SCHREMS II: THE EU'S INFLUENCE ON U.S. DATA PROTECTION AND PRIVACY LAWS

INTRODUCTION

The United States and European Union[1] have been deeply connected since the EU's formation in 1957.[2] Although international trade is a hallmark of the U.S. and EU's relationship, the two have struggled throughout history to align their laws and objectives, despite a collection of evolving international trade agreements.[3] That said, the U.S. and EU's trade relationship is considered to be the "world's largest and most important bilateral commercial relationship."[4] The Transatlantic Economy accounts for 16 million jobs, trillions of dollars in total commercial sales, and one third of the total gross domestic product in terms of purchasing power.[5] More recently, the digital revolution has posed a threat to the Transatlantic Economy, revealing fundamental differences in U.S. and EU law.[6]

To harmonize U.S. and EU law, the respective countries have entered into numerous trade agreements to maximize transatlantic

1 The European Union is made up of 27 member states: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden. *Countries*, EUROPA, https://europa.eu/european-union/about-eu/countries_en (last visited Nov. 13, 2021).

2 *See History of the U.S. and the EU*, U.S. MISSION TO THE EUROPEAN UNION https://useu.usmission.gov/our-relationship/policy-history/io/ (last visited Nov. 13, 2021) ("Diplomatic relations between the U.S. and the European Community were initiated in 1953 when the first U.S. observers were sent to the European Coal and Steel Community . . . ."). Now, they are the most deeply integrated regions in the world. *See generally* DANIEL S. HAMILTON. & JOSEPH P. QUINLAN, THE TRANSATLANTIC ECONOMY 2020: ANNUAL SURVEY OF JOBS, TRADE AND INVESTMENT BETWEEN THE UNITED STATES AND EUROPE (2020).

3 Behind these numerous trade agreements is the Transatlantic Economic Council, which was established in 2007. The Transatlantic Economic Council is "the only EU-US high level forum in which economic issues can be discussed in a coherent and coordinated manner. It brings together a range of ongoing economic cooperation activities in issues of mutual interest and provides a platform to give political guidance to this work. It also provides a political forum for discussing strategic global economic questions. The TEC brings together members of the European Commission and the US Cabinet who have political responsibility for closer economic ties." European Commission, *EU and US boost economic partnership*, EUROPA, https://ec.europa.eu/commission/presscorner/detail/en/IP_11_1481 (last visited Nov. 13, 2021).

4 *See* HAMILTON & QUINLAN, *supra* note 2, at 2.

5 *Id.* at ii. "Subsea cables bring the internet to life. They transmit 99% of all intercontinental telecommunication traffic . . . . Every day they transmit close to $10 trillion in transactions around the world." *Id.* at 41.

6 *Id.* at viii ("Transatlantic flows of data continue to be the fastest and largest in the world, accounting for over one-half of Europe's data flows and about half of U.S. flows. Almost 40% of those flows are through business and research networks.").

data transfers.[7] The EU leverages the importance of the Transatlantic Economy to encourage the U.S. to comply with EU law through numerous court decisions[8] directly targeting the inadequacy of U.S. domestic law compared to the General Data Protection Regulation ("GDPR") and EU Charter. With each international trade agreement and landmark decision, the EU has influenced the U.S. to alter its approach, proving the EU's power as a progressive leader in data protection and privacy laws. This note chronicles previous U.S.-EU trade agreements and the landmark cases ordering their invalidations to demonstrate the EU's influence on the advancement of U.S. data protection and privacy law.

I. UNDERSTANDING THE GAP: U.S. AND EU LAW

A. U.S. Approach to Data Privacy and Protection

The U.S. approach to data privacy and protection consists of state and federal laws in a "patchwork" system.[9] There is no general data privacy protection or all-encompassing law.[10] Further, the U.S. Constitution contains no express right to privacy.[11] Data protection and privacy rights are thus statute and state specific.[12] There is no single authority tasked with enforcing data protection and privacy rights. Instead, the U.S. relies on the broad power of the Federal Trade

7 In addition to the Safe Harbor and Privacy Shield trade agreements mentioned in this paper, the U.S. and EU also engaged in international trade agreements through the Transatlantic Trade and Investment Partnership. *Transatlantic Trade and Investment Partnership (T-TIP)*, OFF. OF THE U.S. TRADE REPRESENTATIVE, https://ustr.gov/ttip (last visited Nov. 13, 2021). "This partnership was aimed at providing greater compatibility and transparency in trade and investment regulation, while maintaining high levels of health, safety, and environmental protection." *Id.*

8 Of focus in this Note are the *Schrems I* and *Schrems II* decisions, which are only two of the numerous cases filed in the EU against the U.S. alleging GDPR violations.

9 See MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RSCH. SERV., U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 3 (May 19, 2016); *see generally* STEVEN CHABINSKY & F. PAUL PITTMAN, INT'L COMPAR. LEGAL GUIDES, USA DATA PROTECTION LAWS AND REGULATIONS 2021 (June 7, 2021), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

10 WEISS & ARCHICK, *supra* note 9, at 3.

11 *Privacy Rights and Personal Autonomy*, JUSTIA (last updated Oct. 2021), https://www.justia.com/constitutional-law/docs/privacy-rights/ (listing the rights of privacy in the U.S. Constitution as determined by the Supreme Court of the United States: right to procreation, right to abortion, right to private consensual homosexual activity, right to pornography, and the right to refuse medical treatment).

12 *See* CHABINSKY & PITTMAN, *supra* note 9; WEISS & ARCHICK, *supra* note 9, at 3.

Commission (FTC), administrative agencies,[13] and the few state judicial systems[14] with established laws for enforcement.

At the federal level, data protection and privacy laws are organized by sector and are industry-specific.[15] For example, the U.S. Privacy Act of 1974[16] was adopted in response to growing concerns of government surveillance.[17] The Act restricts disclosure of personal data held by federal agencies, guarantees individuals the right to access the agency records and the right to amend them, and establishes overarching "fair information practices."[18] It also protects personal data collected by federal agencies (subject to exceptions),[19] prohibits the disclosure of the collected personal data without written consent,[20] and requires agencies to publish a notice of their records.[21]

---

13 CHABINSKY & PITTMAN, *supra* note 9, 1.1, 1.4; *see also* FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2019, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf#:~:text=Federal%20Trade%20Commission%202019%20Privacy%20and%20Data%20Security,prohibits%20unfair%20or%20deceptive%20practices%20in%20the%20marketplace (last visited Nov. 13, 2021) ("Using its existing authority, the Commission has brought hundreds of privacy and data security cases to date. To better equip the Commission to meet its statutory mission to protect consumers, the FTC has also called on Congress to enact comprehensive privacy and data security legislation, enforceable by the FTC.").

14 See *Privacy and Data Security*, OFF. OF ATT'Y GEN. OF CAL., https://oag.ca.gov/privacy (last visited Nov. 13, 2021) for an example of state enforcement authority in California, where the Department of Justice's Privacy Unit "enforces state and federal privacy laws, empowers Californians with information on their rights and strategies for protecting their privacy, encourages businesses to follow privacy-respectful best practices and advises the Attorney General on privacy matters."

15 CHABINSKY & PITTMAN, *supra* note 9, at 1.2, 1.3; *see, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996); Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999); Children's Online Privacy Protection Rule, Pub. L. No. 105-277, 112 Stat. 2681 (1998).

16 Privacy Act of 1974, 5 U.S.C. § 552(a) (2012).

17 *See* U.S. DEP'T OF JUST., OVERVIEW OF THE PRIVACY ACT OF 1974, 4 (2015 ed.), https://www.justice.gov/archives/opcl/file/793026/download ("In 1974, Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies that had been exposed during the Watergate scandal. It was also concerned with potential abuses presented by the government's increasing use of computers to store and retrieve personal data by means of a universal identifier – such as an individual's social security number"). .

18 *See id.* for the four basic policy objectives: "to restrict disclosure of personally identifiable records maintained by agencies, to grant individuals increased rights of access to agency records maintained on themselves, to grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete and to establish a code of 'fair information practices' that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records."

19 *Id.* at 130, 68-115.

20 *Id.* at 4.

21 *Id.* at 138.

At the state level, data protection and privacy laws vary.[22] Some states are more progressive and stricter on data protection than others. Currently, California, Virginia, and Colorado are the only three states with privacy laws in effect.[23] For example, the California Consumer Privacy Act of 2018 ("CCPA") and California Privacy Rights Act of 2020 ("CPRA") provide protection for the most Consumer Rights out of all state law in the U.S.[24] The CCPA and CPRA, together, guarantee California residents eight affirmative consumer rights, including the right to restrict processing of their personal data.[25] Virginia and Colorado follow the CCPA and CPRA closely, but do not afford its citizens the right of restriction or even a limited private right of action like the CPPA and CPRA provide to California citizens.[26]

B. EU Approach to Data Protection and Privacy

The EU's approach to data protection and privacy is the antipode of the U.S. approach. Not only does the EU have uniform, all-encompassing data protection and privacy laws, it explicitly recognizes privacy and data protection as fundamental human rights.[27] Each of the independent countries that make up the EU have coordinated their laws on enforcing data protection and privacy to

22 See Sarah Rippy, *US State Comprehensive Privacy Law Comparison*, INT'L. ASS. OF PRIVACY PROS., https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last updated Sept. 16, 2021) for a complied research table created by the International Association of Privacy Professionals displaying each of the 50 U.S. state's data protection and privacy laws, if any, with a brief overview of general principles.

23 The other two states with privacy laws currently in effect are Virginia and Colorado. *Id.*

24 *Id.*

25 *See* In Brief: CCPA vs. CPRA: What's the Difference? BLOOMBERG LAW, (July 13, 2021) https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/; *see also* Rippy, *supra* note 22.

26 Rippy, *supra* note 22.

27 The EU Charter of Fundamental Rights of the European Union Article 7 generally declares "Everyone has the right to respect for his or her private and family life, home and communications. Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1, art. 7, https://www.europarl.europa.eu/charter/pdf/text_en.pdf [hereinafter "EU Charter"]. EU Charter Article 8 explicitly addresses protection of personal data, stating: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority." *Id.* at art. 8.

create a uniform approach.[28] Further, the EU has independent enforcement bodies, such as the Article 29 Working Party[29] and a Data Protection Officer.[30]

EU data protection and privacy laws have evolved rapidly, beginning with the Data Protection Directive ("DPD") implemented in 1995.[31] To enforce the key principles of the DPD,[32] the EU established an advisory body known as the "Article 29 Working Party."[33] In 2016, the EU replaced the DPD with the General Data Protection Regulation ("GDPR"). With this change came heightened and expanded protection.[34] For example, the GDPR expanded the

---

28 Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 63 [hereinafter GDPR] ("In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.").

29 *Article 29 Working Party*, EUR. DATA PROT. BD., https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en (last visited Nov. 11, 2021) ("The Article 29 Working Party (Art. 29 WP) is the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018 (entry into application of the GDPR").

30 European Commission, *Data Protection Officer*, EUROPA https://ec.europa.eu/info/departments/data-protection-officer_en#:~:text=Data%20Protection%20Officer%20The%20Data%20Protection%20Officer%20(DPO),by%20the%20Commission%20that%20involve%20processing%20personal%20data (last visited Nov. 13, 2021) ("The Data Protection Officer (DPO) ensures, in an independent manner, that the European Commission correctly applies the law protecting individuals' personal data. The DPO keeps a public register explaining all operations carried out by the Commission that involve processing personal data.").

31 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), 1995 O.J. (L. 281) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

32 The Principles are "Notice – individuals should be notified when their personal data is collected; Purpose – use of personal data should be limited to the express purpose for which it was collected; Consent – individual consent should be required before personal data is shared with other parties; Security – collected data should be secured against abuse or compromise; Disclosure – data collectors should inform individuals when their personal data is being collected; Access – individuals should have the ability to access their personal data and correct any inaccuracies; Accountability – individuals should have a means to hold data collectors accountable to the previous six principles." Nate Lord, *What Is the Data Protection Directive? The Predecessor to the GDPR*, DIGITAL GUARDIAN (Sept. 12, 2018), https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr.

33 *See generally Article 29 Working Party*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/art29wp/#:~:text=The%20Working%20Party%20on%20the,Member%20States%2C%20the%20European%20Data (last visited Nov. 13, 2021).

34 *See* SeeUnity, *The Main Differences Between the DPD and the GDPR and How to Address Those Moving Forward*, BRITISH LEGAL TECH. FORUM 2 (2007), https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf, (identifying six broad changes under the GDPR: personal data redefined, individual rights, data

definition of "personal data" to include electronic identification such as IP addresses, mobile device identifiers, geolocation, and biometric data.[35] Thus, the GDPR replaced the DPD to respond to technological advancements and the internet.

The EU's approach to data protection and privacy laws is international in scope and coverage.[36] The European Commission enforces the GDPR throughout the Union, allowing international transfers of EU citizen's personal data without further safeguards only to countries outside the EU deemed to have an "adequate" level of protection.[37] If countries cannot satisfy an "adequate" level of protection, data transfers are suspended or postponed until an adequate level of protection is guaranteed.[38] The GDPR provides

---

controllers vs. data processors, information governance and security, data breach notification and penalties and global impact).

35 *Id.* at 3. "Personal data" was defined in the DPD as "a person's name, photo, email address, phone number, address, or any personal identification number (social security, bank account, etc.)." *Id.* at 2.

36 *Does the GDPR Apply to Companies Outside the EU?*, GDPR, https://gdpr.eu/companies-outside-of-europe (last visited Nov. 13, 2021) ("Article 3.1 states that the GDPR applies to organizations that are based in the EU even if the data are being stored or used outside of the EU. Article 3.2 goes even further and applies the law to organizations that are not in the EU if two conditions are met: the organization offers goods or services to people in the EU, or the organization monitors their online behavior. (Article 3.3 refers to more unusual scenarios, such as in EU embassies.").

37 European Commission, *Adequacy Decisions*, EUROPA, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Nov. 13, 2021). The "European Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, the United Kingdom under the GDPR and the LED and Uruguay as providing adequate protection." *Id.*

38 GDPR, *supra* note 29, art. 45 states, "When assessing the adequacy of the level of protection, the Commission shall take account of the following elements:

> a. the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> b. the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
>
> c. the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."

several options for international data transfers without an adequacy decision but with additional safeguards including: Binding Corporate Rules ("BCRs"),[39] Standard Contract Clauses ("SCCs"),[40] Article 49 derogations,[41] or international trade agreements to transfer personal data.[42] BCRs are usually utilized by businesses established in the EU for transfers of personal data outside of the EU within their business enterprise.[43] SCCs, however, can be utilized by both EU-based businesses and business outside of the EU to maintain compliance with the GDPR.[44] Article 49 derogations have a limited application and can only be used in specific circumstances where no other mechanism of compliance is applicable.[45] Lastly, international trade agreements, such as the Safe Harbor and Privacy Shield agreements, can take the place of an adequacy decision, allowing the free flow of personal data between the EU and the third-party country. However, the EU maintains the authority to reassess and redetermine the adequacy of the agreement, potentially compromising perceptions of the permanence of these international trade agreements and the ability

39 Binding Corporate Rules are subject to numerous detailed requirements set out in paragraph 2 of Article 47 focusing on their structure, legally binding nature, and procedure, among other things. *Id.* art. 47.

40 *See generally id.* art. 46; Press Release, *European Commission adopts new tools for safe exchanges of personal data*, EUROPA (June 4, 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847; Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, 2021 O.J. (L. 199), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0915&locale-en; Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, 2021 O.J. (L. 199), https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en..

41 GDPR, *supra* note 29, art. 49. Article 49 of the GDPR sets out seven conditions under which a transfer of personal data to a third country may take place in the absence of an adequacy decision, BCRs, SCCs, and international trade agreement. *Id.*

42 *Id*.

43 European Commission, *Binding Corporate Rules (BCR)*, EUROPA, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#howistheleadauthoritychosen (last visited Nov. 13, 2021).

44 European Commission, *Standard Contractual Clauses (SCC)*, EUROPA, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (last visited Nov. 13, 2021).

45 GDPR, *supra* note 29, art. 49.

to rely completely on their terms.[46] As a result, third-party countries with international trade agreements may still implement multiple alternative means of compliance with the GDPR to mitigate the consequences of complete reliance.

Because of its expansive coverage and flexible nature, the GDPR is considered the "gold standard" of data protection and privacy.[47] Although the GDPR is not perfect, it is the most progressive and protective approach to data protection and privacy in the world. As a result of its international application, the EU forces other countries wanting to exchange, collect, or maintain personal data with the EU to meet their high standard.

II. BRIDGING THE GAP: PREVIOUS TRADE AGREEMENTS

A. The Safe Harbor Framework

After the implementation of the DPD in the EU and numerous negotiations, the U.S. and EU established the U.S.-EU Safe Harbor Framework ("Safe Harbor Framework").[48] This international trade agreement provided a mechanism by which the U.S. ensured an adequate level of protection without disrupting transatlantic data flow and the transatlantic economy.[49] This framework was necessary for the U.S. to continue receiving personal data from EU citizens, as U.S.

46 European Commission, *supra* note 38 ("At any time, the European Parliament and the Council may request the European Commission to maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the regulation.").

47 "The General Data Protection Regulation (or GDPR) is going to raise the bar for data protection laws around the world." Giovanni Buttarelli, *The EU GDPR as a Clarion Call For a New Global Digital Gold Standard*, EUROPA (Apr. 1, 2016), https://edps.europa.eu/press-publications/press-news/blog/eu-gdpr-clarion-call-new-global-digital-gold-standard_de; *see also* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 453 (2019) ("Many difficulties remain to be overcome, but the GDPR is rapidly evolving into the transnational gold standard of data protection, applicable to all domestic and cross-border transfers of personally identifiable data.").

48 Issuance of Safe Harbor Principles and Transmission to European Commission Notice, 65 Fed. Reg. 45666 (July 24, 2000).

49 *See id.* ("The Principles . . . are intended to serve as authoritative guidance to U.S. companies and other organizations receiving personal data from the European Union. Upon receipt of the Principles, the Commission is expected to issue an 'adequacy determination' for the safe harbor arrangement. Organizations receiving personal data transfers from the EU and complying with the Principles will be considered to meet the 'adequacy' requirements of the European Union's Directive on Data Protection.").

domestic law alone did not guarantee a standard of protection equal to what is required in the EU.[50]

The Safe Harbor Framework required U.S. companies to annually self-certify their compliance with seven basic data protection and privacy principles and requirements necessary to meet the EU's adequacy standards.[51] Enforcement of these standards in the U.S. was handled through federal and state authorities that were already tasked to protect against unfair and deceptive practices, such as the Federal Trade Commission.[52] Over 5,000 U.S. companies self-certified and utilized the Safe Harbor Framework to transfer the personal data and maintain the privacy of EU citizens.[53]

However, the Safe Harbor Framework was not ironclad. Under the Safe Harbor Framework, U.S. compliance with the principles was limited.[54] Therefore, U.S. companies could disregard the principles of the Safe Harbor Framework to the "extent necessary to meet national

50 *See infra*, *Schrems I*and *Schrems II*.

51 *U.S.-EU Safe Harbor Framework: A Guide to Self-Certification*, U.S. DEP'T. OF COM. 19 (updated March 2013), https://2016.export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_061613.pdf.

52 "Section 5(a) of the FTC Act provides that 'unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful.'" Federal Trade Commission, *A Brief Overview of the Federal Trade Commission's Investigate, Law Enforcement, and Rulemaking Authority*, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last visited Nov. 13, 2021) (citing 15 U.S.C. § 45(a)(1)). "'Deceptive' practices are defined in the Commission's Policy Statement on Deception as involving a material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances. An act or practice is 'unfair' if it 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'" *Id.* (citing 15 U.S.C. § 45(n)).

53 *See* Daniel Alvarez, *Safe Harbor Is Dead; Long Live the Privacy Shield?*, AM. BAR ASS'N (May 20, 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/05/09_alvarez/ ("Without Safe Harbor, over 5,000 companies and organizations were forced to adapt their data transfer and privacy policies and practices almost overnight, with little certainty about what might come next.").

54 *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, at 16 COM (2013) 0847 final (Nov. 27, 2013) ("The Safe Harbour Decision provides, in Annex 1, that adherence to the Privacy Principles may be limited, if justified by national security, public interest, or law enforcement requirements or by statute, government regulation or case-law. In order for limitations and restrictions on the enjoyment of fundamental rights to be valid, they must be narrowly construed; they must be set forth in a publicly accessible law and they must be necessary and proportionate in a democratic society. In particular, the Safe Harbour Decision specifies that such limitations are allowed only 'to the extent necessary' to meet national security, public interest, or law enforcement requirements.").

security, public interest, or law enforcement requirements."[55] Ultimately, this limitation provision was called into question by the Court of Justice of the European Union ("CJEU"),[56] highlighting the EU's concern over U.S. government surveillance[57] and the EU's commitment to their data protection and privacy standards.

B. Schrems I & Invalidation of the Safe Harbor Framework

While attending law school in the United States, Austrian-born Maximillian Schrems began investigating Facebook's compliance with EU law after hearing one of Facebook's lawyers speak about data privacy at his school.[58] He requested Facebook to release their personal record on him and received over 1,200 pages of data.[59] After the Snowden revelations,[60] Schrems was concerned about the amount of personal information Facebook maintained in the U.S. He sued Facebook Ireland for keeping its users' data on servers located in the U.S., arguing that U.S. government surveillance is incompatible with

---

55 Issuance of Safe Harbor Principles and Transmission to European Commission Notice, *supra* note 49, at 45667. The U.S. may also limit Safe Harbor Principles "(b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts." *Id.*

56 *See generally* European Union, *Court of Justice of the European Union (CJEU)*, Europa, https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en#how-does-the-cjeu-work (last visited Nov. 13, 2021) ("The Court of Justice of the European Union (CJEU) interprets EU law to make sure it is applied in the same way in all EU countries, and settles legal disputes between national governments and EU institutions. It can also, in certain circumstances, be used by individuals, companies or organisations to take action against an EU institution, if they feel it has somehow infringed their rights.").

57 Case C-362/14, Maximillian Schrems v. Digital Rights Ireland Ltd., ECLI:EU:C:2015:627, ¶ 25(Sept. 23, 2015) [hereinafter "Schrems I"]; *see also id.* at ¶ 35 ("[T]he revelations made by Edward Snowden demonstrated a significant over-reach on the part of the NSA and other similar agencies.").

58 Kashmir Hill, *Max Schrems: The Austrian Thorn in Facebook's Side*, FORBES (Feb. 7, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/?sh=3f1d90d77b0b.

59 *Id.*

60 See generally *Revelations*, FREE SNOWDEN, https://freesnowden.is/revelations/#prism-an-nsa-partnership-with-us-service-providers (last visited Nov. 13, 2021) for a detailed account of all revelations by the former CIA whistleblower. Particularly relevant in *Schrems I* was the overreaching and generalized government surveillance conducted through PRISM: "Numerous documents outline PRISM, which enables the routine collection of data including emails, chats, videos, file transfers and photos from private companies that include Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL and Apple." *Id; see also* Schrems I, *supra* note 58, ¶ 26.

the GDPR.[61] Further, he challenged the legitimacy of the Safe Harbor Framework, and pleaded to the CJEU to evaluate the level of protection afforded by the U.S. under the Safe Harbor Framework. [62]

The CJEU held the U.S. data protection and privacy laws were inadequate and that the Safe Harbor Framework did not sufficiently address these inadequacies, rendering it invalid.[63] In its reasoning, the CJEU focused on the content of the U.S. data protection and privacy laws and its means of ensuring compliance.[64] Ultimately, because of mass government surveillance[65] and the fact that U.S. citizens have no "effective right to be heard on the question of the surveillance and interception of their data,"[66] the U.S. data protection and privacy framework does not guarantee equivalent protection required under EU law.[67] The court further held the Safe Harbor Framework was not specific enough and did not hold enough authoritative value in the U.S. legal system to absolve these deficiencies. Instead, the CJEU found that the Safe Harbor Framework acted as a framework that allows EU citizen's data to be collected by U.S. government intelligence agencies, rather than protecting its citizens' personal data from interference that is not "strictly necessary."[68]

As a result of this decision, transatlantic data transfers were immediately suspended and rendered illegal under the Safe Harbor

---

61 Schrems I, *supra* note 58, ¶ 25.

62 *Id.* at ¶ 49 ("Thus, the complaint relates specifically to transfers of personal data from Facebook Ireland to Facebook USA, while challenging more generally the level of protection ensured for such data under the safe harbour scheme.").

63 *Id.* at ¶ 183 ("Decision 2000/520 must be declared invalid since the existence of a derogation which allows in such general and imprecise terms the principles of the safe harbour scheme to be disregarded prevents in itself that scheme from being considered to ensure an adequate level of protection of the personal data which is transferred to the United States from the European Union.").

64 *Id.* at ¶ 143 ("Examination of the level of protection afforded by a third country must focus on two fundamental elements, namely the content of the applicable rules and the means of ensuring compliance with those rules.").

65 *Id.* at ¶ 164 ("The problem arises essentially from the United States authorities' use of the derogations provided for in that provision. Because their wording is too general, the implementation of those derogations by the United States authorities is not limited to what is strictly necessary.").

66 *Id.* at ¶ 155.

67 *Id.* at ¶ 159 ("Those findings of fact demonstrate, in my view, that Decision 2000/520 does not contain sufficient guarantees. Owing to that lack of guarantees, Decision 2000/520 has been implemented in a manner that does not satisfy the requirements of the Charter or of Directive 95/46.").

68 *Id.* at ¶ 164; *see also id.* at ¶ 46 ("In particular, the guarantee enshrined in Article 7 of the Charter and by the core values common to the traditions of the Member States would be compromised if the public authorities were allowed access to electronic communications on a casual and generalised basis without the need for objective justification based on considerations of national security or the prevention of crime specific to the individuals concerned and attended by appropriate and verifiable safeguards.").

Framework.[69] U.S. businesses had to rely on Standard Contract Clauses, Binding Corporate Clauses, or Article 49 derogations to maintain their transatlantic data flows. Not surprisingly, this decision was met with harsh criticism from the U.S. government.[70] However, the pressure to maintain the Transatlantic Economy did encourage some substantial changes in U.S. law.[71] Despite the initial criticism, the U.S. quickly adapted to restore their compliance status, resulting in a new and improved international trade agreement.

C. The Privacy Shield

The EU-U.S. Privacy Shield Framework ("Privacy Shield") developed after the *Schrems I* decision and addressed the Safe Harbor Framework's weaknesses and imposed stronger obligations on U.S. businesses.[72] As seen during the implementation of the Safe Harbor Framework, the U.S. negotiated this agreement to provide an adequate level of protection under U.S. law and maintain the Transatlantic Economy. This new international trade agreement

69 *Id.* at ¶ 237.

70 WEISS & ARCHICK, *supra* note 9, at 8; *see also Statement from U.S. Secretary of Commerce Penny Pritzker on European Court of Justice Safe Harbor Framework Decision*, U.S. DEP'T. OF COM. (Oct. 6, 2015), https://2014-2017.commerce.gov/news/press-releases/2015/10/statement-us-secretary-commerce-penny-pritzker-european-court-justice.html ("We are deeply disappointed in today's decision from the European Court of Justice, which creates significant uncertainty for both U.S. and EU companies and consumers, and puts at risk the thriving transatlantic digital economy. Among other things, the decision does not credit the benefits to privacy and growth that have been afforded by this Framework over the last 15 years.").

71 *See generally* Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (2016) ("This bill authorizes the Department of Justice (DOJ) to designate foreign countries or regional economic integration organizations whose natural citizens may bring civil actions under the Privacy Act of 1974 against certain U.S. government agencies for purposes of accessing, amending, or redressing unlawful disclosures of records transferred from a foreign country to the United States to prevent, investigate, detect, or prosecute criminal offenses.").

72 *See* Privacy Shield Framework, *Key New Requirements: EU-U.S. Privacy Shield Framework, Key New Requirements for Participating Companies*, PRIVACY SHIELD, https://www.privacyshield.gov/Key-New-Requirements (last visited Nov. 13, 2021) for the key new requirements for participating companies, including: informing individuals about data processing, providing free and accessible dispute resolution, cooperating with the Department of Commerce, maintaining data integrity and purpose limitation, ensuring accountability for data transferred to third parties, transparency related to enforcement actions, and ensuring commitments are kept as long as data is held.

reinforced the basic privacy principles with stronger commitments and requirements from the U.S.[73]

Although the Privacy Shield is built upon the same principles as Safe Harbor,[74] the Privacy Shield now requires statements clarifying the method of enforcement of the principles, a new avenue for redress for EU citizens, and stricter onward transfer limitations.[75] More specifically, the U.S. developed an "Ombudsperson Mechanism" for complaints on possible access from intelligence agencies.[76] This independent office was created within the U.S. State Department with the specific purpose of providing redress to EU citizens.[77] The U.S. Department of Justice and Office of the Director of National Intelligence both gave written promises of their commitment to the safeguards of the Privacy Shield in a published white paper, directly addressing the concerns raised by the CJEU.[78]

However, the Privacy Shield is not without faults. Some suggest that the "new and improved" agreement is not different enough from its predecessor, often referring to the Privacy Shield as the same agreement under a new name.[79] The Article 29 Working Party expressed concern that U.S. verbal commitments are

---

73 Behnam Dayanim & Sherrese M. Smith, *Five Ways the Privacy Shield is Different from Safe Harbor and Five Simple Steps Companies Can Take to Prepare for Certification*, PAUL HASTINGS (July 14, 2016), https://www.paulhastings.com/insights/client-alerts/five-ways-that-privacy-shield-is-different-from-safe-harbor-and-five-simple-steps-companies-can-take-to-prepare-for-certification.

74 *See id.* ("The Privacy Shield principles are largely the same as Safe Harbor and include Notice, Choice, Access, Security, Onward Transfer, Data Integrity/Purpose Limitation, and Redress. However, Privacy Shield policies must include statements regarding the enforcement body, a new arbitration right, disclosures to public authorities, and the company's liability for onward transfers.").

75 *See id.*; WEISS & ARCHICK, *supra* note 9, at 10.

76 *Privacy Shield Ombudsperson*, U.S. DEP'T OF STATE, https://www.state.gov/privacy-shield-ombudsperson/ (last visited Nov. 13, 2021). The Privacy Shield Ombudsperson will work closely with appropriate officials from other departments and agencies. The Ombudsperson is independent from the Intelligence Community. The Ombudsperson reports directly to the Secretary of State who will ensure that the Ombudsperson carries out its function objectively and in accordance with the Ombudsperson Mechanism Implementation Procedures. *Id.*

77 *See* WEISS & ARCHICK, *supra* note 9, at 10.

78 *Id.*

79 Schrems, while commenting on the Privacy Shield agreement, stated: "The EU and the U.S. tried to put about 10 layers of lipstick on a pig, but the core problems were obviously not solved." David Gilbert, *Safe Harbor 2.0: Max Schrems Calls 'Privacy Shield' National Security Loopholes 'Lipstick on a Pig,'* INT'L BUS. TIMES (Feb. 26, 2016), https://www.ibtimes.com/safe-harbor-20-max-schrems-calls-privacy-shield-national-security-loopholes-lipstick-2327277. Others drew more of a distinction: "At first glance, the Shield bears a strong resemblance to Safe Harbor, which misled some commentators to denounce it as a mere duplicate in disguise." Sotirios Petrovas, Cynthia J. Rich, & Bastiaan Suurmond, *Privacy Shield vs. Safe Harbor: A Different Name for an Improved Agreement?*, SOCIALLY AWARE (Morrison Foerster) April 2016, https://media2.mofo.com/documents/160428sociallyaware.pdf.

insufficient to reconcile its inadequacy and inability to provide essentially equivalent protection under domestic law.[80] Specifically, they took issue with the redress mechanisms, finding them too complex to address violations of data protection and privacy rights in a timely manner.[81] Ultimately, it was only a matter of time before history repeated itself. Two years following the implementation of the Privacy Shield, the GDPR became effective, providing the perfect opportunity for Schrems to return to the CJEU to question the U.S.'s adequacy under the new data protection and privacy laws in the EU.

III. *SCHREMS II*

Following the implementation of the Privacy Shield and the GDPR, Maximillian Schrems again challenged the adequacy of U.S. data protection and privacy laws, citing continuing concerns over the U.S. Government's surveillance efforts.[82] Ultimately, the CJEU agreed, invalidated the Privacy Shield, and found the U.S. inadequate for a second time.[83] *Schrems II* addressed issues of the interpretation and validity of SCCs[84] and the interpretation and validity of the

80 WEISS & ARCHICK, *supra* note 9, at 10-12; *see also* ARTICLE 29 WORKING PARTY, OPINION 01/2016 ON THE EU-U.S. PRIVACY SHIELD DRAFT ADEQUACY DECISION 57 (Apr. 13, 2016), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640157. ("The first concern is that the language used in the draft adequacy decision does not oblige organisations to delete data if they are no longer necessary. . . . Secondly, the WP29 understands from Annex VI that the U.S. administration does not fully exclude the continued collection of massive and indiscriminate data. . . . The third point of concern regards the introduction of the Ombudsperson mechanism.").

81 The Article 29 working party recognized "overly complex redress mechanisms" as a "strong concern" when commenting on the Privacy Shield Agreement. WEISS & ARCHICK, *supra* note 9, at 11.

82 *See* Case C-311/18, Maximillian Schrems v. Facebook Ireland, Ltd., ECLI:EU:C:2020:559, ¶ 55 (July 16, 2020), [hereinafter "Schrems II Judgement"]; *see also* Section 702 of the Foreign Intelligence Surveillance Act, also known as "Bush's warrantless wiretapping program," allows the U.S. government to wiretap communications between a foreign target and an American inside the U.S. Executive Order 12333 allows the NSA to conduct electronic surveillance overseas, allowing for "bulk collection" of American communication and data. Section 215 of the Patriot Act, passed after the 9/11 terrorist attacks, allows the NSA to collect "'any tangible thing' from third parties (such as telephone companies) if it could persuade the FISA Court that the item was "relevant" to a foreign intelligence investigation." *Foreign Intelligence Surveillance (FISA Section 702, Executive Order 12333, and Section 215 of the Patriot Act): A Resource Page*, BRENNAN CENTER FOR JUST. (Oct. 25, 2018), https://www.brennancenter.org/our-work/research-reports/foreign-intelligence-surveillance-fisa-section-702-executive-order-12333.

83Schrems II Judgement, *supra* note 83, at ¶ 203.

84 Case C-311/18, Maximillian Schrems v. Facebook Ireland, Ltd., ECLI:EU:C:2019:1145, ¶ 21 (Dec. 19, 2019), [hereinafter "Schrems II Opinion"].

Privacy Shield[85] under the GDPR and the EU Charter.[86] The CJEU upheld the validity of SCCs as an "effective mechanism" for the transfer of personal data to third party countries[87] and invalidated the Privacy Shield.[88]

Despite recognizing the limitations of SCCs, the CJEU upheld their validity in light of the GDPR and EU Charter provisions.[89] The CJEU focused on the ability of SCCs to ensure protection equivalent to the level of the GDPR and EU Charter in other countries.[90] The CJEU reasoned that the purpose of SCCs is only to provide "contractual guarantees that apply uniformly in all third countries."[91] SCCs impose an obligation on the parties to the contract to verify, prior to data transfers, that the level of protection in the target country is equivalent to that afforded under the GDPR and EU Charter.[92] Further, the GDPR encourages countries to "provide additional safeguards . . . that supplement standard [data] protection clauses" when SCCs do not afford adequate protection alone.[93] SCCs, the court reasoned, inherently ensure adequate protection in the country through its verification obligation, even though they do not specifically bind the country to their terms.[94]

In addressing the Privacy Shield, the CJEU focused significantly on the U.S.' commitment to the principles of the agreement. The agreement stated that U.S.' adherence to the principles is limited "to the extent necessary to meet national security, public, or law

85 Schrems II Judgement, *supra* note 83, at ¶ 43.

86 *Id.* at ¶ 1.

87 *Id.* at ¶ 148 ("The SCC Decision provides for effective mechanisms which, in practice, ensure that the transfer to a third country of personal data pursuant to the standard data protection clauses in the annex to that decision is suspended or prohibited where the recipient of the transfer does not comply with those clauses or is unable to comply with them.").

88 *Id.* at ¶ 199.

89 *Id.* at ¶ 148 ("It follows that the SCC Decision provides for effective mechanisms which, in practice, ensure that the transfer to a third country of personal data pursuant to the standard data protection clauses in the annex to that decision is suspended or prohibited where the recipient of the transfer does not comply with those clauses or is unable to comply with them.").

90 *Id.* at ¶ 129.

91 *Id.* at ¶ 133.

92 *Id.* at ¶ 142.

93 *Id.* at ¶ 132.

94 *See id.* at ¶¶¶ 136, 137, 142.

enforcement requirements."[95] In other words, any time Privacy Shield obligations conflict with U.S. national security, public interest, or law enforcement requirements, the U.S. could entirely ignore the Privacy Shield and data protection and privacy of EU citizens.[96] The Privacy Shield also did not provide "any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter."[97] Thus, the Privacy Shield was incompatible with the GDPR and EU Charter and was therefore an invalid means of transferring and maintaining EU citizen personal data.

This decision highlights the struggle of enforcing EU law on an international scale, especially with countries such as the U.S. that have a fundamentally different approach to domestic law. Now that transfers under the Privacy Shield are illegal, U.S. businesses are struggling to maintain their transatlantic data flows through SCCs and other means.[98] Data transfers through SCCs may require undefined "supplemental protections" and verification of compliance on a case-by-case basis, making SCCs costly and time consuming to administer.[99] Further, the EU granted no grace period for this

95 *Id.* at ¶ 164; *see also* U.S. DEP'T OF COM., EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES 2, https://www.statewatch.org/media/documents/news/2016/mar/eu-us-com-privacy-shield-annex2.pdf.

96 Schrems II Judgement, *supra* note 83, at ¶ 164.

97 *Id.* at ¶ 197.

98 *EDPB Publishes FAQs on Implications of the Schrems II Case*, Hunton Andrews Kurth: Priv. & Info. Sec. L. Blog (July 24, 2020), https://www.huntonprivacyblog.com/2020/07/24/edpb-publishes-faqs-on-implications-of-the-schrems-ii-case/ ("There is no grace period for companies that relied on the EU-U.S. Privacy Shield framework during which they can continue transferring data to the U.S. without assessing the legal basis relied on for those transfers. Transfers based on the EU-U.S. Privacy Shield framework are now, according to the EDPB, illegal.").

99 "Whether or not you can transfer personal data on the basis of SCCs will depend on the result of your assessment, taking into account the circumstances of the transfers, and supplementary measures you could put in place. The supplementary measures along with SCCs, following a case by-case analysis of the circumstances surrounding the transfer, would have to ensure that U.S. law does not impinge on the adequate level of protection they guarantee." EUROPEAN DATA PROTECTION BOARD, FREQUENTLY ASKED QUESTIONS ON THE JUDGEMENT OF THE COURT OF JUSTICE OF THE EUROPEAN UNION IN CASE C-311/18 – DATA PROTECTION COMMISSIONER V FACEBOOK IRELAND LTD AND MAXIMILLIAN SCHREMS 3 (July 23, 2020), https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/07/20200724_edpb_faqoncjeuc31118.pdf.

transition, significantly intensifying the effect of the outcome on U.S. business compliance.[100]

IV. DATA PROTECTION AND PRIVACY AFTER *SCHREMS II*

A. Standing the Test of Time – SCCs, BCRs, and Article 49 Derogations

With another international trade agreement invalidated, the U.S. is left with few options to continue transatlantic data transfers without significant changes to its domestic law to achieve an agreeable adequacy decision. SCCs, BCRs, and Article 49 derogations have survived as valid methods of maintaining adequate protection. However, they have not been accepted as the preferred system of data transfers, as demonstrated by the U.S.'s continuing desire to enter into international trade agreements instead.

BCRs are available only to companies established in the EU for internal data transfers to offices outside of the EU.[101] BCRs differ from SCCs, as companies create and submit the BCRs for approval in the EU once rather than on a case-by-case basis for each contract.[102] However, there are fourteen minimum requirements BCRs must specify, such as the rights of data subjects in regard to processing and the means to exercise those rights.[103] If the BCRs are approved, the submitting company can then utilize its BCRs to transfer data internationally while ensuring adequate data protection and privacy under the GDPR.[104] BCRs are preferred over SCCs because they can

100 "The implications of the unavailability of a grace period are serious for organizations, as interrupted data flows can create business disruptions for organizations on both sides of the Atlantic. This is particularly concerning given all of the other operational challenges and economic downturns that organizations are facing due to the coronavirus (COVID-19) pandemic." Pulina Whitaker, *No Grace Period After Invalidation of EU-US Privacy Shield in Schrems II*, MORGAN LEWIS (July 27, 2020), https://www.morganlewis.com/pubs/2020/07/no-grace-period-after-invalidation-of-eu-us-privacy-shield-in-schrems-ii.

101 European Commission, *supra* note 44.

102 *Id.*

103 GDPR, *supra* note 29, art. 47(2).

104 European Commission, *supra* note 44. For more info on the approval process, see ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT SETTING FORTH A CO-OPERATION PROCEDURE FOR THE APPROVAL OF "BINDING CORPORATE RULES" FOR CONTROLLERS AND PROCESSORS UNDER THE GDPR (Apr. 11, 2018), https://ec.europa.eu/info/files/working-document-approval-procedure-binding-corporate-rules-controllers-and-processors-wp263rev01_en.

be tailored to the specific business and are much easier to implement than numerous individual contracts.[105] This preferential method, is only available to companies with an established office in the EU, whereas SCCs can be used by any business, anywhere.[106]

SCCs provide a single set of rules that is applicable in the absence of an adequacy determination for all non-EU countries in the form of model contract clauses.[107] These clauses are pre-approved by the Commission and ensure compliance with requirements for safe data transfers.[108] There are two sets of SCCs: one "for use between controllers and processors",[109] and one "for the transfer of personal data to third countries.".[110] Both sets of SCCs were amended after the *Schrems II* judgement, allowing companies to ensure their compliance with the *Schrems II* decision and clearly understand the conditions under which SCCs can be used.[111] However, SCCs are not as easily utilized as their fill-in-the-blank format suggests. SCCs may not ensure complete adequacy, meaning that the use of SCCs may require independent supplementary measures to ensure adequacy

105 PRICEWATERHOUSECOOPERS, BINDING CORPORATE RULES 1, https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf (last visited Feb. 19, 2021).

106 Google, for example, has several data centers in EU member states, such as Finland, Netherlands, Denmark, Ireland, and Belgium. Google Data Centers, *Discover Our Data Center Locations*, https://www.google.com/about/datacenters/locations/ (last visited Nov. 13, 2021). Other large companies, such as TikTok, have since started building data centers within the EU so they would not have to transfer data outside of Europe. Leo Kelion, *TikTok to Open $500m Data Centre in Ireland*, BBC (Aug. 6, 2020), https://www.bbc.com/news/technology-53664997.

107 Press Release, *European Commission adopts new tools for safe exchanges of personal data*, EUROPA (June 4, 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

108 *Id.*

109Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, 2021 O.J. (L. 199), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0915&locale-en. Processors defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." GDPR, *supra* note 29, art. 4. "Controller" is defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." *Id.*

110 Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, 2021 O.J. (L. 199), https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en.

111 Press Release, *supra* note 108.

depending on the circumstances of the transfer.[112] Even so, some large companies, such as Google, rely on SCCs over international trade agreements.[113]

Article 49 derogations provide a method for international data transfers when there are no adequacy decisions, SCCs, or BCRs in place. However, Article 49 derogations can only be used for specific situations and under strict conditions. Under most of the listed methods, the data transfer must be "necessary"[114] for a specified and approved purpose, such as to exercise or defend legal claims.[115] There is also the option of explicit consent, which must be obtained from the data subject before the proposed transfer and after explaining the risks and safeguards in place.[116] If the international data transfer does not qualify for one of the listed derogations under Article 49, it still may occur, subject to even stricter conditions.[117]

---

112 *See* U.S. DEP'T OF COM., Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II 6 (Sept. 2020), https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF ("[C]ompanies transferring personal data from the EU to the United States may choose to rely on SCCs, which the ECJ expressly upheld in Schrems II with the caveat that companies are responsible for determining whether the law of the United States ensures adequate protection as afforded in EU law, including by providing, where necessary, additional safeguards.").

113 *See* Google, *Legal Framework for Data Transfers*, (Eff. Sep. 30, 2020), https://policies.google.com/privacy/frameworks?hl=en-US.

114 EUROPEAN DATA PROTECTION BOARD, GUIDELINES 2/2018 ON DEROGATIONS OF ARTICLE 49 UNDER REGULATION 2016/679 5 (May 25, 2018), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf ("One overarching condition for the use of several derogations is that the data transfer has to be 'necessary' for a certain purpose. The necessity test should be applied to assess the possible use of the derogations of Articles 49 (1) (b), (c), (d), (e) and (f). This test requires an evaluation by the data exporter in the EU of whether a transfer of personal data can be considered necessary for the specific purpose of the derogation to be used.").

115 GDPR, *supra* note 29, art. 49(1)(e).

116 *Id.* art. 49(1)(a) ("[T]he data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards").

117 *Id.* art 49(1) ("Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.").

Ultimately, an adequacy decision is the preferred method of compliance for all parties whether outside or inside the EU for numerous reasons. Although valid, BCRs, SCCs, and Article 49 derogations are more costly and time consuming to administer than an all-inclusive adequacy decision. Previously, the U.S. had avoided these limitations and alternate solutions through negotiating international trade agreements. However, as Maximillian Schrems has demonstrated, international trade agreements are temporary solutions to a permanent problem that is inherent in the fundamental differences of U.S. and EU domestic law. In the absence of a substantial overhaul of U.S. data protection and privacy laws, the U.S. is again struggling to balance its legal independence with the consequences of its inadequacy determination under EU law.[118]

B. U.S. Progression of Data Protection and Privacy – Current Legislation

Although there are certain fundamental aspects of U.S. law that inhibit the development of an overarching federal data protection and privacy law,[119] the U.S. has shown signs of progress in data protection and privacy laws that inch closer towards a more GDPR-like

118 U.S. DEP'T. OF COM., Letter from Deputy Assistant Secretary James Sullivan on the Schrems II Decision (Sept. 2020), https://www.commerce.gov/sites/default/files/2020-09/WhitePaperCoverLetterfromJamesSullivan.pdf ("The ECJ's ruling has generated significant legal and operational challenges for organizations around the world at a time when the ability to move, store, and process data seamlessly across borders has never been more crucial. Cross-border data flows have become indispensable to how citizens on both sides of the Atlantic live, work, and communicate. They power the international operations and growth of American and European businesses of every size and in every industry, and underpin the $7.1 trillion transatlantic economic relationship. Most importantly, they enable governments, private companies, and organizations worldwide to leverage the data sharing and collaborative research critical to understanding the COVID-19 virus, mitigating its spread, and expediting the discovery and development of treatments and vaccines.").

119 STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., DATA PROTECTION LAW: AN OVERVIEW (Mar. 25, 2019). There are certain fundamental aspects of U.S. law that inhibit the development of an overarching federal data protection and privacy law, including standing, preemption, and the First Amendment. With the implementation of a federal law, plaintiffs would need to establish Article III standing to pursue redress, a much higher and more difficult to reach standard than what is present in state courts. *Id.* at 59-61. There is also the issue of preemption. A new federal law must consider the state law already enacted in the U.S. and determine how to handle redress and conflict preemption to allow states to continue legislating in this area of law. *Id.* at 62-63. Lastly, the interpretation of the First Amendment can lead to possible challenges if the regulation of personal data and online communication is considered regulation of "speech." *Id.* at 64-69.

approach.[120] There are three bills currently introduced in Congress, with the purpose of increasing data protection and privacy in the U.S. They contain similar underlying principles to those the EU enforces with the authority of the GDPR.

The Consumer Online Privacy Rights Act, introduced in December 2019, would require the FTC to establish a new bureau to assist with enforcement of its provisions.[121] It would require entities that process or transfer personal data to make their privacy policy publicly available, provide access to personal data, delete or amend personal data upon request, establish data security practices, and designate a privacy officer to ensure compliance and run risk assessments.[122] Additionally, this bill would prohibit engaging in deceptive or harmful data practices and transferring data without consent and beyond what is reasonably necessary.[123]

The Consumer Data Privacy and Security Act of 2020, introduced in March 2020, similarly promises to establish a clear federal standard for data protection and privacy by providing a uniform standard.[124] However, this bill does not require the creation of a new enforcement body. Instead, it would "equip the FTC and state attorney general with authority to uniformly enforce federal consumer privacy protections while providing the FTC the resources necessary to carry out those authorities."[125]

Most recently, the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act ("the Safe Data Act") was introduced after the invalidation of the Privacy Shield in September of 2020.[126] This bill would provide the "rights to access,

120 See Sarah Cosgrove & Nagumotu, *2021 Proposed Comprehensive US Privacy Legislation*, INT'L. ASS. OF PRIVACY PROS., https://iapp.org/resources/article/2021-proposed-comprehensive-us-privacy-legislation/ (last updated Sept. 2021) for an overview of recent proposals of comprehensive federal privacy legislation and their proposed individual rights protections, business obligations, and enforcement.

121 S. 2968, 116th Cong. § 301(a)(1) (2019).

122 *Id.* § 102.

123 *Id.* § 101.

124 *Sen. Moran Introduced Landmark Federal Data Privacy Legislation* (Mar. 12, 2020), https://www.moran.senate.gov/public/index.cfm/news-releases?id=5C11EECE-DE43-4B2B-AEDE-76504D1D6186#:~:text=The%20Consumer%20Data%20Privacy%20and%20Security%20Act%20would%3A&text=prohibit%20companies%20from%20collecting%20data,from%20unauthorized%20access%20and%20disclosure.

125 *Id.*

126 S. 4626, 116th Cong. (2020).

notice, deletion, opting out, and correction" that are present in the GDPR.[127] Moreover, it would require express consent before processing and transferring personal data.[128] Like the Consumer Data Privacy and Security Act of 2020, and unlike the Consumer Online Privacy Rights Act, the Safe Data Act would empower the FTC to enforce its rules through injunctions and equitable remedies.[129]

Even with new legislation and an overarching federal data protection and privacy laws, it is not certain that the U.S. will attain adequacy under the GDPR.[130] Although U.S. law is progressing, it is not likely to immediately reach the very high standards of the EU. Indeed, while the progress is promising for both U.S. citizens and the Transatlantic Economy, it is still not enough to resolve the fundamental differences between U.S. and EU law, such as whether data protection and privacy is viewed as a human right.[131]

C. U.S. Data Privacy and Protection Under the Biden-Harris Administration

The *Schrems II* decision alone provides the opportunity for an overhaul of U.S. data protection and privacy laws, which may be achieved in one of many ways. However, this is not the only area of uncertainty that the U.S. faces in the evolution of its data protection

127 *Senate Republicans Stitch Together Safe Data Ideas into New Bill*, NAT'L L. REV. (Sept. 24, 2020), https://www.natlawreview.com/article/senate-republicans-stitch-together-safe-data-ideas-new-bill.

128 *Id.*

129 *Id.*

130 GDPR, *supra* note 29, recital 104 details conditions of attaining an adequacy determination: "The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress."

131 One fundamental difference between the EU Charter and the U.S. Constitution is how the entities declare rights: either in the positive or the negative. The EU explicitly declares privacy and data protection as human rights in their Charter, among 19 other positive fundamental human rights. U.S. citizens rely on the interpretation of the Supreme Court and case law for their right to privacy and negative freedoms to protect their recognized Constitutional human rights. *See Privacy Rights and Personal Autonomy*, *supra* note 11. This distinction is clearly demonstrated by the declaration of the freedom of expression. The EU Charter Article 11 states "everyone has the right to freedom of expression." EU Charter, *supra* note 28, art. 11. Whereas the U.S. Constitution's First Amendment states "Congress shall make no law … abridging the freedom of speech." U.S. CONST. amend. I.

and privacy laws. The effect of the *Schrems II* decision and subsequent invalidation of the Privacy Shield is made more pertinent by the timing of the decision: the beginning of a U.S. presidential term. With President Biden and Vice President Harris in the White House and a Democratic majority in the House and Senate, the U.S. is likely to experience a stronger focus on evolving data protection and privacy laws than with former President Trump.[132]

President Biden, former Vice President to President Obama, has a track record of advancing data protection and privacy policy.[133] The Obama Administration has experience addressing inadequacy decisions, as the Safe Harbor agreement was invalidated during Obama's term. In response, the Obama Administration enacted the Judicial Redress Bill, demonstrating a desire to cooperate and willingness to change U.S. law to meet the EU's demands.[134] Vice President Harris advanced California's data protection and privacy laws throughout her career as Attorney General.[135] During her tenure, the California's Attorney General's Office created the Privacy and

132 "Rather than pursuing a prescriptive model in which the government defines (or prescribes) data protection rules, the Trump Administration advocates for what it describes as an outcome-based approach whereby the government focuses on the outcomes of organizational practices, rather than on dictating what those practices should be." MULLIGAN & LINEBAUGH, *supra* note 120, at 52; *cf President Biden Signs Executive Order to Promote Fair Competition and Further Regulate Data Privacy*, HUNTON ANDREWS KURTH (July 23, 2021), https://www.huntonprivacyblog.com/2021/07/23/president-biden-signs-executive-order-to-promote-fair-competition-and-further-regulate-data-privacy/ ("Data privacy is a key concern addressed in the Executive Order, particularly the collection and aggregation of data and the surveillance of users. The Executive Order encourages the Federal Trade Commission to establish rules that regulate 'unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy.'").

133 *See* Dipayan Ghosh, *What Will Tech Regulation Look Like in the Biden Era?*, Harv. Bus. Rev. (Dec. 17, 2020), https://hbr.org/2020/12/what-will-tech-regulation-look-like-in-the-biden-era ("In 2012, the Obama administration passed the progressive Consumer Privacy Bill of Rights and pushed for a series of legislative proposals focused on protecting consumer privacy and children's privacy in educational contexts.").

134 *President Obama Signs Amended Judicial Redress Act of* 2015, Ass'n of Corp. Couns. (Dec. 18, 2015), https://advocacy.acc.com/advocacy_filing/president-obama-signs-amended-judicial-redress-act-of-2015/ ("On February 24, President Obama signed the Judicial Redress Act of 2015 into law, following its passage by congress in early February. The Act serves as a critical step in restoring trans-Atlantic personal data exchange following the invalidation of the Safe Harbor program by the European Court of Justice (ECJ) in October 2015.").

135 *See, e.g.*, Press Release, *Attorney General Kamala D. Harris Issues Guidance on Privacy Policies and Do Not Track Disclosures*, OFF. OF ATT'Y GEN. OF CALI. (May 21, 2014), https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-issues-guide-privacy-policies-and-do-not-track; Press Release, *Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit*, OFF. OF ATT'Y GEN. OF CALI. (July 19, 2012), https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection.

Enforcement and Protection Unit to enforce the California Consumer Privacy Act.[136]

President Biden and Vice President Harris seem to be willing to support the several bills currently working their way through Congress, inciting hope of a federal data protection and privacy law. This change in leadership could not have occurred at a more perfect time; U.S. businesses are looking to the U.S. government to support the Transatlantic Economy and provide a more permanent solution to the ongoing problems caused by temporary international trade agreements. With more support than ever and an expectation of a quick solution, the Biden-Harris Administration can advance U.S. data protection and privacy laws and strengthen the U.S.-EU relationship when it is needed most.[137]

CONCLUSION

Although an adequacy determination could end all the uncertainty and challenges facing the Transatlantic Economy, the it is unlikely that U.S. will reinvent its legal framework to come into compliance with the EU's commands. Ultimately, the best decision to address the differences inherent in the U.S. and EU's laws is one that balances the U.S.' independence and the success of the Transatlantic Economy: complying with EU law rather than replicating it.

136 Kristin Bryan et al., *Election 2020: Looking Forward to What a Biden Presidency May Mean for Data Privacy and Data Privacy Litigation*, NAT'L L. REV. (Nov. 12, 2020), https://www.natlawreview.com/article/election-2020-looking-forward-to-what-biden-presidency-may-mean-data-privacy-and; Lydia de la Torre et al., *What Biden Presidency May Mean for Data Privacy Litigation*, LAW360 (Nov. 30, 2020), https://www.law360.com/articles/1331148/what-biden-presidency-may-mean-for-data-privacy-litigation.

137 The timing of the *Schrems II* decision also lined up squarely with the global pandemic and spread of COVID-19. The UK Government published a response to the *Schrems II* decision, noting the importance of international data transfers in finding a cure and mitigating the consequences of COVID-19. "The recent crisis has shown how data transfers keep economies moving and societies functioning, being crucial to working from home, supporting a marked shift to communications and commerce moving online and underpinning the healthcare response." Dep't for Digital, Culture, Media & Sport, *UK Government Response to the European Court of Justice Decision in the Schrems II Case*, GOV.UK (July 17, 2020), https://www.gov.uk/government/news/uk-government-response-to-the-european-court-of-justice-decision-in-the-schrems-ii-case.

Progression of data protection and privacy laws has become increasingly important in today's digital world.[138] However, the U.S. must be allowed to adjust its laws on its own terms. As an independent and powerful nation, the U.S. does not have to answer to the EU's demands for a higher data protection and privacy standard. The GDPR requires a level of protection essentially equivalent to that afforded in the EU, not an identical legal framework. Thus, it is in the best interest of the U.S. to utilize the more reliable and consistent methods of compliance, such as SCCs, BCRs, and Article 49 derogations. These alternative methods for data transfers, although costly and time consuming, will allow the U.S. to continue progressing its laws on its own terms and honor its legal history and framework. Instead of overhauling data protection and privacy laws, the U.S. can encourage the use of SCCs, BCRs, and Article 49 derogations through government programs aimed at assisting businesses with their compliance.

As the U.S. advances its laws and gets closer to the GDPR standards, compliance through these means will only become easier. Although not the easiest or cheapest option, it provides the most stability and does not require reliance on international trade agreements that have been consistently overturned. Altering business practices to comply with SCCs, BCRs, and Article 49 derogations is the most permanent solution available that still allows the U.S. to maintain its power and authority over its own laws.

Most notably for the U.S., the new presidency provides an opportunity for substantial change. With several bills already at Congress's fingertips, current President Biden may finally get the U.S. an adequacy determination. Although it is unclear whether passing any of the several proposed acts will be enough for the EU's high standards, it is certainly the closest the U.S. will get to an adequacy decision. Ultimately, though, the EU retains its authority to reject and redetermine adequacy decisions. Even if there is an

138 *See* HAMILTON & QUINLAN, *supra* note 2, at 28 ("More than 5.19 billion people now use mobile phones, 4.5 billion people are now online, and 3.8 billion use social media. . . . Over the next three years, companies are expected to spend $7.4 trillion on digital transformation. In five years, digital ecosystems will account for more than 30% ($60 trillion) of global corporate revenue. By that time, an average connected person is likely to interact with Internet-of-Things (IoT) devices nearly 4,900 times a day – the equivalent of one interaction every 18 seconds.").

adequacy decision now, the U.S. can easily find itself pushed back again by the dominant force that is the EU's GDPR. No matter the solution the U.S. chooses to implement, the EU has undoubtedly influenced the advancement of U.S. data protection and privacy law.

Donna Calia[139]

139 Donna Calia is the Outreach Coordinator at the Washington University Global Studies Law Review and a J.D. Candidate at Washington University School of Law (2022).