CATÓLICA
FACULDADE DE DIREITO
ESCOLA DE LISBOA

CATÓLICA
Global
School of
Law

Data Transfers between the EU and US: The impact of Schrems I and Schrems II for cross-border data flows, privacy, and national security.

Bora Duli

Master of Transnational Law

Supervisor: Prof. Luís Heleno Terrinha

May 31, 2021

Abstract

This dissertation seeks to outline the implications of the CJEU judgment in Case C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II) on international data transfers, particularly for data transfers between the European Union and the United States. The Schrems II judgment has invalidated the Privacy Shield, making it the second data transfer mechanism between the EU and the US that the CJEU strikes down. It also leaves Standard Contractual Clauses (SCCs) as one of the only options for data transfers, creating significant burdens for companies/organizations to assess the laws and practices of third countries to be able to transfer data. The Schrems II decision, without a doubt, will change the relationship between global data flows and national security, and we have already started to see the legal uncertainties brought forward by the case. This dissertation aims to give an overview of the history of data protection laws in both the EU and the US, including differences in their approaches to data protection. It then examines the two Schrems cases and the invalidated transfer mechanisms, as well as the legal landscape for transfers after CJEU's last decision. Lastly, it discusses the impact of the decision on cross-border data flows, data privacy, surveillance, and national security, while trying to chart a path forward by examining possible solutions for the continuance of data transfers.

Keywords: data protection, surveillance, privacy

Table of Contents

Introduction

The world we live in is in almost every sense tied to international data transfers, and much of it came from the exponential growth of the Internet and technology. Flows of data continue to increase every day, bringing forth regulatory challenges in protecting individuals' privacy. Data protection is considered a fundamental right in Europe. Its laws aim for high levels of protection within its borders and seek to provide the same protection to the data of EU individuals when they are transferred from the EU to third countries. The main principle for data transfers from the EU to third countries is providing 'adequate protection,' meaning that transfers can happen if the third country offers protection that is 'essentially equivalent' to that in the EU. Around the world, countries have embraced the EU's view of privacy and data protection by enacting similar laws. Other countries, the US being one of them, have different views of privacy and how data protection should be regulated.

These differences present a threat to the EU-US trade, of which a considerable amount involves personal data. To mend issues rising from different views of privacy between the two, the EU and the US have created mechanisms for transfers of data. The main purpose of these mechanisms was to ensure adequate protection for data and compliance with EU standards. Although these mechanisms helped many companies and organizations transfer personal data to the US, their demise came with the Edward Snowden revelations in 2013, which showed the extent of data surveillance of EU citizens by the US surveillance agencies. The leaks led to a case before the CJEU, Maximillian Scherm’s v Data Protection Commissioner (Schrems I), and the invalidation of the first mechanism, the Safe Harbour. Once again, the EU and US negotiated a second mechanism called 'The Privacy Shield,' which in July 2020 had the same fate as its predecessor and was invalidated for lack of adequate protection. The EU and US are once again in talks about creating a new mechanism to continue the free flow of data. The requests set out by the two Schrems judgments have set the standards that need to be followed by the new agreement, but we still do not know how this agreement will look.

This dissertation aims not to evaluate the extent to which US law meets the EU law requirements for transferring personal data. Instead, it analyzes and gives an overview of the current data protection landscape post-Schrems II. In Part 1, the dissertation explores the history of data protection laws in the EU and the US and how they regulate data protection while also discussing mass surveillance by national security agencies and their access to

individuals' data. Part 2 gives an overview of international data transfers between the EU and the US, the Safe Harbour and Privacy Shield mechanism and the two Schrems cases which have led to their invalidation, along with the options still valid for data transfers and data localization. Part 4 will deal with the issues Schrems II brought forward when trying to negotiate a new agreement. It discusses the balancing of national security with privacy, the data surveillance by EU Member States intelligence agencies, and the issues that might arise for past and future adequacy agreements between the EU and third countries. The dissertation will conclude with the options available and the paths that the EU and US might take for a future agreement.

1. History of data protection in the EU and US

The legal systems of both the EU and the US have acknowledged how vital protecting personal data is, along with the risks that come from data misuse. While the same goal of data protection is shared on the two sides of the Atlantic, there are differences in their regulatory models and personal data protection.[1] This section will look into the history of data protection in the EU and US and their laws. It will also discuss how both sides view privacy and give a short overview of the US's mass surveillance of personal data.

1.1 Data protection in the EU

European data law has developed from a common protection system into a legal domain that protects personal data and the privacy of individuals over the years. The protection of personal data and the privacy of communications is recognized as a fundamental right in Articles 7 and 8 of the EU Charter of Fundamental Rights,[2] which is binding on all EU member states.[3] Although Europe did not have a uniform data law, the right to privacy was recognized with the European Convention of Human Rights in the 1950s.[4] The first data protection laws were enacted in the 1970s in different member states. The German Federal State of Hessen is considered to have adopted the first data protection law,[5] with many European countries such

[1] Reidenberg, Joel R. 'Resolving Conflicting International Data Privacy Rules in Cyberspace'. Stanford Law Review 52, no. 5 (May 2000): 1315.
[2] Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN
[3] Art. 6 of the Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 December 2007, 2007/C 306/01. http://publications.europa.eu/resource/cellar/688a7a98-3110-4ffe-a6b3-8972d8445325.0007.01/DOC_19
[4] Art. 8 of European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, https://www.echr.coe.int/documents/convention_eng.pdf
[5] Hessian Data Protection Act of Oct. 7, 1970, GESETZ UND VERORDNUNGSBLATT [GVBI] 625.

as France, [6] Ireland,[7] Austria,[8] and Finland[9] adopting privacy laws shortly afterward. These laws aimed to stop the evasion of the legal protection of data processing by transferring personal data to countries that did not have any data protection laws.[10]

The OECD developed the "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data"[11] in 1980, a set of international guidelines that established several important privacy and data protection principles and which many member states of the EU decided to adopt into their national laws.[12] From a global perspective, these guidelines are the first attempt of countries to regulate transborder data flows. While they were seen as having their limitations because of their non-binding nature, these guidelines received great support because they aimed to create minimum privacy and personal data protection standards and eliminate any restrictions to transborder data flows from OECD countries.[13] The following year "Convention 108"[14] was adopted by the Council of Europe, making it the first binding international instrument for protecting individuals against abuses that may come from automatic processing of personal data. "Convention 108" provided comprehensive coverage and is considered one of the instruments which gave considerable rise to the right to data protection, as its primary objective was the protection of individuals and regulation of transborder flows of personal data.[15]

Still, harmonization of rules at the EU level continued to be a challenge for Europe. While some member states had passed strict rules, procedures, and limitations, others had no rules regarding data protection and cross-border transfers of personal data.[16] Conflicting national laws proved to be trade barriers in the internal market, so the EU decided to create a

---

[6] Act No. 78-17 on Information Technology, Data Files and Civil Liberties, 1978.
[7] Data Protection Act 1988 (25/2988).
[8] Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener.
[9] Personal Data File Act, 30 April 1987/471 (CJ-PD (88) 15).
[10] Christopher Kuner, '*Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future*', OECD Digital Economy Papers, vol. 187, OECD Digital Economy Papers, 8 December 2011.
[11] https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[12] 'Data Protection Regulations and International Data Flows: Implications for Trade and Development | UNCTAD' (UNCTAD (United Nations Conference on Trade and Development), 2016), https://unctad.org/webflyer/data-protection-regulations-and-international-data-flows-implications-trade-and
[13] Ibid., p. 27.
[14] Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, 28 January 1981, ETS 108, https://rm.coe.int/1680078b37
[15] Kuner, '*Regulation of Transborder Data Flows under Data Protection and Privacy Law'*, p.15.
[16] Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means', *Information & Communications Technology Law* 28, no. 1 (2 January 2019).

Directive to improve cross-border trade by removing any obstructions to the flow of data within the common market.[17] Directive 95/46,[18] known as the Data Protection Directive, was introduced in 1995 with articles and provisions which included data quality, the rights of data subjects, and supervisory authorities. Under Directive 95/46, member states were required to adopt national privacy laws "equivalent" to one another to provide the same level of protection throughout the EU.[19] Intended to cover only the EU member states, the Directive had a powerful impact on data processing practices globally.[20]

In 2012 the negotiation of new data protection rules began across Europe, intending to achieve greater harmonization of data privacy laws and better protect individuals' data privacy rights.[21] The current Directive, created in the nineties in a time when the Internet had just begun to have its "boom," had to be updated since our lives had and would continue to change as a consequence of the Internet and big data. In 2018, the EU introduced its stringiest data protection rules to the world when it enforced the General Data Protection Regulation (GDPR).[22] The GDPR solidified the harmonization of data protection across the EU by bringing forward one unified regulation and made it simpler for organizations and companies to continue their business within the EU while ensuring that individuals' rights were protected and gave individuals more control over their data.[23] It also gave Data Protection Authorities (DPAs) extensive powers and covers the transfer of personal data outside the EU.[24]

The GDPR, made up of seven principles, asks for personal data to be "processed lawfully, fairly and in a transparent manner."[25] Among other requirements, it asks for data to be collected only for the purposes claimed and says that data cannot be processed in a manner

---

[17] Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, *The Brussels Effect* (Oxford University Press, 2020).
[18] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995.
[19] Ibid., Art. 8.
[20] Neil Robinson et al., 'Review of EU Data Protection Directive: Summary', *RAND Europe*, 2009, 14.
[21] Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46.
[22] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC 2016) OJ L119/1, [hereinafter GDPR].
[23] European Commission and Directorate-General for Justice and Consumers, *The GDPR: New Opportunities, New Obligations. What Every Business Needs to Know about the EU's General Data Protection Regulation.* (Luxembourg: Publications Office, 2018), https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-sme-obligations_en.pdf.
[24] Aurelia Tamò-Larrieux, *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things*, 1st ed. 2018, Issues in Privacy and Data Protection 40 (Cham: Springer International Publishing : Imprint: Springer, 2018).
[25] GDPR, Art. 5(1).

incompatible with those purposes. Data also has to be protected against "unauthorized or unlawful processing."[26] There are several options for transfers of personal data outside of the EU under the GDPR. Data can be transferred to a third country that has been given an 'adequacy decision' by the Commission, meaning that the third country provides an 'adequate level of data protection' as that afforded in the EU.[27] Other means include appropriate safeguards such as standard contractual clauses (SCCs) or binding corporate rules (BCRs) and derogations in specific situations.[28]

Many countries over the years have entered into negotiations with the EU to obtain adequacy agreements. With the GDPR, it is for the Commission to decide whether a country ensures such a level of protection for data to be transferred without additional safeguards. When assessing the adequacy of the level of protection, the Commission considers the rule of law of the country and respect for human rights and fundamental protections. It also looks at the existence and functioning of an independent supervisory authority responsible for ensuring and enforcing compliance with data protection rules and the international commitments by the third country regarding the protection of personal data.[29] Until now, the Commission has recognized Switzerland, Andorra, Israel, Argentina, South Korea, and eight other countries as providing adequate protection.[30]

The other legal basis for transferring personal data outside of the EU, SCC's, is an agreement by data exporters in the EU and the data receiving party outside the EU to provide adequate protection to the data transferred.[31] BCR's can also be used as legally binding data protection obligations that must be respected by all the entities in a corporate group and need approval by the DPA in the relevant member state.[32]

1.2 Data Protection in the US

In contrast to the EU, the US has long advocated a very liberal approach to data protection. The US does not have a single central data protection regime; instead, a wide range

[26] Ibid. Art. 5(a)(f).
[27] Ibid., Art. 45.
[28] Ibid., Art. 46.
[29] Ibid., Art. 45.
[30] European Commission. (2019). Adequacy Decisions, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[31] Commission Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries.
[32] Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems', *German Law Journal* 18, no. 4 (July 2017): 881–918.

of federal and state laws regulate personal data privacy and security.[33] Even though the US Constitution does not explicitly guarantee the right to privacy, interpretations have provided individuals with the right to protection against unreasonable searches and seizures from the government.[34] Congress has passed several federal laws for the privacy and protection of individuals' data, which the Federal Trade Commission is tasked with enforcing. States have also enacted statutes with varying purposes and scope at the state level, such as personal information held by internet service providers, website privacy policies, and medical records.[35]

Several federal laws protect the personal information of individuals. These laws are not extensive and usually lay down data protection obligations for specific sectors of industries, such as health care and financial institutions, or specific data types such as children's data.[36] Similar laws also apply to private entities. For example, The Stored Communications Act (SCA)[37] has outlawed the disclosure or unauthorized access of particular electronic communications stored by Internet Service Providers.[38] While federal laws impose limits on how companies can handle personal data, there is no institution in the US whose main task is to enforce data protection. Instead, a consumer protection agency, the Federal Trade Commission (FTC), has the authority under the Federal Trade Commission Act to protect US citizens' data and take action against 'unfair' or 'deceptive' business practices that ensue privacy violations.[39]

In 1974, the Federal Privacy Act[40] was enacted to regulate how the federal government collects, maintains, uses, and discloses personal information in records systems. The law came as a response to concerns about the effect of records of individuals held by federal agencies on individuals' privacy rights. Although considered the historical beginning of codification of fundamental personal privacy principles in the US, the Act does not require companies to

[33] Stephen P Mulligan and Chris D Linebaugh, 'Data Protection Law: An Overview' (Congressional Research Service, 25 March 2019) https://fas.org/sgp/crs/misc/R45631.pdf.
[34] Rory Little, 'Protecting Privacy Under the Fourth Amendment', *The Yale Law Journal* 91 (1981): 31.
[35] Mulligan and Linebaugh, 'Data Protection Law: An Overview'.
[36] Ibid.
[37] The Stored Communications Act (SCA), 18 U.S.C. § 2701 https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter121&edition=prelim
[38] Mulligan and Linebaugh, 'Data Protection Law: An Overview', p. 8.
[39] Bradford, *The Brussels Effect*.
[40] Privacy Act of 1974, 5 U.S.C. § 552a, https://uscode.house.gov/view.xhtml?req=(title:5%20section:552a%20edition:prelim.

comply with specific data protection policies. It only requires them to comply with their published data security and data privacy promises.[41]

In addition to federal laws, hundreds of state laws focus on data privacy and data security. State laws usually impose restrictions and obligations on entities on collecting, using, disclosing, and safeguarding their residents' data.[42] Some states are more focused on data protection than others. However, the US has seen an unprecedented number of legislative proposals regulating data privacy at the state level in the last year alone.[43] An example of a state that has enacted a comprehensive data protection regime is California, which passed the California Privacy Rights Act (CPRA) in 2018. One of the stringiest comprehensive privacy protections in the US, the CPRA gives consumers more control over personal data collected from companies and the right to opt out of the sale of their information.[44] New York also updated their data breach notification law in 2019, with specific requirements for entities to introduce "reasonable" safeguards to protect private information's confidentiality, security, and integrity.[45]

1.3 Different views of privacy

The main area of regulatory divergence between the EU and the US in their approaches is attributed to their different data protection views.[46] The US has long held a system of self-regulation and enforcement by the industry and companies, in which the industry is responsible for the privacy policies they create, and consumers are supposed to bargain with the companies for the level of protection they expect to receive.[47] This view grants individuals direct participation in market relations to trade their data or 'commodity' as it is considered.[48] In the European system, fundamental rights protect the individual's data, and the EU institutions must

[41]Harold C Relyea, 'The Privacy Act: Emerging Issues and Related Legislation' (Congressional Research Service., 26 February 2002), https://fas.org/irp/crs/RL30824.pd.f.
[42] Global Legal Group, 'International Comparative Legal Guides', Text, International Comparative Legal Guides International Business Reports (Global Legal Group), United Kingdom, https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.
[43] David McCabe and Cecilia Kang, 'As Congress Dithers, States Step In to Set Rules for the Internet', The New York Times, 14 May 2021, https://www.nytimes.com/2021/05/14/technology/state-privacy-internet-laws.html.
[44] California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100].
[45] Global Legal Group, 'International Comparative Legal Guides', Chapter 1, 1.2.
[46] Lauren B Movius and Nathalie Krup, 'U.S. and EU Privacy Policy: Comparison of Regulatory Approaches', 2009, 19.
[47] Anupam Chander, Margot E. Kaminski, and William McGeveran, 'Catalyzing Privacy Law', *SSRN Electronic Journal*, 2019, p.13.
[48] Paul M Schwartz and Karl-Nikolaus Peifer, 'Structuring International Data Privacy Law', *International Data Privacy Law* 7, no. 2 (2021): 49.

safeguard these rights.[49] Over the years, several EU Member States have recognized the right to privacy and related rights as constitutional rights, either through their national constitutions or through case law.[50] The right to privacy and data protection in the EU does not provide individuals with protection only against their governments; they also protect them against private entities.[51] In contrast to the EU, the US looks at individuals' right to privacy from a commercial standpoint and refers to individuals whose personal data is processed as "consumers."[52]

In addition, the EU follows a "prescriptive" approach in which the law stipulates data protection laws and obligations, whereas the US follows more of a "performance-based approach" with more flexible regulations which outline objectives but leave to the industry to decide on how they will achieve them.[53] Any limitation to data protection has to be provided for by law and proportionate in the EU. The interest of EU data law is focused on economic interests and the free flow of information, but most importantly, it focuses on safeguarding the fundamental rights of individuals. The CJEU, in its case law, has explained that no breach of fundamental rights to privacy and the protection of data can be justified by the economic interests that entities have from that processing.[54] This differs from US data protection law, where the marketplace is the dominant logic, and personal data processing is considered to impact the digital economy and innovation positively.

1.4 Mass surveillance by the US and systematic government access to private-sector data

For a long time now, governments around the world have collected personal information about individuals for different purposes, including national security and law enforcement. The collection of data has grown over the years, especially in the twenty-first century, due to continuous threats to countries' national security due to terrorist attacks and cybersecurity attacks. Governments have also found it easy to collect personal data due to the enormous

[49] Movius and Krup, 'U.S. and EU Privacy Policy: Comparison of Regulatory Approaches', p.172.
[50] Bert-Jaap Koops et al., 'A TYPOLOGY OF PRIVACY', *University of Pennsylvania Journal of International Law* 38, no. 2 (2017): 483–575.
[51] GDPR, Art. 3.
[52] Paul M Schwartz, 'GLOBAL DATA PRIVACY: THE EU WAY', *NEW YORK UNIVERSITY LAW REVIEW* 94 (October 2019): 48.
[53] Stephen P Mulligan and Chris D Linebaugh, 'Data Protection and Privacy Law: An Introduction', An Introduction, 9 May 2019, p. 3.
[54] Case C-131/12, Google Spain SL & Google Inc. v Agencia Española de Protecccción de Datos (AEPD) & Mario Costeja González, ECLI:EU:C:2014:317, paragraph 81.

amount of data generated and stored about individuals every day and the easy access to data collected and stored by third parties from individuals and organizations using their services.[55]

US surveillance programs present obstacles to the transfers of personal data from the EU to the US as several US laws allow for foreign data collection and data surveillance for national security reasons by US intelligence agencies. An essential part of the US's data collection is made possible by the framework of national security inquiries, namely the Foreign Intelligence Surveillance Act (FISA) and the PATRIOT Act.[56] These statutory provisions provide US public authorities with access to electronic surveillance of foreign information in the interest of national security. Through amendments, they now also provide access to certain business records for foreign intelligence and investigations of international terrorism.[57] There is a lack of transparency as the FISA court orders along with the evidence and the decisions taken for that court order remain secret, leaving the supervisory oversight to data retention programs extremely weak.[58] While the Fourth Amendment protects individuals' right to data privacy, the constitutional restrictions do not include information provided to the public authorities by third parties.[59] It has been ruled that a 'legitimate expectation of privacy' does not exist in the information provided to third parties and that these public authorities are not limited by constitutional rights when it comes to data obtained from these entities.[60]

The US has over the years enacted acts to limit the access that public authorities have to personal data online. In 1986, the Electronic Communications Act was introduced to limit the unauthorized access of law enforcement agencies to a person's electronic communications,[61] along with the Stored Communications Act to limit the ability of the government to access user data and limit the ability of Internet Service Providers from voluntarily disclosing the data of their users to the government.[62] However, Edward Snowden's revelations regarding the

[55] Fred H Cate, James X Dempsey, and Ira S Rubinstein, 'Systematic Government Access to Private-Sector Data', *International Data Privacy Law* 2, no. 4 (2012): 5.
[56] Joel R Reidenberg, 'The Data Surveillance State in Europe and the United States' 49 (Wake Forest L): 27.
[57] European Parliament. Directorate General for Internal Policies of the Union., *A Comparison between US and EU Data Protection Legislation for Law Enforcement Purposes.* (LU: Publications Office, 2015). https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf
[58] Chris D Linebaugh and Edward C Liu, 'EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield' (Congressional Research Service, 2021), p. 8, https://fas.org/sgp/crs/row/R46724.pdf.
[59] Little, 'Protecting Privacy Under the Fourth Amendment', p.315.
[60] Smith v. Maryland, 442 US. 735 (1979).
[61] Orin S Kerr, 'The Next Generation Communications Privacy Act', University of Pennsylvania Law Review 162 (2014): 373–419., p.375.
[62] Orin S. Kerr, 'A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It', George Washington Law Review 72 (2004): 1208–1243.

surveillance programs by national security agencies have rightfully concerned individuals about their data privacy and security.[63] Even though public knowledge that most countries have surveillance programs in place, the extent of those unauthorized surveillance programs fuelled resentment and distrust towards entities that collect the data and surveillance agencies with access to it.[64]

2. International data transfers between EU and US

Transfers of personal data across national borders are imperative to economic growth, social interaction, and technology advancements in our day and age.[65] Thousands of companies and individuals who use their services depend on international data transfers. The EU and the US continue to be each other's most significant trading and investment partner, and transfers of personal data across the two have contributed to the strengthening of trade and innovation.[66] International data flows are imperative to the business and greater economy of the EU and the US. Any restriction impacts trade and investment opportunities, which in turn increases costs for individuals and organizations.[67]

This section will discuss the agreements between the EU and the US for in data transfers, namely the Safe Harbour[68] and Privacy Shield[69] frameworks, both now invalidated by the CJEU due to the Schrems I[70] and Schrems II[71] cases. The section will discuss both frameworks, the cases that invalidated them, and the mechanisms still in place that allow for the international transfers of data.

[63] The Privacy and Civil Liberties Oversight Board found the NSA's bulk collection of telephone metadata to be unauthorized under Section 215 and in violation of the Electronic Communications Privacy Act. See 'Report on the telephone record programme conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court', https://fas.org/irp/offdocs/pclob-215.pdf.
[64] Holmes, Dawn E. Big data: a very short introduction. Oxford University Press, 2017.
[65] Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems', p. 882.
[66] Shayerah Ilias Akhtar, 'U.S.-EU Trade and Investment Ties: Magnitude and Scope' (Congressional Research Service, 2020), https://fas.org/sgp/crs/row/IF10930.pdf.
[67] Andrew D Mitchell and Jarrod Hepburn, 'DON'T FENCE ME IN: REFORMING TRADE AND INVESTMENT LAW TO BETTER FACILITATE CROSS-BORDER DATA TRANSFER', *TECHNOLOGY Vol.* 19 (2018): 56.
[68] Commission Decision 2000/520 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, 26 July 2000, [hereinafter Safe Harbour]
[69] Commission Decision 2016/1250 on the adequacy of the protection provided by the EU-US. Privacy Shield, 12 July 2016, [hereinafter Privacy Shield]
[70] Case C–362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650), [hereinafter Schrems I]
[71] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems and intervening parties, ECLI:EU:C:2020:559, [hereinafter Schrems II].

2.1 Safe Harbour Agreement and Schrems I

Shortly after adopting Directive 95/46, negotiations started between the European Commission and the US Department of Commerce for a framework that would eliminate the restrictions and the disruption of personal data transfers by the Directive. The termination of data transfers was a threat for both EU and the US, the various industries, and businesses, as it had real chances of diminishing trade.[72] This framework would allow US companies to meet the EU requirements for data protection and allow transfers of personal data between the two. The final result was the 'International Safe Harbour Privacy Principles' adopted as a Commission Adequacy decision.[73]

Notice, choice, onward transfers, security, data integrity, access, and enforcement were the seven basic principles the Commission had decided companies in the US had to comply with to be considered as providing an "adequate level of protection."[74] Companies were required to self-certify to the US Department of Commerce annually to show their compliance with the principles leading the way for them to transfer personal data collected in the EU to the US.[75] While negotiations for the principles were underway, the Article 29 Working Party had considered the decision as important and significant progress towards protecting personal data; however, it criticized the number of exceptions to the principles.[76] Activists from both sides of the Atlantic argued that the agreement did not succeed in providing the same protections and substantive rights as Directive 95/46. Despite all the criticism in the EU, over two thousand US companies adopted the Safe Harbour principles in the first two years.[77] Still, advocates of the data privacy field continued to voice their concerns, this time about US corporations not complying with the principles and the lack of enforcement and transparency from the US authorities. This issue, coupled with the fact that the US did not have an institution assigned to ensure data protection enforcement, was very worrying.[78]

---

[72] Martin A Weiss and Kristin Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield' (Congressional Research Service, 2016), p. 6, https://fas.org/sgp/crs/misc/R44257.pdf.
[73] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520
[74] Safe Harbour, Annex I.
[75] Ibid., recital 6 and Annex VII.
[76] Article 29 Data Protection Working Party, Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles", https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp32_en.pdf
[77] Schwartz and Peifer, 'Transatlantic Data Privacy Law', p. 177.
[78] Marc Rotenberg, 'Schrems II, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection', *European Law Journal* 26, no. 1–2 (2020).

Although the Safe Harbour problems were well known and argued, the Snowden revelations about mass surveillance by the NSA in the US became one of the critical drives to its invalidation.[79] The leaked documents showed US intelligence services' access to personal data transferred from the EU to the US by the companies certified by the Safe Harbour mechanism. In 2013 Max Schrems, an Austrian national, filed a complaint with the Irish Data Protection Authority asking for them to prohibit Facebook from transferring his data from their servers in Europe to Facebook Inc. in the US.[80] In light of leaks of US surveillance public authorities' activities - particularly the NSA, Schrems argued that the law and practices in force in the US did not allow for adequate protection of his personal data.[81] In particular, Schrems asked the Irish DPC to interpret the 'Safe Harbour' Decision in line with Directive 95/46 and fundamental rights, and brought up the possibility of the decision's invalidation if it did not provide enough protection for the data of EU citizens.[82] The Irish DPC rejected the complaint as unfounded, saying that it had no inclination to investigate since Facebook adhered to the Safe Harbour Principles, and went on to say that any question of the adequacy of data protection in the US would be determined in accordance with the Safe Harbour Decision which the Commission had already found as providing an adequate level of protection as required by Directive 95/46.[83] Schrems then took the case to the Irish High Court, who then referred it to the CJEU requesting a preliminary ruling to determine if DPA's of Member States had the power to investigate individual complaints related to a Commission Decision to assess the adequacy of that decision.[84]

In October 2015, the CJEU issued their decision in which they found that the existence of a Commission Decision did not reduce, interfere or eliminate the powers of DPAs of member states.[85] The second part of the judgment focused on whether the Safe Harbour Adequacy Decision was invalid. The CJEU did not focus on US surveillance programs' legitimacy but instead decided to deal with the concept of "adequacy." The CJEU noted that there was no definition for the concept of "adequate level of protection."[86] After looking at the Directive 95/46 wording, it decided that the level of protection in a third country had to be "essentially

[79] 'Edward Snowden: Leaks That Exposed US Spy Programme', *BBC News*, 17 January 2014, https://www.bbc.com/news/world-us-canada-23123964.
[80] Schrems I, Paragraph 27.
[81] Ibid., Paragraph 28.
[82] Complaint against Facebook Ireland Ltd – 23 "PRISM", http://www.europe-v-facebook.org/prism/facebook
[83] Ibid., Paragraph 29.
[84] [2014] 2 ILRM 401, [2014] IEHC 310, pargraph 84.
[85] Schrems I, paragraph 53.
[86] Ibid., paragraph 70.

equivalent" to that in the EU. Meaning that while the protection mechanisms could be different, they would have to lead to the same result.[87] Analyzing Article 25 (6) of Directive 95/46,[88] the CJEU further explained that the Commission, when examining the level of protection in a third country, must evaluate the "applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules"[89] before making an adequacy decision. As a consequence of the Commission not having made such an analysis before issuing the Safe Harbour Adequacy Decision, the principles were declared invalid and could no longer be used for transfers of personal data from the EU and US.[90]

There were four issues around which the CJEU primarily based its decision to invalidate Safe Harbour. First, it found that the Adequacy Decision was implemented without "sufficient findings" regarding the measures by which the United States ensures an adequate level of protection[91] as required by Article 25 (6) of Directive 95/46, especially since companies could simply claim they were complying with the principles. Second, the CJEU found that in most cases, US law prevailed over Safe Harbour principles[92] and stressed that the Commission had to evaluate its adequacy decisions periodically to ensure that "the level of protection ensured by the third country in question is still factually and legally justified."[93] Third, the CJEU found that the US's data protection level had not been accurately reviewed, as there was no documented reason why the protection in the US should be deemed adequate.[94] The fourth issue that the CJEU discussed was the violations of fundamental rights. It found that the essence of the fundamental right to respect for private life is violated when US law enforcement authorities have "access on a generalized basis to the content of electronic communications."[95]

---

[87] Bräutigam, Tobias. 'The Land of Confusion: International Data Transfers between Schrems and the GDPR'. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 19 December 2016. p.154.
[88] Art. 25 (6) states: 'The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.'
[89] Schrems I, Paragraph 75.
[90] European Parliament. Directorate General for Parliamentary Research Services., From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU US Data Transfer Rules : In Depth Analysis. (LU: Publications Office, 2017), https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf.
[91] Schrems I, Paragraph 83.
[92] Bräutigam, Tobias. 'The Land of Confusion: International Data Transfers between Schrems and the GDPR', p. 154.
[93] Schrems I, Paragraph 76.
[94] Bräutigam, Tobias. 'The Land of Confusion: International Data Transfers between Schrems and the GDPR', p. 154.
[95] Ibid., Paragraph 94.

It also found that since there was no effective remedy for individuals whose personal data was accessed, Article 47 of the Charter of Human Rights was infringed.[96] With its decision, the CJEU decided that the Safe Harbour agreement did not ensure a proper balance of national security and privacy rights in the US, along with insufficient redress mechanisms for EU individuals in cases of personal data breaches.[97]

2.2 Privacy Shield and Schrems II

With the Safe Harbour Privacy Principles invalidation, it was back to the drawing board for Europe and the US to develop a new and improved agreement, as any data transfer under Safe Harbour was now unlawful. While the Safe Harbour adequacy agreement had aimed to balance individuals' privacy with economic concerns, it had instead underlined the differences in the philosophical ideas of privacy between the two. Both sides now sought an agreement that would provide adequate protection while also defending their interests, be it economic or security-related. The Schrems I judgment and the criticism over the years showed that the new agreement needed stronger privacy protections, more robust enforcement mechanisms, and safeguards regarding US authorities' access to individuals' data.[98]

The EU and US, working with a very tight schedule, announced in February of 2016 that they had agreed to replace the Safe Harbour Agreement with one that would comply with the CJEU requirements in the Schrems I decision. The new adequacy agreement had stronger privacy protections, enhanced enforcement mechanisms, restrictions on law enforcement access, and several redress options for EU citizens, including a US Ombudsperson.[99] Following the draft adequacy decision announcement, several organizations and institutions in the EU gave their opinions and analysis. The Article 29 Working Party was especially concerned about data retention periods, continued collection of massive amounts of data, and the Ombudsperson as an effective redress mechanism.[100] Negotiations between the EU and the US continued, and certain sections of the agreement were amended, paving the way for the Member States to approve the final version. The Commission then approved the decision, and the Privacy Shield entered into force in August 2016.[101] Once again, the US had a mechanism under which its

[96] Ibid., Paragraph 95.
[97] Miettinen and Bräutigam, *Data Protection, Privacy and European Regulation in the Digital Age*. p.154.
[98] Bradford, *The Brussels Effect*.
[99] European Commission, Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-US. Privacy Shield https://ec.europa.eu/commission/presscorner/detail/en/IP_16_433
[100] Article 29 Working Party, Opinion 01/2016 on the EU – US. Privacy Shield draft adequacy decision (2016).
[101] European Commission, EU-US. Privacy Shield launched https://ec.europa.eu/commission/presscorner/detail/en/ac_16_3701.

organizations and companies could transfer personal data. Companies began self-certifying, and in more than three years, around five thousand companies participated in the EU-US Privacy Shield framework. In the yearly reviews, the US was praised for ensuring companies' compliance with the principles through monthly checks, the enforcement actions of FTC for numerous cases, and the fact that EU individuals had been using the redress mechanisms and exercising their rights under the Privacy Shield. At the same time, there were complaints concerning companies making false claims of participation in the framework.[102]

Although the new adequacy agreement's principles seemed very similar to those of the Safe Harbour, changes were made regarding the obligations that companies and organizations have.[103] The Notice principle obligates organizations to provide individuals with information regarding the processing of their data, including the intent of their data collection and use.[104] Organizations were also obliged to make their privacy policies public and provide an independent dispute resolution body.[105] Individuals also have the right to opt-out from having their personal data used for different purposes than the original purpose of the data collection or disclosed to a third party under the Choice principle.[106] Regarding the transfers of data to third parties, the Onward Transfers principle states that these transfers between the companies and third-party data controllers can only happen if parties enter into a contract that requires the data to be processed for limited and specific purposes.[107] Third parties should, irrespective of their location, provide the same level of protection as guaranteed by the principles.[108] Individuals also enjoy the right of access to their personal information that an organization holds. The Access principle gives data subjects the right to verify the accuracy of the information held about them and to be able to correct, delete or amend that information without having to justify their reason.[109] According to the Data Integrity and Purpose Limitation Principle, personal information must be limited only to what is relevant for processing.[110] The organization that controls the data must ensure that the data is accurate, current, and complete. It also states that data cannot be retained for longer than what is necessary to fulfill the purposes

[102] EU-US. Privacy Shield: Third review welcomes progress while identifying steps for improvement, October 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134.
[103] European Parliament. Directorate General for Parliamentary Research Services., *From Safe Harbour to Privacy Shield*, p. 22.
[104] Privacy Shield, Art. 20.
[105] Ibid., Art. 45.
[106] Ibid., Art. 22.
[107] Ibid., Art. 28.
[108] Ibid.
[109] Ibid., Art. 25.
[110] Ibid., Art. 21.

for which it was collected.[111] Like Safe Harbour, the Privacy Shield relied on a system of certification. Organizations went through annual self-certifications to show the US Department of Commerce their compliance with the privacy requirements.[112]

Several redress options for EU citizens are listed in the Privacy Shield, including filing claims directly with the US self-certified company,[113] through a national DPA,[114] and with the US Department of Commerce,[115] among others, when national authorities access one's personal data in the US. However, they were still seen as very restrictive,[116] as the main issue was the ability for EU individuals to prove standing in surveillance cases. One example is the FISA Act, under which non-US citizens can challenge illegal electronic surveillance. While there are many claims that an individual can bring, the possibility of redress is minimal as EU citizens would have to prove the existence of damage or the government's attempt to use or disclose their personal data in administrative or judicial proceedings.[117] Even more complicated are cases of classified information, as it would be unlikely for an individual to be informed that they have been part of a surveillance investigation.[118] Because of these limitations, the Privacy Shield also created an Ombudsperson Mechanism in the US to deal with individual complaints regarding activities of US intelligence agencies.[119] Being independent of intelligence agencies,[120] the Ombudsperson reports directly to the US Secretary of State and works with the DPAs of Member States who submit the complaints of EU citizens.[121] After receiving a complaint, the Ombudsperson is required to confirm the request's investigation, followed by checking if US law was complied with, and if it has not, then the violation has to be remedied. However, the Ombudsperson, in its response, does not disclose if an individual has been the target of surveillance by US national intelligence services[122] or the nature of the remedy that was applied.[123]

---

[111] European Parliament. Directorate General for Parliamentary Research Services., *The Privacy Shield*, p. 14.
[112] Privacy Shield, Paragraph 14.
[113] Ibid. Paragraph 43.
[114] Ibid. Paragraph 48.
[115] Ibid. Paragraph 52.
[116] Linebaugh, Chris D, and Edward C Liu. 'EU Data Transfer Requirements and U.S. Intelligence Laws', p. 6.
[117] Ibid., p. 1.
[118] Anna-Laure Philouze, 'The EU-US Privacy Shield: Has Trust Been Restored?', *European Data Protection Law Review* 3, no. 4 (2017): 463–72.
[119] Privacy Shield, Paragraph 116.
[120] Ibid., Paragraph 121.
[121] Ibid., Paragraph 119.
[122] EU Commission, Guide to the EU-US. Privacy Shield, https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf.
[123]Privacy Shield, Annex III, 4 (e).

The Privacy Shield framework was met with mixed but, for the most part, negative reactions in the EU. Activists argued the negotiated agreement was, on the whole, the same as the Safe Harbour and that because the agreement did not change the practices of US intelligence agencies in any way, fundamental violations of rights would persist.[124] The principles were also seen as lacking legal effect and designed to let the companies off the hook too easily.[125] On the contrary, EU and US officials maintained that the new framework included greater privacy protections and mechanisms for oversight and redress and new safeguards concerning US intelligence services surveillance access to personal data.[126]

While the Privacy Shield was negotiated and approved, Max Schrems reformulated his complaint due to the invalidation of the Safe Harbour agreement by the Schrems I judgment, and after Facebook Ireland had clarified that they were using SCCs to transfer data to the Facebook US. In his complaint to the DPA, Schrems claimed that using the SCC Decision could not justify transferring personal data from the EU to the US as the US surveillance programs did not allow for sufficient protection of EU individuals' personal data.[127] Schrems also claimed that the Privacy Shield mechanism did not provide an adequate level of protection for the personal data of EU individuals in the US. The Irish DPC brought the proceedings before the High Court, which asked the CJEU if data transfers under the SCCs violate the EU Charter of Fundamental Rights[128], the level of protection provided for transfers under the SCCs, and if there were adequate safeguards under SCCs. Lastly, it asked if the Privacy Shield ensures an adequate level of protection under Article 45 of the GDPR.[129]

On 16 July 2020, the CJEU in the Schrems II decision ruled that the Privacy Shield framework was invalid, making it the second adequacy decision that the CJEU had brought down but upheld the validity of the SCCs as an export mechanism for the transfer of personal data to third countries. Regarding the Privacy Shield, the CJEU discussed two main issues which were determinantal in invalidating the data transfer mechanism. The CJEU expressed its doubts about whether US law granted an adequate level of protection as required by EU law, precisely because it did not believe that US laws provided the necessary limitations and

[124] Miettinen and Bräutigam, *Data Protection, Privacy and European Regulation in the Digital Age*, p.25
[125] Ibid.
[126] Weiss and Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield'.
[127] Schems II, Paragraphs 50-57.
[128] Ibid., Paragraph 68.
[129] Christopher Kuner, 'The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation', *European Law Blog* (blog), 17 July 2020, https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/.

safeguards against the access of national surveillance practices.[130] In examining Section 702 of the FISA and Executive Order 12333 of the US, the CJEU found that US surveillance programs were not limited to only what is strictly necessary, resulting in interference of protecting the personal data of EU subjects.[131] US surveillance practices on personal data transferred to the US from the EU showed that the requirements under EU law to provide essentially equivalent protection were not fulfilled.[132]

The CJEU also found no effective judicial protection against the interferences of US surveillance programs and declared that the Ombudsperson mechanism was insufficient in remedying this lack of redress.[133] The Ombudsperson, according to the CJEU, does not have the power to adopt decisions that are binding on the intelligence services of the US,[134] nor can it be considered independent from the intelligence community since it has to report directly to the Secretary of State.[135] Therefore, the Ombudsperson was not a sufficient redress mechanism as it restricted the right to effective judicial protection afforded to EU subjects by EU law.[136]

Regarding the SCC Decision, the CJEU did not find anything that would affect the decision's validity and affirmed its use as a transfer mechanism.[137] However, the CJEU clarified that routine reliance on SCCs to legitimize cross-border data transfers without understanding the level of protection in the third country where the transfer will occur does not suffice any longer. SCCs are binding only on the controllers from the EU and recipients in the third countries and do not bind the authorities of that country.[138] To avoid situations in third countries that do not guarantee the same level of protection as that in the EU and where public authorities can interfere in the rights of data subjects, data controllers who wish to transfer data based on SCCs shall ensure that laws in third countries where they intend to transfer data ensure adequate protection, as that afforded under EU law.[139] This means that companies will have to verify on a case-by-case basis whether the laws of the third country they want to transfer data to ensure

[130] Schrems II, paragraph 168.
[131] Ibid., Paragraph 184.
[132] Ibid., Paragraph 185.
[133] Ibid., Paragraph 168.
[134] Ibid., Paragraph 196.
[135] Ibid., Paragraph 195.
[136] Hendrik Mildebrath, 'The CJEU Judgment in the Schrems II Case', At a Glance (European Parliamentary Research Service, 2020), https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.
[137] Schrems II, paragraph 149.
[138] Ibid., Paragraph 125.
[139] Ibid., Paragraph 105.

adequate protection.[140] If not, they need to adopt additional measures to ensure compliance.[141] Companies unable to provide adequate protection through additional measures are required to suspend transfers. If they fail to do so, the EU data protection authorities must suspend or prohibit transfers where the SCC cannot be complied with.[142]

The CJEU, besides confirming the validity of the SCCs in Schrems II, which seems to be the mechanism that will be most used for data transfers, also suggested using Article 49 of GDPR, known as "derogations" for transfers of data.[143] The EDPB, however, has underlined the fact that these mechanisms apply only in certain situations, which are usually processing activities that are non-repetitive and occasional.[144] Another idea that has resurfaced post-Schrems II is that of data localization. There have been concerns about Schrems II making data transfers risky for companies and organizations to the point where they are almost pressured to localize their data to avoid legal issues.[145]

2.3 SCC's and BCR's

The Schrems decision has indeed affirmed the validity of the SCCs, but it has also brought upon companies' new obligations and uncertainties. Around 88 percent of EU companies rely on SCCs to transfer data outside of the EU. With the decision of the CJEU, the pressure will fall on these companies to evaluate the level of protection in third countries they wish to transfer to.[146] The requirement for SCCs to be used for transfers in third countries whose national laws do not offer an adequate level of protection only if controllers adopt "additional safeguards" or "supplementary measures" for the protection of the data transferred places a cumbersome burden on data exporters wishing to use this transfer mechanism. They are now responsible for considering the laws and practices of the countries they plan to transfer data to, especially in cases with risks of access to data by public authorities.

BCRs are also a transfer mechanism that organizations and companies can use. Post-Schrems II, for BCRs to be used, risk assessments followed by supplemental measures are needed to satisfy the requirements of the decision. Organizations must show the

[140] Ibid., Paragraph 134.
[141] Ibid., Paragraph 133.
[142] Ibid., Paragraph 135.
[143] Ibid., Paragraph 202.
[144] Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf, p. 3,4.
[145] Anupam Chander, 'Is Data Localization a Solution for Schrems II?', *SSRN Electronic Journal*, 2020.
[146] Genna Churches and Monika Zalnieriute, 'A GROUNDHOG DAY IN BRUSSELS: SCHREMS II AND INTERNATIONAL DATA TRANSFERS', 2020, 8.

implementation of the supplemental measures across the corporate group along with all its entities.[147] Following the Schrems II decision, the EDPB published its first response in the form of "FAQs"[148] to clarify and give companies preliminary guidance regarding the use of legal instruments for personal data transfers to third countries, including the US. The EDPB said they would analyze what the ruling entailed for the SCC and other mechanisms and identify the supplementary measures a company could take to continue data transfers. The EDPB issued two documents with recommendations in November of 2020, the first being recommendations on supplementary measures[149] and another with the Essential Guarantees for surveillance measures.[150]

The EDPB recommendations for supplementary measures provide companies with a six-step plan on assessing and protecting data transfers in light of the Schrems II judgment. The document provides examples of contractual, technical, and organizational measures that it considers acceptable for data transfers and scenarios where data transfers should be terminated.[151] Setting out scenarios of cases, the EDPB explains the safeguards that can be used for various data transfers. For the technical safeguards, it recommends using encryption along with pseudonymization and split or multi-party processing. It also gives examples of two cases where no effective measures were found to ensure an essentially equivalent level of protection, such as unencrypted processing and remote data access for business purposes.[152] Scenarios provided by the EDPB show the rejection of risk-based approach[153] and the fact that data transfers to third countries that do not offer an adequate level of protection are allowed only if the data is pseudonymized or encrypted in such a way that no one in the receiving country can read it; not even those who receive the data. The other issue that arises from the EDPB

[147] Bojana Bellamy, Markus Heyder, and Nathalie Laneret, 'A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision' (Centre for Information Policy Leadership (CIPL), September 2020).
[148] European Data Protection Board, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.
[149] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Annex 2.
https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf
[150] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures
edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf (europa.eu)
[151] European Data Protection Board, 41st Plenary session: EDPB adopts recommendations on supplementary measures following Schrems II, https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_en
[152] Recommendations 01/2020 on measure., Annex 2.
[153] CCIA, 'CCIA Comments on Draft EDPB Recommendations on Supplementary Measures', 2020.
https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/12-21-2020_-_ccia_response_to_the_edpb_on_schrems_ii_guidelines.pdf.

recommendations is that organizations, especially smaller ones, might not have the means to employ the technical measures it recommends.

The EEG Recommendations, based on the law and jurisprudence of the EU, aim to help organizations assess whether surveillance measures of third countries are compatible with EU law. The recommendations follow the GDPR and state that a third country's data protection laws need not be identical to those of the EU, allowing for different ways of assessing foreign surveillance laws. They also stipulate that the 'equivalent protection' test is failed by countries that do not meet the document's requirements. The CJEU already found in its decision that the US does not provide essentially equivalent protection. Given that SCCs do not bind public authorities in third countries, it seems that no data can be transferred in a lawful way to the US from the EU.[154] BCRs are not explicitly mentioned in the Schrems II ruling. However, the EDPB has included them in their recommendation, stating they are to go through the same re-assessments as organizations and companies that use SCCs.

2.4 Data localization

Another area that has gained much traction since the Schrems II judgment is 'data localization' and the idea that European individuals' data should be stored and processed in Europe only.[155] Many countries worldwide have chosen to adopt legal or administrative requirements preventing data from being transferred to third countries based on legitimate concerns of unlawful access of foreign surveillance agencies, and there have been calls in the EU too for such measures.[156] Data localization measures were pushed by the Snowden leaks, giving momentum to data localization laws worldwide to protect the privacy of individuals and governmental data.[157] Nevertheless, the European approach for protecting personal data has never been that data should not be transferred to other countries but that it should always travel with protections.[158]

---

[154] Theodore Christakis, '"Schrems III"? First Thoughts on the EDPB Post-Schrems II Recommendations on International Data Transfers (Part 1)', *European Law Blog*, 13 November 2020, https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/.

[155] Theodore Christakis, *'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy* (Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute, 2020).

[156] Dan Svantesson, 'Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines', OECD Digital Economy Papers, vol. 301, OECD Digital Economy Papers, 22 December 2020.

[157] Laura K Donohue, 'High Technology, Consumer Privacy, and U.S. National Security', 2015, 29.

[158] Christakis, '"European Digital Sovereignty"', p. 68.

The Schrems II judgment and the EDPB recommendations have, without a doubt, complicated matters of cross-border transfers, so it was only natural for calls to be made once again in favor of data localization. High officials in the EU, such as the Commissioner for the Internal Market, have claimed that Europeans should demand that their data be stored, processed, and handled in Europe for years.[159] One day after the Schrems II decision, a call came from the Berlin DPA, who asked Berlin-based data controllers that store personal data in the US to transfer that data to the EU.[160] In October of 2020, leaked documents from the Commission's Data Governance Act showed a list with requirements for the providers of data sharing services to be located in the EU or an EEA country.[161] Although, after much criticism in the bloc, the requirement was removed from the final version of the regulation.[162] Reading the EDPB recommendations, it might seem that data localization is one of the few options left. While it might help some isolated cases, such as organizations and companies for whom personal data transfers are not a necessity but a convenience, data localization cannot be a broad-scale solution.[163] In theory, data localization is an excellent solution to personal data privacy. However, the reality is that it also has an abundance of adverse effects, such as protectionism, cybersecurity risks, economic costs, and even potential human rights implications.[164]

But is data localization the answer to restrict foreign surveillance on Europeans? Data stored in the EU does not prevent US surveillance agencies from being able to access it. Through Section 702 of FISA, the NSA for foreign intelligence matters has the authorization to collect foreigner's communication.[165] The NSA's senior officials have revealed that more than a hundred thousand foreign nationals were under the NSA's surveillance, showing the

[159] Thierry Breton: «C'est aux Gafa de s'adapter à nos règles, pas l'inverse» https://www.lefigaro.fr/secteur/high-tech/2018/04/06/32001-20180406ARTFIG00280-thierry-breton-c-est-aux-gafa-de-s-adapter-a-nos-regles-pas-l-inverse.php. Translation by DeepL.
[160] Nach „Schrems II“: Europa braucht digitale Eigenständigkeit https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf translation by DeepL
[161] Samuel Stolton, ‘Data Sharing Services Must Be “established in the EU,” Leaked Regulation Reveals’, w*ww.Euractiv.Com*, 30 October 2020, https://www.euractiv.com/section/digital/news/data-sharing-services-must-be-established-in-the-eu-leaked-regulation-reveals/.
[162] Samuel Stolton, ‘New EU Data Brokers Won’t Have to Be European, Commission Says’, w*ww.Euractiv.Com*, 26 November 2020, https://www.euractiv.com/section/digital/news/new-eu-data-brokers-wont-have-to-be-european-commission-says/.
[163] Thomas Streinz, ‘The Evolution of European Data Law’, in *The Evolution of EU Law*, 3rd ed. (Oxford, New York: Oxford University Press, 2021).
[164] Chander, ‘Is Data Localization a Solution for Schrems II?’, p. 13.
[165] Linebaugh, Chris D, and Edward C Liu. ‘EU Data Transfer Requirements and U.S. Intelligence Laws’.

extent of the US's foreign operations.[166] US intelligence services do not even have to be in the country where they are conducting surveillance using, among others, malware for information collection. EU intelligence services are also no strangers to these activities, having shared and received data from the US and other third countries. The leaks have shown strong evidence for this exchange of data between intelligence agencies in many countries, making the location where data is stored irrelevant to the fact that it might be accessed and shared by foreign intelligence services.[167]

3. A path forward?

3.1 The difficult task of balancing national security with privacy

National security has for quite some time been used by countries and their security agencies as a means to justify the potential limits of our rights.[168] It is not to say that the security exception that limits the protection of human rights is illegitimate; there are indeed times when these limitations are lawful and necessary for protecting the state and its citizens.[169] The evolution of technology and its sophistication has made it possible for surveillance to expand significantly, leading to the collection of personal data by national security agencies, among other intrusions to our privacy.[170] The potential for abuse of the national security exemption has highlighted the need for a balance between surveillance and privacy protection, including more stringent transparency requirements and greater oversight of intelligence activities. There have been many calls for legal reforms and policy changes around the world to control and create oversight mechanisms for surveillance practices.[171] At the same time, countries have continued to engage in surveillance programs that have allowed them to continue surveillance

[166] Jim Sciutto and Zachary Cohen, 'NSA Reveals 100,000 Foreign Nationals under Surveillance', *CNNPolitics*, 25 September 2017, https://edition.cnn.com/2017/09/25/politics/fisa-section-702-surveillance-nsa/.
[167] Anupam Chander and Uyên P. Lê, 'Data Nationalism', *EMORY LAW JOURNAL* 64 (2015): 64.
[168] 'National Secutiry and European Case Law' (Council of Europe/European Court of Human Rights, 2013), https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf.
[169] 'Recommendations on the Protection of Fundamental Rights in the Context of National Security' (CCBE, 2019), https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf.
[170] Michelle Cayford and Wolter Pieters, 'The Effectiveness of Surveillance Technology: What Intelligence Officials Are Saying', *The Information Society* 34, no. 2 (15 March 2018): 88–103, p. 97.
[171] European Union Agency for Fundamental Rights., *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II, Field Perspectives and Legal Update.* (LU: Publications Office, 2017).

in their countries and abroad legally.[172] It is not possible to argue that one is more important, national security or human rights. National security might be a legitimate means of limiting one's privacy, but at the same time, laws should be adopted with certain principles to ensure that invasions to the right of privacy are as limited as possible.[173] The position of the ECtHR, which has delivered a variety of surveillance-related cases, has been very consistent that while in the fight against terrorism, surveillance measures can be crucial, the risk exists of democracy being undermined by this surveillance. When deciding if surveillance of individuals is justified under Article 8 of the ECHR,[174] the Court has looked at three criteria. First, it asks that legitimate aims justify the surveillance. Second, it requires surveillance to be necessary for legitimate aims to be achieved, making a necessity and proportionality test crucial. The third criteria requires the surveillance to be based on domestic laws which meet specific minimum standards.[175] While this criteria test has helped the Court decide on many surveillance cases until now, the ever-expanding and sophistication of technology is bound to bring even more sophisticated surveillance practices and a new generation of issues and court cases.

Another side of the privacy versus national security issue is that states do not carry out surveillance only within their borders; surveillance is indeed international. The ease and quantity at which data moves across borders show the tension between data transfers' international and local aspects. Attacks such as September 11 have drastically changed countries' approaches in how privacy is treated when it comes to national security matters.[176] Moreover, the issues upon which Schrems II was decided show the need for a global approach to safeguard the right to privacy when large-scale surveillance is conducted in the name of national security. Data transfers present a somewhat more complicated matter, as both sides require different policy goals to fulfill their requirements. To assure more robust privacy, the EU requirements for data to be transferred to third countries only if they offer the same

[172] The US has different laws for conducting foreign surveillance, such as Section 702 of FISA Act and Section 215 of the PATRIOT ACT. Various EU Member States, such as Germany, UK, Sweden and France have also been revealed to have cooperated with the US in mass surveillance operations. See footnote 84.
[173] UN Office of the High Commissioner for Human Rights (OHCHR), Fact Sheet No. 32, Human Rights, Terrorism and Counter-terrorism, July 2008, No. 32, p. 49.
https://ohchr.org/Documents/Publications/Factsheet32EN.pdf
[174] Article 8 (2) of ECHR says: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'
[175] Christakis Théodore and Bouslimani Katia, 'Part III Security Governance Tools, Ch.38 National Security, Surveillance, and Human Rights', in *The Oxford Handbook of the International Law of Global Security*, by Christakis Théodore and Bouslimani Katia (Oxford University Press, 2021).
[176] A. James McAdams, 'Internet Surveillance after September 11: Is the United States Becoming Great Britain?', ed. Cynthia Brown et al., *Comparative Politics* 37, no. 4 (2005): 479–98.

standards for privacy as the EU is in contrast to what drives surveillance - the free flow of data.[177] Why should we restrict the fundamental right to privacy and data protection to the residence or nationality of a person when states do not face any restrictions when it comes to the surveillance of another country's nationals? These shortcomings in both the national and international legal sphere open up the possibility of a new international agreement to protect personal data. There is no international human rights treaty that mentions the need for data protection explicitly at the moment. While there might be obstacles such as the nature and development of technology, having an international framework would mean having a clear set of standards for data protection would help countries uphold the right of privacy while also catering to national security requirements.[178]

3.2 Evaluating data surveillance practices of EU Member States

It is no surprise that surveillance programs exist in member states of the EU, but reports that emerged after the Snowden leaks uncovered the true extent of the member states' data surveillance practices. At the time, the UK, still a member of the EU, cooperated with the NSA and had surveilled EU member states' embassies and EU institutions as a part of UK-US surveillance activities. In addition, Germany, France, and Sweden were also developing or already running their internet interception programs and exchanging data with the NSA.[179] There has been much discussion about the US's surveillance practices, but it seems that those of the EU member states are off-limits. Schrems I and Schrems II have shown the disconnect between the international impact of the GDPR and its application on the EU member states' national security agencies. While the GDPR and EU law offers an exception to the EU member states to balance the right to privacy with national security requirements,[180] the same right is not extended to third countries' intelligence services. The CJEU, with the Schrems decisions, has put itself in the position to judge the way third countries access data for national security purposes and has made requirements for third countries' national security agencies while unable to do so for the national security agencies of the member states, until recently.[181]

---

[177] Joshua P Meltzer, 'After Schrems II: The Need for a US-EU Agreement Balancing Privacy and National Security Goals', *Global Privacy Law Review* 2, no. 1 (2021): 83–89.
[178] Kristian P. Humble, 'International Law, Surveillance and the Protection of Privacy', *The International Journal of Human Rights* 25, no. 1 (2 January 2021): 1–25.
[179] European Parliament. Directorate General for Internal Policies of the Union., *National Programmes for Mass Surveillance of Personal Data in EU MS and Their Compatibility with EU Law.* (LU: Publications Office, 2013).
[180] Art. 4 of Treaty of Lisbon, 2007/C 306/01.
[181] Václav Stehlík and Lusine Vardanyan, 'Schrems II: Will It Really Increase the Level of Privacy Protection against Mass Surveillance?', *Bratislava Law Review* 4, no. 2 (31 December 2020): 111–28.

The CJEU issued its first rulings, in the fall of 2020, to the limitations of EU fundamental rights on data collection and retention programs of member states' intelligence services. The CJEU dealt with whether activities of security agencies of Member States fall under EU law jurisdiction.[182] It also dealt with whether national legislation obligating electronic communication service providers to disclose the traffic and location data of users to public authorities along with general and indiscriminate retention of such data for national security matters and crime prevention is lawful.[183] The CJEU, in its decision, said that national intelligence services could not override EU data protection and privacy laws for the purposes of regular bulk data collection.[184] Cases when member states intelligence agencies put obligations on electronic communication services to collect, transfer and retain data for their use, the CJEU said, fell within the scope of EU law.[185] In contrast, the CJEU decided that in cases when intelligence agencies do not impose obligations on communication services but instead process the data themselves, their activities fall under the jurisdiction of their national laws instead of EU law.[186] For the general and indiscriminate retention of data for national security, the Court recognized the right of intelligence services to do so when justified by serious national security threats.[187] While such cases are a step towards slowly extending the reach of EU law to the national security realm of the member states, a proposal by France accepted for the new Privacy Regulation threatens to undo both judgments and leave processing activities and operations related to national security or defence, whether private operators or public authorities conduct them, out of the scope of EU law. If this broad national security exception is accepted, member states will be able to conduct data collection and retention without any obstacles.[188] If this ends up being the reality, the EU risks creating a double standard on data protection and surveillance standards for its member states and third countries. The GDPR asks third countries to provide 'essentially equivalent' protection to data as that offered under EU law. However, if member states continue to partake in such surveillance and

[182] Ibid.
[183] Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier ministre and Others, ECLI:EU:C:2020:791, paragraph 68.
[184] Case C-623/17, The Investigatory Powers Tribunal (United Kingdom), in the proceedings Privacy International Case, ECLI:EU:C:2020:790; Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier ministre and Others, ECLI:EU:C:2020:791.
[185] Ibid, Paragraph 94-97, 101
[186] Cases C-511/18, C-512/18 and C-520/18, Paragraph 103.
[187] Ibid., Paragraph. 141.
[188] Christakis Théodore and Kenneth Propp, 'How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States', *Lawfare*, 8 March 2021, https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states.

get away with it, third countries might see it as unfair to follow the EU law requirements when they are not afforded the same exceptions.[189]

The US has already brought forward an argument based on the Court's differentiation on direct and indirect access to data. Hoping to change the course of the new adequacy decision, the US argues that since direct access of EU member states to personal data is not subject to EU law, "a data exporter would have no comparative standard by which to assess whether privacy protections offered by a destination country for the same type of activities are "essentially equivalent" to protections required by EU law."[190] However, this argument fails to look at the fact that regardless of the "national security exemption of member states from the scope of EU law, the ECHR articles that cover privacy continue to apply to member states' surveillance laws. The ECHR is still binding on all member states even though the EU has not acceded to it. Moreover, the ECtHR does not give much importance to whether there has been direct or indirect access to data in its surveillance decisions.[191] The question remains, how effective is the ECHR in removing the doubt of there being a double standard for non-EU member states. Although all member states of the EU are parties to the ECHR, there is always the chance that their laws will not necessarily comply with the standards that the ECHR and ECtHR case law have developed. Besides the fact that Member states might not respect the treaty, when a case is taken to the ECtHR, it can take years for a decision to be reached, and we can never be sure that member states will respect those decisions.[192]

3.3 Schrems II implications for past and future adequacy decisions

With the Privacy Shield invalidated, twelve countries remain recognized by the European Commission as providing adequate protection.[193] The Schrems II decision has underlined the weaknesses of the data transfer mechanisms under the GDPR, and the protections offered by existing adequacy agreements could very well be called into question.

---

[189] Vincent Manancourt, 'EU to US on Surveillance: Do as I Say, Not as I Do', *POLITICO*, 17 March 2021, https://www.politico.eu/article/eu-to-us-surveillance-data-flows/.
[190] COMMENTS ON PROPOSED EDPB RECOMMENDATIONS 01/2020, P.9, https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/2020.12.21_-_us_comments_on_edpb_supp_measures_final.pdf.
[191] Theodore Christakis, 'Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 1)', *European Law Blog*, 12 April 2021, https://europeanlawblog.eu/2021/04/12/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part1/.
[192] Christakis Théodore, 'Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2)', *European Law Blog*, 13 April 2021, https://europeanlawblog.eu/2021/04/13/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part2/.
[193] See footnote 29.

The EU Commission considers the diplomatic relations and the impact that the termination of transatlantic data transfers will have on trade and investment when assessing laws and practices of third countries to determine their adequacy under the GDPR. This is not the case for DPA's of member states and the CJEU, who, if the question arises, are only concerned with whether these third countries provide the same level of protection as required by EU laws and the ECHR. It is these differences that render the existing adequacy decisions vulnerable to being invalidated by the CJEU.[194]

After Schrems I, the European Commission decided that for countries with adequacy decisions it would "on an ongoing basis, monitor developments, both in law and in practice, that could affect the functioning of such decisions, including developments concerning access to personal data by public authorities."[195] Many countries with adequacy decisions have gone through these periodic reviews, and future reviews will be defined by the standards that Schrems II has set. Countries with adequacy decisions that share personal data information with the US, such as the Five-Eyes Collective, which New Zealand is part of, will likely have this issue and other requirements arise from Schrems II - especially if they provide only limited redress rights - as part of future reviews, although the CJEU has not directly addressed this. It seems, however, that as long as essentially equivalent protection and the right of redress for individuals is provided, third countries will be able to retain their adequacy agreements.[196]

Besides assessing the adequacy of South Korea, over the past months, the EU Commission has also assessed the laws and practices regarding personal data protection for the UK since it is no longer part of the EU. For years, the UK's surveillance practices have been considered more invasive than the surveillance practices of other Member States.[197] The EU Commission issued a draft adequacy decision which the EDPB then examined. In their opinion, the EDPB said the UK should be granted an adequacy decision noting the key areas of "strong alignment between the EU and the UK data protection frameworks."[198] Indeed, the impact of

[194] Joshua P. Meltzer, 'The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security', *Brookings*, 5 August 2020, https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/.
[195] Commission Implementing Decision (EU) 2016/2295 of 16 December 2016.
[196] Mark Smith, 'ANALYSIS: Will Schrems II Cause Five Eyes to Blink?'. *Bloomberg Law*, 16 November 2020. https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-will-schrems-ii-cause-five-eyes-to-blink.
[197] Didier Bigo et al., *Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law* (CEPS, 2013), p. 39.
[198] Opinions on draft UK adequacy decisions, Guidelines on the application of Article 65(1)(a) GDPR, Guidelines on the targeting of social media users and Statement on international agreements including transfers, p. 5, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf

Schrems II is seen in the opinion, with the case mentioned throughout the document various times. EDPB's opinion on the UK draft adequacy decision mentions issues that require the EU Commissions' greater assessment, such as onward transfers, that the EDPB identifies as potentially undermining the level of protection of personal data transferred from the EU/EEA.[199] Referring to Article 44 of the GDPR, the opinion reiterates the fact that it is not enough for the UK's legislation to be "essentially equivalent" to that of the EU and that rules of the UK "shall ensure that an essentially equivalent level of protection will continue to be provided" for onward transfers of personal data to third countries.[200]

International agreements between the UK and third countries are also discussed in the opinion. The EDPB has invited the EU Commission to investigate UK's international commitments, including those towards the US, to monitor and take action in the chance of the protection of personal data of the EU individuals being undermined by these agreements, including intelligence sharing ones. It also calls for a deeper examination of the safeguards that UK law provides when dealing with national security exemptions leading to the overseas disclosure of personal data to ensure that the rights of individuals and core safeguard are not circumvented.[201] Suppose the EU Commission gets the approval of the member states and adopts a final decision regarding the adequacy decision without addressing some of the shortcomings pointed out until now. In that case, there is a good chance of the adequacy decision having the same fate as the Privacy Shield and its predecessor and ends up invalidated.

3.4 How do we go forward? A new agreement?

The Privacy Shield invalidation has again brought the EU and US together to negotiate a new adequacy decision. Discussions between the European Commission and the US Department of Commerce kicked off in August 2020 to "evaluate the potential for an enhanced EU-US Privacy Shield framework to comply with the judgment of the Court in the Schrems II case."[202] With negotiations intensifying, both sides have recognized the transatlantic data flows importance and expressed their commitment to data protection, privacy, and the rule of law.[203]

[199] Ibid., p. 6.
[200] Ibid.
[201] Opinions on draft UK adequacy decisions, Paragraphs 15, 18, 33 and 34.
[202] Joint Press Statement from European Commissioner for Justice Didier Reynders and US. Secretary of Commerce Wilbur Ross https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en
[203] Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and US. Secretary of Commerce Gina Raimondo https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443

The Snowden leaks and the Schrems judgments have shown the necessity for US surveillance laws to be changed, starting by defining the limitations on bulk data collection, especially for foreign nationals, and extending judicial protection to non-US individuals. An issue to consider would be changing Section 702 of FISA and EO 12333 in order for data flows to continue without any obstacles.[204] The US has not shown any willingness on this matter, saying that an overhaul of surveillance powers is impossible in the short term.[205] Negotiating a third agreement along the same line as the previous ones with minor changes is no longer an option for the EU Commission, especially if the EU wants to maintain its position as a global regulator in the realm of data protection. While there are many uncertainties about what this new agreement will entail, one thing is certain: both sides should work to negotiate a comprehensive agreement that does not risk being shot down by the CJEU for a third time. The issues leading to the invalidation of the Privacy Shield were, for the most part, the same as those which had invalidated the Safe Harbour mechanism. Throughout negotiations for both adequacy agreements, many have argued that the Safe Harbour and Privacy Shield's invalidation shows that an internal document of the EU Commission does not provide a sufficient level of privacy and data protection. The EU and US could go another route and conclude a binding international agreement such as a treaty on cross-border transfers and protecting personal data from governmental surveillance. The issue with this option is that negotiations of past agreements between the US and EU have proven to be challenging and time-consuming, and there is a risk that a new treaty will be the same way. This treaty would also bring lengthy modifications of US law at a time when companies have been left with the burden of assessing the laws of the US for compliance along with challenging and costly safety measures.[206]

Still, it is not only up to the US to make changes to achieve the data protection that the EU requires. There are also some areas in which the EU can improve, starting with ensuring member states' compliance with CJEU decisions for data retention/collection. For the GDPR to be respected both at home and internationally, the EU should find a way to ensure the compliance of member states and their national security agencies with the data protection laws

[204] Barker Tyson, 'Breaking the Transatlantic Data Trilemma: The EU Must Step Up Its Approach to EU-US Data Flows', *Forschungsinstitut Der Deutschen Gesellschaft Für Auswärtige Politik e.V.*, DGAP Policy Brief, no. 27 (2020): 10.
[205] EU's rejection of US surveillance also tests its commitment to privacy https://www.politico.eu/article/rejection-of-us-surveillance-tests-eu-mettle-on-privacy-shield/
[206] Theodore Christakis and Fabien Terpan, 'EU–US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options', *International Data Privacy Law*, 12 February 2021.

of the EU. The data retention/collection decisions are a step in the right direction to enforce the limitations to the national security "exemption" as they contribute to dismissing the "double standards" the EU is said to apply.[207] The affirmation that the EU applies the same protection standards within the Union and to third countries could create a set of standards by the EU and US for activities of national security agencies and their access to personal data.[208] This international set of principles brings forth the question of what standards could the EU and the US agree on. The EEG Recommendations by EDPB provide a combination of ECtHR and CJEU case-law to set the "standards to be followed" by the US.[209] Although the US needs to comply with these standards to continue data transfers,[210] there have been cases where the countries that are parties to the Convention themselves have not followed them.[211] Both parties will have to decide if the ECHR and the standards ECtHR case law has created apply to the international surveillance activities of the US. If it is decided that the ECHR indeed applies to the international surveillance practices of the US, the EU, and the US would have to decide on the practices, safeguards, and standards that would govern their agreement.[212] If this is not the case, the EU and the US would have to find a solution for adequate safeguards that would satisfy EU data protection laws for future data transfers between the two in addition to the safeguards given by the recommendations of EDPB.[213]

Another way to create a long-term agreement without any major changes to the US surveillance laws is to have an agreement that addresses the issues that brought down the Privacy Shield: the necessity and proportionality of US surveillance practices and the lack of individual redress for EU individuals.[214] The Ombudsperson mechanism, already designated as not independent and impartial,[215] can no longer be used for a new agreement in the same format. For the judicial redress requirement, the US needs to present a credible mechanism

[207] Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II, White Paper, U.S. Department of Commerce, U.S. Department of Justice, Office of the Director of National Intelligence (Sept. 2020), https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.
[208] Théodore, 'Squaring the Circle?' (Part 1).
[209] Recommendations 02/2020 on the European Essential Guarantees., Paragraph 11.
[210] Ibid., Paragraph 52.
[211] 'Table of cases and groups of cases under enhanced supervision' by the Committee of Ministers shows that there are cases when parties to the Convention have not executed or are having issues executing decisions by the ECtHR, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a1c7f2.
[212] Ira Rubinstein and Peter Margulies, 'Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground', *SSRN Electronic Journal*, 2021, p.35.
[213] Théodore, 'Squaring the Circle?' (Part 1).
[214] Christopher Docksey, 'Schrems II and Individual Redress—Where There's a Will, There's a Way', Lawfare, 12 October 2020, https://www.lawfareblog.com/schrems-ii-and-individual-redress-where-theres-will-theres-way.
[215] Schrems II, Paragraph 195.

with the ability to conduct credible inquiries – independent oversight - into the activities of surveillance agencies and the opportunity of a claim before an independent judicial body[216] in the case that rights have been violated. For the effective redress mechanism, the US could transfer the duty of an effective and independent factual inquiry to an existing mechanism under US surveillance law. This existing mechanism, to satisfy the requirements of the GDPR, would ideally have the responsibilities that data protection officers have along with the jurisdiction of expert bodies that are tasked with supervising the activities of the intelligence communities in EU member states.[217] Giving the task to undergo this fact-checking to an existing mechanism under US surveillance law would also require creating standards for the investigation procedure, which would benefit both US and EU individuals.[218] The CJEU in Schrems II brought up the possible inability of an EU individual to prove standing before a US court and seek remedy.[219] There is also the issue of the Ombudsperson not disclosing whether an individual has been subject to surveillance by US national intelligence services.[220] The US could try to rectify this issue by creating a means for EU individuals to bring complaints before a court,[221] and then following the independent factual inquiry with an answer to the complaining party of whether no US surveillance law has been violated or if there has been any violation, that it has been corrected.[222] Having an independent mechanism report this final decision without disclosing any information that would undermine national security would fulfill the requirement of the EU to give enough information for individuals to this standing before a US court.[223]

The nature of the issues that have invalidated both adequacy decisions indicates that having a codified set of standards is the only way to ensure the adequacy of protection while catering to national security needs and avoiding double standards. Not only would the rights of individuals be protected on both sides of the Atlantic, but the EU and the US would also protect each other's interests and set a global standard.

[216] Sharon Bradford Franklin et al., 'Executive Summary', Strengthening Surveillance Safeguards After Schrems II (New America, 2021).
[217] Kenneth Propp and Peter Swire, 'After Schrems II: A Proposal to Meet the Individual Redress Challenge', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 13 August 2020), p.3.
[218] Ibid.
[219] Schrems II, paragraph 191.
[220] Privacy Shield, Annex A, 4 (e).
[221] Chris D Linebaugh and Edward C Liu, 'EU Data Transfer Requirements and US. Intelligence Laws', p. 16
[222] Kenneth and Swire, 2020, p. 4.
[223] Propp and Swire, 'After Schrems II'.

Conclusion

The expansion of the Internet and new technologies have been tremendous in terms of the opportunities and benefits they have given to individuals, businesses, and in general to the world. Still, we cannot turn a blind eye to the reality that these benefits have also come with implications to our fundamental rights, including the protection of our privacy and personal data. Despite the Internet's global reach, we still do not have an international data protection law accepted universally, which creates various challenges for transfers of personal data. Mass surveillance and unauthorized access to personal data have been among the key issues we have dealt with in the past decade. The Snowden leaks showed us the severity of this surveillance by intelligence and national security agencies in the name of national security, and these revelations led to the CJEU invalidating two data transfer mechanisms between the EU and the US. The Schrems decisions have best shown the difference between EU and non-European countries, such as the US, regarding the privacy and protection of personal data. The US has not shown that it has the oversight and control mechanisms or effective redress mechanisms, as requested by the EU, in order for data transfers to continue between the two without any obstacles.

While the EU and the US are trying to develop a solution for the free flow of personal data post-Schrems II, many other questions have arisen. There have been many arguments and calls for the EU to re-evaluate the adequacy decisions with other third countries, along with voices that have raised the question of whether the EU's Member States are violating EU law with their surveillance practices. The invalidation of Schrems II has also brought forward many uncertainties about the future of data transfers. Leaving SCC's as one of the few options for companies to transfer data has made matters even more complicated as companies are now required to assess the laws and practices of third countries before beginning data transfers. This has led to the idea of data localization being brought up multiple times to protect the personal data of EU citizens. However, this option does not provide any real protection against foreign surveillance and is bound to have more negative rather than positive outcomes. On the other hand, the US has not shown any willingness to change its laws or create comprehensive legislation that would grant non-US individuals the same rights as those afforded in the EU.

Striking a balance between national security requirements and personal data protection will require the EU and US to develop a long-term solution to an issue that keeps bringing them back to square one. Asking the US to follow more stringent rules than those asked of EU

member states would mean that there are double standards in place, so an option could be creating data protection standards to be followed by both the EU and US. Both sides will have to work together to create a cross-border legal framework that guarantees protection against the unjustified access of personal data and the option of redress in the event this happens, and sets a standard for all future data transfers.

Bibliography

Akhtar, Shayerah Ilias. 'U.S.-EU Trade and Investment Ties: Magnitude and Scope'. Congressional Research Service, 2020. https://fas.org/sgp/crs/row/IF10930.pdf.

Article 29 Data Protection Working Party. Opinion 01/2016 on the EU – US Privacy Shield Draft Adequacy Decision., 2016. https://ec.europa.eu/newsroom/article29/items/640157

Article 29 Data Protection Working Party, 'Opinion 4/2000 on the Level of Protection Provided by the "Safe Harbor Principles"'. 2000. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp32_en.pdf.

Bayart, Betille, and Jacques-Olivier Martin. 'Thierry Breton: «C'est aux Gafa de s'adapter à nos règles, pas l'inverse»'. LEFIGARO, 2018. https://www.lefigaro.fr/secteur/high-tech/2018/04/06/32001-20180406ARTFIG00280-thierry-breton-c-est-aux-gafa-de-s-adapter-a-nos-regles-pas-l-inverse.php.

Bellamy, Bojana, Markus Heyder, and Nathalie Laneret. 'A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision'. Centre for Information Policy Leadership (CIPL), September 2020. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_gdpr_transfers_post_schrems_ii__24_september_2020__2_.pdf

Bigo, Didier, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi, Amandine Scherrer, Didier Bigo, and Belgium) Centre for European Policy Studies (Brussels. *Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law*. CEPS, 2013. https://www.ceps.eu/publications/mass-surveillance-personal-data-eu-member-states-and-its-compatibility-eu-law.

Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*. *The Brussels Effect*. Oxford University Press, 2020.

Bräutigam, Tobias. 'The Land of Confusion: International Data Transfers between Schrems and the GDPR'. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 19 December 2016. https://papers.ssrn.com/abstract=2920181.

Burgess, Matt. 'What Is GDPR? The Summary Guide to GDPR Compliance in the UK'. *Wired UK*, 24 March 2020. https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

Cate, Fred H, James X Dempsey, and Ira S Rubinstein. 'Systematic Government Access to Private-Sector Data'. *International Data Privacy Law* 2, no. 4 (2012): 5. https://doi.org/10.1093/idpl/ipu004.

Cayford, Michelle, and Wolter Pieters. 'The Effectiveness of Surveillance Technology: What Intelligence Officials Are Saying'. *The Information Society* 34, no. 2 (15 March 2018): 88–103. https://doi.org/10.1080/01972243.2017.1414721.

CCIA. 'CCIA Comments on Draft EDPB Recommendations on Supplementary Measures', 2020. https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/12-21-2020_-_ccia_response_to_the_edpb_on_schrems_ii_guidelines.pdf.

Chander, Anupam. 'Is Data Localization a Solution for Schrems II?' *Georgetown Law Faculty Publications and Other Works.* 2300 (2020). https://doi.org/10.2139/ssrn.3662626.

Chander, Anupam, Margot E. Kaminski, and William McGeveran. 'Catalyzing Privacy Law'. *SSRN Electronic Journal*, 2019. https://doi.org/10.2139/ssrn.3433922.

Chander, Anupam, and Uyên P. Lê. 'Data Nationalism'. *EMORY LAW JOURNAL* 64 (2015): 64. https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2/

Case C-131/12, Google Spain SL & Google Inc. v Agencia Española de Proteccción de Datos (AEPD) & Mario Costeja González, ECLI:EU:C:2014:317.

Case C–362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650).

Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems and intervening parties, ECLI:EU:C:2020:559.

Case C-623/17, The Investigatory Powers Tribunal (United Kingdom), in the proceedings Privacy International Case, ECLI:EU:C:2020:790.

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

Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

CCBE, Recommendations on the Protection of Fundamental Rights in the Context of National Security'. 2019. https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf

Christakis, Theodore. *'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy*. Rochester, NY: Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute, 2020. https://doi.org/10.2139/ssrn.3748098.

———. '"Schrems III"? First Thoughts on the EDPB Post-Schrems II Recommendations on International Data Transfers (Part 1)'. *European Law Blog*, 13 November 2020. https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/.

———. 'Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 1)'. *European Law Blog*, 12 April 2021. https://europeanlawblog.eu/2021/04/12/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part1/.

Christakis, Theodore, and Fabien Terpan. 'EU–US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options'. *International Data Privacy Law*, 12 February 2021. https://doi.org/10.1093/idpl/ipaa022.

Churches, Genna, and Monika Zalnieriute. 'A GROUNDHOG DAY IN BRUSSELS: SCHREMS II AND INTERNATIONAL DATA TRANSFERS', 2020, 8. https://doi.org/10.17176/20200716-235718-0.

Commission Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=en

Commission Decision 2000/520 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, 26 July 2000. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0520&from=en

Commission Decision 2016/1250 on the adequacy of the protection provided by the EU-US. Privacy Shield, 12 July 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN

Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108, https://rm.coe.int/1680078b37

Council of Europe, Table of cases and groups of cases under enhanced supervision. March 2021. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a1c7f2

Council of Europe/European Court of Human Rights, 'National Secutiry and European Case Law'. 2013. https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf.

'Data Protection Regulations and International Data Flows: Implications for Trade and Development | UNCTAD'. UNCTAD (United Nations Conference on Trade and Development), 2016. https://unctad.org/webflyer/data-protection-regulations-and-international-data-flows-implications-trade-and.

Docksey, Christopher. 'Schrems II and Individual Redress—Where There's a Will, There's a Way'. *Lawfare* (blog), 12 October 2020. https://www.lawfareblog.com/schrems-ii-and-individual-redress-where-theres-will-theres-way.

Donohue, Laura K.' High Technology, Consumer Privacy, and US National Security', 2015, 29. https://scholarship.law.georgetown.edu/facpub/1457/

Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995. https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

'Edward Snowden: Leaks That Exposed US Spy Programme'. *BBC News*, 17 January 2014, sec. US & Canada. https://www.bbc.com/news/world-us-canada-23123964.

European Commission, 'EU-U.S. Privacy Shield Launched'. 12 July 2016. https://ec.europa.eu/commission/presscorner/detail/en/ac_16_3701.

European Commission, 'EU-U.S. Privacy Shield: Third Review'. 23 October 2019. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6134.

European Commission, 'Intensifying Negotiations on Transatlantic Data Privacy Flow'. 25 March 2021. https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443

European Commission, 'Joint Press Statement from European Commissioner for Justice Didier Reynders and US Secretary of Commerce Wilbur Ross'. 10 August 2020. https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en

European Commission, 'Restoring Trust in Transatlantic Data Flows through Strong Safeguards: European Commission Presents EU-U.S. Privacy Shield'. https://ec.europa.eu/commission/presscorner/detail/eng/IP_16_433.

European Commission and Directorate-General for Justice and Consumers. *Guide to the EU-U.S. Privacy Shield*. Luxembourg: Publications Office, 2016. https://ec.europa.eu/info/sites/default/files/2016-08-01-ps-citizens-guide_en.pd_.pdf

———. *The GDPR: New Opportunities, New Obligations. What Every Business Needs to Know about the EU's General Data Protection Regulation.* Luxembourg: Publications Office, 2018. https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-sme-obligations_en.pdf

European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, https://www.echr.coe.int/documents/convention_eng.pdf

European Parliament. Directorate General for Internal Policies of the Union. *'A Comparison between US and EU Data Protection Legislation for Law Enforcement Purposes*.' LU: Publications Office, 2015. https://data.europa.eu/doi/10.2861/036283.

———. *National Programmes for Mass Surveillance of Personal Data in EU MS and Their Compatibility with EU Law*. LU: Publications Office, 2013. https://data.europa.eu/doi/10.2861/48584.

European Parliament. Directorate General for Parliamentary Research Services. *From Safe Harbour to Privacy Shield: Advances and Shortcomings of the New EU-US Data Transfer Rules: In Depth Analysis.* LU: Publications Office, 2017. https://data.europa.eu/doi/10.2861/09488.

———. *The Privacy Shield: Update on the State of Play of the EU-US Data Transfer Rules: In Depth Analysis.* LU: Publications Office, 2016. https://data.europa.eu/doi/10.2861/675548.

European Union Agency for Fundamental Rights. *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II, Field Perspectives and Legal Update.* LU: Publications Office, 2017. https://data.europa.eu/doi/10.2811/792946.

European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

European Data Protection Board, 41st Plenary Session: 'EDPB Adopts Recommendations on Supplementary Measures Following Schrems II'. 11 November 2020. https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_en.

European Data Protection Board, Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf

European Data Protection Board, Opinions on draft UK adequacy decisions, Guidelines on the application of Article 65(1)(a) GDPR, Guidelines on the targeting of social media users and Statement on international agreements including transfers https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf

European Data Protection Board, Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data'. 2020. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. 2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

Franklin, Sharon Bradford, Lauren Sarkesian, Ross Schulman, and Spandana Singh. 'Executive Summary'. Strengthening Surveillance Safeguards After Schrems II. New America, 2021. https://www.jstor.org/stable/resrep30591.3.

Global Legal Group, 'International Comparative Legal Guides'. Text. International Comparative Legal Guides International Business Reports. Global Legal Group. United Kingdom. 2020. https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

Holmes, Dawn. *Big Data: A Very Short Introduction*. Very Short Introductions. Oxford, New York: Oxford University Press, 2018.

Hoofnagle, Chris Jay, Bart van der Sloot, and Frederik Zuiderveen Borgesius. 'The European Union General Data Protection Regulation: What It Is and What It Means'. *Information & Communications Technology Law* 28, no. 1 (2 January 2019): 65–98. https://doi.org/10.1080/13600834.2019.1573501.

Humble, Kristian P.' International Law, Surveillance and the Protection of Privacy'. *The International Journal of Human Rights* 25, no. 1 (2 January 2021): 1–25. https://doi.org/10.1080/13642987.2020.1763315.

Kerr, Orin S.' A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It'. *George Washington Law Review* 72 (2004): 1208–43. https://doi.org/10.2139/ssrn.421860.

Kerr, Orin S. 'The Next Generation Communications Privacy Act'. *University of Pennsylvania Law Review* 162 (2014): 373–419. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1546&context=penn_law_review

Koops, Bert-Jaap, Bryce Clayton Newell, Tjerk Timan, Tomislav Chokrevski, and Maša Gali. 'A TYPOLOGY OF PRIVACY'. *University of Pennsylvania Journal of International Law* 38, no. 2 (2017): 483–575. https://scholarship.law.upenn.edu/jil/vol38/iss2/4/

Kuner, Christopher. 'Reality and Illusion in EU Data Transfer Regulation Post Schrems'. *German Law Journal* 18, no. 4 (July 2017): 881–918. https://doi.org/10.1017/S2071832200022197.

———. 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future'. OECD Digital Economy Papers. Vol. 187. OECD Digital Economy Papers, 8 December 2011. https://doi.org/10.1787/5kg0s2fk315f-en.

———. 'The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation'. *European Law Blog* (blog), 17 July 2020. https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/.

Linebaugh, Chris D, and Edward C Liu. 'EU Data Transfer Requirements and US Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield'. Congressional Research Service, 2021. https://fas.org/sgp/crs/row/R46724.pdf.

Little, Rory. 'Protecting Privacy Under the Fourth Amendment'. *The Yale Law Journal* 91 (1981): 31. https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=6716&context=ylj

Manancourt, Vincent. 'EU to US on Surveillance: Do as I Say, Not as I Do'. *POLITICO*, 17 March 2021. https://www.politico.eu/article/eu-to-us-surveillance-data-flows/

McAdams, A. James. 'Internet Surveillance after September 11: Is the United States Becoming Great Britain?' Edited by Cynthia Brown, Nancy Chang, David Cole, James X. Dempsey, Nat Hentoff, and Stephen J. Schulhofer. *Comparative Politics* 37, no. 4 (2005): 479–98. https://doi.org/10.2307/20072905.

McCabe, David, and Cecilia Kang. 'As Congress Dithers, States Step In to Set Rules for the Internet'. *The New York Times*, 14 May 2021, sec. Technology. https://www.nytimes.com/2021/05/14/technology/state-privacy-internet-laws.html

Meltzer, Joshua P. 'After Schrems II: The Need for a US-EU Agreement Balancing Privacy and National Security Goals'. *Global Privacy Law Review* 2, no. 1 (2021): 83–89. https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\GPLR\GPLR2021007.pdf

Meltzer, Joshua P.' The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security'. *Brookings* (blog), 5 August 2020. https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/.

Miettinen, Samuli, and Tobias Bräutigam. *Data Protection, Privacy and European Regulation in the Digital Age*, 2016.

Mildebrath, Hendrik. 'The CJEU Judgment in the Schrems II Case'. At a Glance. European Parliamentary Research Service, 2020.

https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

Mitchell, Andrew D, and Jarrod Hepburn. 'DON'T FENCE ME IN: REFORMING TRADE AND INVESTMENT LAW TO BETTER FACILITATE CROSS-BORDER DATA TRANSFER'. *TECHNOLOGY Vol.* 19 (2018): 56. https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1128&context=yjolt

Movius, Lauren B, and Nathalie Krup. 'US and EU Privacy Policy: Comparison of Regulatory Approaches'. *International Journal of Communication* 3 (2009): 19. https://ijoc.org/index.php/ijoc/article/viewFile/405/305

Mulligan, Stephen P, and Chris D Linebaugh. 'Data Protection and Privacy Law: An Introduction'. *An Introduction*, 9 May 2019, 3. https://fas.org/sgp/crs/misc/IF11207.pdf

Philouze, Anna-Laure. 'The EU-US Privacy Shield: Has Trust Been Restored?' *European Data Protection Law Review* 3, no. 4 (2017): 463–72. https://doi.org/10.21552/edpl/2017/4/8.

POLITICO. 'EU's Rejection of US Surveillance Also Tests Its Commitment to Privacy', 17 July 2020. https://www.politico.eu/article/rejection-of-us-surveillance-tests-eu-mettle-on-privacy-shield/.

Propp, Kenneth, and Peter Swire. 'After Schrems II: A Proposal to Meet the Individual Redress Challenge'. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 13 August 2020. https://doi.org/10.2139/ssrn.3680148.

Reidenberg, Joel R.' The Data Surveillance State in Europe and the United States' 49 (n.d.): 27. https://ir.lawnet.fordham.edu/faculty_scholarship/645/

Reidenberg, Joel R. 'Resolving Conflicting International Data Privacy Rules in Cyberspace'. Stanford Law Review 52, no. 5 (May 2000): 1315. https://doi.org/10.2307/1229516.

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC 2016) OJ L119/1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Relyea, Harold C.' The Privacy Act: Emerging Issues and Related Legislation'. Congressional Research Service., 26 February 2002. https://fas.org/irp/crs/RL30824.pdf

Robinson, Neil, Hans Graux, Maarten Botterman, and Lorenzo Valeri. 'Review of EU Data Protection Directive: Summary'. *RAND Europe*, 2009, 14. https://ico.org.uk/media/about-the-ico/documents/1042347/review-of-eu-dp-directive-summary.pdf

Rotenberg, Marc. 'Schrems II, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection'. *European Law Journal* 26, no. 1–2 (2020). https://doi.org/10.1111/eulj.12370.

Rubinstein, Ira, and Peter Margulies. 'Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, US Surveillance, and the Search for Common Ground'. *SSRN Electronic Journal*, 2021. https://doi.org/10.2139/ssrn.3786415.

Schrems, Max. 'Complaint against Facebook Ireland Ltd – 23 "PRISM"', 2013. http://www.europe-v-facebook.org/prism/facebook.

Schwartz, Paul M.' GLOBAL DATA PRIVACY: THE EU WAY'. *NEW YORK UNIVERSITY LAW REVIEW* 94 (October 2019): 48. https://paulschwartz.net/wp-content/uploads/2019/10/NYULAWREVIEW-94-4-Schwartz.pdf

Schwartz, Paul M, and Karl-Nikolaus Peifer. 'Structuring International Data Privacy Law'. *International Data Privacy Law* 7, no. 2 (2021): 49.

———. 'Transatlantic Data Privacy Law'. *THE GEORGETOWN LAW JOURNAL* 106 (2017): 65. https://escholarship.org/content/qt1ws1r1cz/qt1ws1r1cz_noSplash_816c6e2b4eaaaec14b0a03ecedd4031b.pdf?t=p68tx6

Sciutto, Jim, and Zachary Cohen. 'NSA Reveals 100,000 Foreign Nationals under Surveillance'. *CNNPolitics*, 25 September 2017. https://edition.cnn.com/2017/09/25/politics/fisa-section-702-surveillance-nsa/index.html.

Smith, Mark. 'ANALYSIS: Will Schrems II Cause Five Eyes to Blink?'. *Bloomberg Law*, 16 November 2020. https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-will-schrems-ii-cause-five-eyes-to-blink.

Nach „Schrems II“: Europa braucht digitale Eigenständigkeit https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf. Translation by DeepL

Stehlík, Václav, and Lusine Vardanyan. 'Schrems II: Will It Really Increase the Level of Privacy Protection against Mass Surveillance?' *Bratislava Law Review* 4, no. 2 (31 December 2020): 111–28. https://doi.org/10.46282/blr.2020.4.2.215.

Stolton, Samuel. 'Data Sharing Services Must Be "established in the EU," Leaked Regulation Reveals'. 30 October 2020. https://www.euractiv.com/section/digital/news/data-sharing-services-must-be-established-in-the-eu-leaked-regulation-reveals/.

———. 'New EU Data Brokers Won't Have to Be European, Commission Says'. *Www.Euractiv.Com* (blog), 26 November 2020. https://www.euractiv.com/section/digital/news/new-eu-data-brokers-wont-have-to-be-european-commission-says/.

Streinz, Thomas. 'The Evolution of European Data Law'. In *The Evolution of EU Law*, 3rd ed. Oxford, New York: Oxford University Press, 2021. https://doi.org/10.2139/ssrn.3762971.

Svantesson, Dan. 'Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines'. OECD Digital Economy Papers. Vol. 301. OECD Digital Economy Papers, 22 December 2020. https://doi.org/10.1787/7fbaed62-en.

Tamò-Larrieux, Aurelia. *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things*. 1st ed. 2018. Issues in Privacy and Data Protection 40. Cham: Springer International Publishing : Imprint: Springer, 2018. https://doi.org/10.1007/978-3-319-98624-1.

'The Digital Person: Technology and Privacy in the Information Age'. *Choice Reviews Online* 42, no. 09 (1 May 2005): 42-5512-42–5512. https://doi.org/10.5860/CHOICE.42-5512.

Théodore, Christakis. 'Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2)'. *European Law Blog*, 13 April 2021. https://europeanlawblog.eu/2021/04/13/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part2/.

Théodore, Christakis, and Bouslimani Katia. 'Part III Security Governance Tools, Ch.38 National Security, Surveillance, and Human Rights'. In *The Oxford Handbook of the International Law of Global Security*, by Christakis Théodore and Bouslimani Katia. Oxford University Press, 2021. https://doi.org/10.1093/law/9780198827276.003.0039.

Théodore, Christakis, and Kenneth Propp. 'How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States'. *Lawfare*, 8 March 2021. https://www.lawfareblog.com/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states.

Tracol, Xavier. '"Schrems II": The Return of the Privacy Shield'. *Computer Law & Security Review* 39 (November 2020): 105484. https://doi.org/10.1016/j.clsr.2020.105484.

Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 December 2007, 2007/C 306/01. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT

Tyson, Barker. 'Breaking the Transatlantic Data Trilemma: The EU Must Step Up Its Approach to EU-US Data Flows'. *Forschungsinstitut Der Deutschen Gesellschaft Für Auswärtige Politik e.V.*, DGAP Policy Brief, no. 27 (2020): 10. https://dgap.org/sites/default/files/article_pdfs/dgap-policy_brief-2020-27-en_0.pdf

UN Office of the High Commissioner for Human Rights (OHCHR), Fact Sheet No. 32, Human Rights, Terrorism and Counter-terrorism, July 2008, No. 32. https://ohchr.org/Documents/Publications/Factsheet32EN.pdf

United States, 'COMMENTS ON PROPOSED EDPB RECOMMENDATIONS 01/2020', 2020. https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/2020.12.21_-_us_comments_on_edpb_supp_measures_final.pdf.

Weiss, Martin A, and Kristin Archick. 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield'. Congressional Research Service, 2016. https://fas.org/sgp/crs/misc/R44257.pdf.