate rules (BCRs) are a common mechanism to transfer data among large corporations, when an adequacy decision is lacking.[238] However, BCRs are designed for a group of undertakings and are usually costly to negotiate. Moreover, regarding the U.S. as a recipient country, BCRs could suffer from similar consequences as SCCs after *Schrems II*.

The CJEU sends a strong message: there is no legal vacuum after invalidating PS. Therefore, there is no will to maintain the effects of the Privacy Shield decision for the purposes of avoiding the creation of a legal vacuum, because according to its judgment, legal vacuum does not exist.[239] Article 49 of the GDPR provides derogations for specific situations, like explicit subject data's consent or necessity for the performance of a contract. In the case of consent of the data subject, the individual must have been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards by virtue of article 49 (1)(a) of the GDPR. Hence, *Schrems II* will condition the used of the consent exemption regarding transatlantic data transfers.[240]

Recital 112 GDPR offers some examples of public interest reasons, including the case of contact tracing for contagious diseases. The second paragraph of art. 49 of the GDPR allows a transfer to a third country provided that is not repetitive, concerns only a limited number of data subjects and is necessary for the purposes of compelling legitimate interests pursued by the controller. In this scenario, the controller should inform the data protection

[236] *Schrems II*, *supra* note 43, ¶ 196.
[237] *Schrems II*, *supra* note 43, ¶ 86.
[238] *See* GDPR, arts. 46, ¶ 2(b), 47.
[239] *Schrems II*, *supra* note 43, ¶ 202.
[240] Pedro A. De Miguel Asensio, *La Nueva Sentencia Facebook—Schrems más Allá de la Invalidez del Escudo de Privacidad* (July 20, 2020), https://pedrodemiguelasensio.blogspot.com/2020/07/la-nueva-sentencia-facebook-schrems-mas.html#more.

authority of the transfer and assess all the circumstances surrounding the transfer.

Nonetheless, article 49 of the GDPR should work as a last resort mechanism for transfers of exceptional nature because derogations should be interpreted restrictively.[241] The use of derogations per se does not imply in all cases that the country of destination does not ensure an adequate level of protection, and it does not ensure the opposite either.[242]

According to the European Data Protection Board, derogations are for specific situations that are exceptional, based on individual cases and cannot be used for massive or repetitive transfers.[243] Recital 113 of the GDPR also refers to not repetitive transfers, but does not exempt the controller from providing suitable safeguards to protect fundamental rights and freedoms of natural persons.

The *Schrems II* decision applies to all types of companies, regardless of size and organization. Case-by-case assessment of circumstances is going to be essential in practice. Not only the derogations from Article 49 of the GDPR, but also the nature of the data and whether U.S. companies are electronic communications service providers subject to Section 702 FISA or if they are not electronic communications service providers, but rely on them, for example, by storing data in the cloud. For instance, the EU-U.S. data transfers could continue from a European micro-company dependent on the flow of data to the U.S. because the U.S. recipient is not obliged under FISA to possible access by U.S. authorities and the data being transferred relates to health.

E. Further Consequences of Invalidating International Agreements

The invalidation of SH by the CJEU was seen as an obstacle to commerce, but the question is why to endorse laws that are not enforceable. The Privacy Shield has also been challenged under CJEU scrutiny. Indeed, the Advocate General in the controversial decision of *Schrems II* clearly considered that PS is not compatible with the EU legal order. However, he suggested the Court not to rule on the PS and limit their judgment to the Standard Contractual Clauses issued by the EU Commission. According to him, the SCCs are compatible with data protection law and if companies use

[241] Working Document 12/2001, Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the Data Protection Directive (July 24, 1998); Report on the Additional Protocol to Convention 108 on the Control Authorities and Cross Border Flows of Data, art. 2(2)(a), http://conventions.coe.int/Treaty/EN/Reports/Html/181.htm.
[242] Working Party, Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, 2093/05/EN WP 114 at 6 (Nov. 25, 2005).
[243] European Data Prot. Bd., Guidelines 2/18 on Derogations of Article 49 under Regulation 2016/679 at 4 (May 25, 2018).

them as a ground to transfer personal data from the EU to the U.S., they are safe with regard to the legality of the transborder mechanism used. The practical issue is how a mechanism can be compatible as an alternative when the international treaty—which supposes to guarantee data privacy—does not afford an equivalent level of protection to the EU order. The inconsistency of AG Opinion in *Schrems II* suggestion can only be explained by the difficult balance that has to be struck between the current international commerce and enforcement of data privacy principles. Safe Harbour principles were a political-economic compromise to continue cross-border data flows and Privacy Shield inherits the same character of being a negotiable instrument as a voluntary mechanism for U.S. companies. The *Schrems I* judgement influenced and accelerated reaching to the Privacy Shield agreement, but some scholars rightly stated that perhaps temporary. Then, Privacy Shield would have been like a patch waiting for new reforms in the U.S. on data protection and intelligence power.

The CJEU decided that the party is over again and the invalidation of PS did not come by surprise. The judgement represents a continuation of the Court's jurisprudence on the regulation of international data transfers, although it does not follow in its entirety the non-binding opinion by the AG. The Irish Data Protection Commission welcomes *Schrems II* judgement, underscoring that the CJEU endorses the substance of the concerns expressed by the Irish High Court and the Data Protection Commission, but pointing that using SCCs as a valid transfer mechanism, many questions still remain concerning the application of the SCCs to EU-U.S. data transfers.[244] Therefore, further and careful examination on a case-by-case basis is required. Moreover, the Irish Data Protection Commission observes that a supervisory authority could not suspend data transfers while an adequacy decision was in force[245] and offers its collaboration with the rest of supervisory authorities to develop a common position for an effective implementation of *Schrems II*. By contrast, the Berlin supervisory authority states that personal data may generally no longer be transmitted to the U.S. as before until the legal situation changes.[246] Relocating services in the EU or in a country that offers an adequate level of protection may be mandatory. Exceptions exist in the special cases provided for by law, for instance when booking a hotel in the U.S.

The U.S. Secretary of Commerce has immediately expressed its deeply disappointment with the European Commission's adequacy decision

[244] Data Protection Commission, DPC Statement on CJEU Decision (July 16, 2020), https://www.dataprotection.ie/en/news-media/press-releases/dpc-statement-cjeu-decision.
[245] *See supra* Section II(B)(i).
[246] Press Release, Berliner Beauftragte für Datenschutz und Informationsfreiheit [Berlin Comm'r for Data Protection], Nach „Schrems II": Europa braucht digitale Eigenständigkeit [According to *Schrems II*: Europe Needs Digital Independence] (July 17, 2020) (Ger.) (on file with author).

underlying the EU-U.S. Privacy Shield.[247] The U.S. approach seems to want to "educate" the CJEU on U.S. national security data access laws and practices, underlining that U.S. rules exceed European ones. From a practical perspective, the Department of Commerce asseverates to continue with the certification of the PS. It makes sense that the privacy principles are maintained, because the lack of compatibility is due to a surveillance mechanism that private companies cannot solve by themselves.

However, the consequences of the reasoning of the Court reach beyond transatlantic partners. Requiring data controllers to evaluate if a third-country offers an adequate level of protection when applying SCCs means that they should have in-depth knowledge of a third-country legal order. Likewise, as it was stated by experts when invalidating SH, non-democratic governments would not qualify as an adequate protection, which would need to re-examine every mechanism to transfer personal data beyond the EU.

On the one hand, a relevant country to look into is the UK. From 2021 the UK will not belong to the EU. The ruling could complicate reaching an agreement after Brexit, considering the mass surveillance taking place in that country. This judgment is an indicator of what EU data processors could do to transfer data to the UK. Some ideas already on the table could be to encrypt every data and to develop codes of conduct or certification mechanisms to be used as legal basis for the data transfer together with binding and enforceable commitments.[248] However, this is an optimistic viewpoint because if circumvention of the GDPR is not permitted, an adequate level of protection in the third country would be needed. At least, with respect to data transfers to the U.S., irrespective of the mechanism used, the lack of surveillance limitations seems to be solved by amending domestic legislation. It would be expected that the analysis in any other country, including the UK, would need to pass muster the GDPR's interpretation in light of the EU Charter.

On the other hand, to accommodate third country norms would be challenging, in particular when law enforcement rules are not existent or intricate to obtain.[249]

---

[247] *See* Press Release, U.S. Dep't of Com., U.S. Secretary of Commerce Wilbur Ross Statement on *Schrems II* Ruling and the Importance of EU-U.S. Data Flows (July 16, 2020), https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and

[248] *See* GDPR, art. 46(2)(e)-(f).

[249] *See* Christopher Kuner, *The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation,* EUR. L, BLOG (July 17, 2020), https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/.

IV. CONCLUSION

Whereas privacy laws exist in a territory, citizens would naturally think that they can be respected. If the EU advances data protection as a fundamental right for their citizens and their personal data is out of control when they use the internet, why do Europeans have rules that can be so easily manipulated? If privacy is dead, why should legislators care about data transfers? The answer could be that data privacy is a subjective concept, difficult to prove harm individually but affecting every future step of an individual life. Individuals have protection only through laws and enforcement of laws. Competition is another area where tech giants are in trouble, but it is precisely the abuse of their market dominant position that is more prevalent and the lack of public and private enforcement would not be good news for consumers. The absence of choice between companies in relation to services have negative consequences for consumers. No data privacy laws and lack of public and independent enforcement leave citizens unarmed in the digital society.

Some authors have made an analogy of data protection dynamics in 2016 and the dynamics after the end of the Second World War.[250] Data protection depend on normative commitments established in advance.[251] The regulation of data privacy involves a relationship of power, that is why the State gets involved. If laws like the GDPR provide EU residents with "fundamental rights", the lack of enforcement turns the Regulation and any other binding agreement into worthless scraps of paper. The Sacramento effect as a kind of privacy superregulator in the United States[252] could be considered a reaction of the EU data privacy model success in the marketplace of ideas. The EU had shown bargaining power with flexibility,[253] however, flexibility that tends to build bridges cannot disadvantage European citizens in a U.S. context when U.S. companies operate in Europe.

Reaching a solution will involve diplomacy. A transatlantic interoperability is needed between languages and among cultures.[254] Negotiations between authorities have shown that enforcing power in a unilateral way is not an alternative. Both authorities have an interest in enforcing their privacy laws in an extraterritorial manner. The final solution will be to understand that data have a value in itself and that data protection legislation must play its role. The problem is the surveillance society in which

---

[250] Simon Davies, *The Data Protection Regulation: A Triumph of Pragmatism Over Principle*, 2 EUR. DATA PROT. L. REV. 290, 291 (2016).
[251] Bambauer, *supra* note 169, at 673.
[252] Chander et al., *supra* note 27, at 5.
[253] Schwartz, *supra* note 19, at 774.
[254] For a study on "legal interoperability", *see generally* JOHN PALFREY & URS GASSER, INTEROP, THE PROMISE AND PERILS OF HIGHLY INTERCONNECTED SYSTEMS 177-192 (2012).

we are immersed. Governments must respect data protection and privacy as human rights. The International Principles on the Application of Human Rights to Communications Surveillance[255] (2014) is a good start. Indeed, big American tech companies very recently said that they would temporarily stop processing requests from other governments for user data, which seems a commitment with fundamental rights abroad.[256] Citizens must raise their voice. Private society must convince and argue why our privacy is important not only in the country of residence but also abroad. Finally, safeguards must be in place to restrict government agencies' access to private data of citizens.

[255] NECESSARY & PROPORTIONATE, INTERNATIONAL PRINCIPLES ON THE APPLICATION OF HUMAN RIGHTS TO COMMUNICATIONS SURVEILLANCE (2014), https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf.

[256] *See* Hadas Gold, *Facebook, Google and Twitter won't Give Hong Kong Authorities User Data for Now*, CNN (July 7, 2020), https://www.cnn.com/2020/07/06/tech/whatsa pp-facebook-hong-kong/index.html.