CAN'T TOUCH THIS: HOW THE EUROPEAN UNION IS KEEPING ITS CITIZENS' DATA FROM REACHING THE UNITED STATES

Kendall R. Pipitone[*]

ABSTRACT

If you are an internet user, there is no doubt that some portion of your personal data—including shopping habits and website engagement—is being held by public and/or private entities. It is almost impossible to browse a website without seeing a pop-up requiring the visitor to agree to the entities' privacy policy and terms of use. Although people historically have been unaware of their data being collected and even sold, the modern era of social media and the internet has begun to change that. People are becoming increasingly mindful and wary of the data they are sharing and with whom. While the fundamental right to privacy, especially regarding personal data held by entities both domestically and globally, has been widely recognized, ensuring its protection poses international problems proving difficult to resolve. Recent developments in international law have only exacerbated these issues, and the U.S. is struggling to keep up with E.U. privacy standards. For the U.S. to continue collecting and using international data, it will need to perform a serious overhaul of its federal data privacy and protection policies. This Article explores how the U.S. may do that.

 Kendall R. Pipitone received her J.D. from Elisabeth Haub School of Law at Pace University in 2021. She received her Bachelor of Science from Binghamton University in 2016.

TABLE OF CONTENTS

I. INTRODUCTION

It is no secret that public and private entities have access to collect, process, and redistribute personal data globally. It is almost impossible to visit a website nowadays that does not have a privacy policy or Cookies pop-up that requires users to agree to some form of terms of use. Historically, most people did not think twice about what data was being collected and how various entities were using that data. In the last few decades, the Internet has had a meteoric rise, leading to myriad technological advancements. During that time, the United States ("U.S.") and the European Union ("E.U.") have made various efforts to ensure that its citizens' right to privacy is being safeguarded and that their data is being protected.

Over time, the U.S. and the E.U. have increasingly recognized the fundamental right to privacy, more recently in regards to personal data held by entities both domestically and globally. While this right has been widely recognized, ensuring its protection poses problems proving ever more complicated to resolve. Recent developments in international law have made this area even murkier, and the U.S. is struggling to keep up with E.U. standards.

This Article explores data protection in the U.S. and the E.U., including the evolution of privacy protections in each, in addition to the efforts to provide cooperative protections between the two. Part I discusses the history and evolution of data privacy in the U.S. and the E.U., and how the philosophy of protecting the right to privacy differs between the two. Part II examines the evolution of mechanisms for the protection of data transferred between the E.U. and the U.S., including various attempts at achieving sufficient and successful frameworks. Part III analyzes the latest development set forth by

the recent *Schrems II* case, and how it has left a certain degree of global uncertainty in its wake. Finally, Part IV offers criticisms and suggestions on how the U.S. and E.U. may move forward in their quest for data protection and compliance.

II. DATA PRIVACY HISTORY AND BACKGROUND

A. Data Privacy in the U.S.

In colonial America, there were common law protections against eavesdropping and trespass, but no formal recognition of a right to privacy.[1] Increased press production and advancements in technology, including more sophisticated cameras, eventually led to the formulation and development of the right to privacy, otherwise coined as the "right to be let alone."[2] Since 1890, the U.S. began to recognize "privacy torts" protecting individuals' rights to lead "secluded and private" lives.[3] Recognition and enforcement of these torts varied widely by state, but constitutional law has developed alongside state law to recognize the right of privacy for Americans, protecting citizens against governmental intrusions, including where the citizens' information is shared with third parties.[4]

In 1977, the Supreme Court recognized that the constitutional right to privacy necessarily constitutes individual interest in avoiding disclosure of personal matters.[5] However, the Supreme Court has struggled in defining the exact boundaries of this right, noting that states may sometimes have legitimate governmental interests in obtaining and sharing the individual's information.[6]

In efforts to give firmer protection, the federal government slowly began establishing a "patchwork" of laws to provide citizens statutory protection of their personal information.[7] For example, the Gramm-Leach-Bliley Act ("GLBA") governs data protection obligations of financial institutions, focusing on consumers' nonpublic personal information; the Health Insurance

---

[1] STEPHEN P. MULLIGAN ET AL., DATA PROTECTION LAW: AN OVERVIEW 3 (Cong. Rsch. Serv. ed., 2019) [hereinafter CRS DATA PROTECTION LAW REPORT].

[2] *See id.* at 3–4.

[3] *Id.* at 4.

[4] *E.g.*, *id.* at 4–5; Katz v. United States, 389 U.S. 347 (1967) (recognizing reasonable expectation of privacy in a phone booth); Whalen v. Roe, 429 U.S. 589 (1977) (upholding the adequacy of the New York State Controlled Substances Act in protecting personal data shared between prescribing doctors, dispensing pharmacies, and the state department of health); Carpenter v. United States, 138 S. Ct. 2206 (2018) (holding that tracking someone via their phone records violated their right to privacy).

[5] *See Whalen*, 429 U.S. at 598–99.

[6] *E.g.*, *id. at* 604–06; *see* Nixon v. Adm'r. of Gen. Servs., 433 U.S. 425, 455 (1977).

[7] CRS DATA PROTECTION LAW REPORT, *supra* note 1, at 7.

Portability and Accountability Act ("HIPAA") governs protections of medical information; the Electronic Communications Privacy Act ("ECPA") governs protections of electronic communications including obligations of governmental *and* non-governmental actors.[8] Notably, there is no overarching federal framework on data privacy generally.[9]

The U.S. protections of the right to privacy generally focus on governmental intrusions into private life.[10] However, the European Union focuses more on *any* intrusion and accumulation of personal data, providing much broader, far-ranging protection.[11]

B. Data Privacy in the E.U.

In the 1970s, European countries initially began enacting national statutes on data protection.[12] However, these statutes differed between States, resulting in different privacy and protection standards, and thus restricting the flow of information between European countries.[13]

In response to this restriction, the E.U. enacted the 1995 Directive of the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the "Data Protection Directive").[14] This Data Protection Directive applied across the E.U. while simultaneously giving individual countries the ability to implement their own requirements into national laws, thereby maintaining some degree of individual State sovereignty.[15] By 2012, however, the different implementations by different States proved problematic.[16] As a result, the E.U. began moving to develop a single regulation to reduce or eliminate fragmentation and to keep current with technological advancements.[17]

Between 2016 and 2018, the 1995 Data Protection Directive was replaced with the enactment of the General Data Protection Regulation (the "GDPR").[18] The GDPR regulates the processing of personal data—including

---

[8] *Id.* at 8, 10, 25.

[9] Christopher Hart, *What Is Data Privacy?*, NE. UNIV. GRADUATE PROGRAMS BLOG (Nov. 26, 2019), https://www.northeastern.edu/graduate/blog/what-is-data-privacy/.

[10] CRS DATA PROTECTION LAW REPORT, *supra* note 1, at 40; *see* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1728 (2020).

[11] CRS DATA PROTECTION LAW REPORT, *supra* note 1, at 40; Hartzog & Richards, *supra* note 10, at 1729.

[12] CRS DATA PROTECTION LAW REPORT, *supra* note 1, at 41.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*; Jonathan McGruer, *Emerging Privacy Legislation in the International Landscape: Strategy and Analysis for Compliance*, 15 WASH. J. L. TECH. & ARTS 120, 121 (2020).

collection, use, storage, organization, disclosure, etc.—within certain territorial limits.[19] The GDPR contains seven key principles.[20] Essentially, these principles require any data collection and/or processing to be lawful, transparent, and fair, and the data must be collected for a specific legitimate purpose.[21] Data collection must be limited to what is adequate and relevant to achieving the purpose it is being collected for, must be kept only for as long as necessary to achieve that purpose, and must be kept in such a way so that it is readily identifiable and protected against unauthorized processing, loss, or destruction.[22] The data must also be accurate, and individuals have the right to correct any inaccurate data or erase the data entirely.[23] Finally, the entity that holds the data has the responsibility of ensuring compliance with the GDPR.[24]

Tracking its guiding principles, the GDPR also provides for corresponding rights of individuals and related obligations of those who control the data.[25] The rights afforded to individuals are the rights to access, rectify, erase, restrict, and object to any data collected, and the right to obtain any data previously collected and/or processed.[26]

Additionally, the GDPR allows data transfers from the E.U. to a non-E.U. country if the receiving country ensures adequate levels of personal data protection that are "essentially equivalent" to those of the GDPR.[27] Because the E.U. framework of data protection is much more cohesive and stringent than the U.S.' "patchwork" of federal data protection, the U.S. and the E.U. have struggled to establish a sufficient framework equivalent to that of the GDPR for safeguarding data being shared between them.

III. EVOLUTION OF MECHANISMS FOR THE PROTECTION OF PERSONAL

---

[19] Council Regulation 2016/679, art. 4, 2016 O.J. (L 119) 1, 33 (EU) [hereinafter GDPR]; CRS DATA PROTECTION LAW REPORT, *supra* note 1, at 42.

[20] CRS DATA PROTECTION LAW REPORT, *supra* note 1, at 43 (listing the following principles: (1) lawfulness, fairness, and transparency, (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality; (7) accountability).

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.* at 44.

[26] *Id.* at 45–46; GDPR, *supra* note 19, at 39–46.

[27] CRS DATA PROTECTION LAW REPORT, *supra* note 1, at 48.

DATA SHARED BETWEEN THE E.U. AND THE U.S.

A. Safe Harbor

In 2000, following the enactment of the 1995 Data Protection Directive, the U.S. and the E.U. developed a legal framework, called Safe Harbor, for protecting personal data being transferred from the E.U. to the U.S.[28] This framework requires U.S. companies to self-certify with the Department of Commerce that they comply with the established Safe Harbor Principles and the corresponding requirements.[29] The Federal Trade Commission enforces the promises of these companies that they are compliant with the framework.[30] The seven Safe Harbor Principles are as follows.

First, *notice*, which requires the organization to notify individuals about why they are collecting and using the information, and providing information on how the individual may contact the organization with questions or complaints.[31] Second, *choice*, which requires organizations to give individuals the chance to choose, or opt-out of, whether their personal information is disclosed to third parties.[32] Third, *onward transfer*, which requires organizations to apply the notice and choice principles in disclosing information to third parties and ensure the third party also subscribes to the Safe Harbor Principles or is otherwise subjected to the 1995 Data Protection Directive.[33]

Fourth, *access*, which requires organizations to give individuals access to their personal information and opportunities to correct, amend, and/or delete the inaccurate information.[34] Fifth, *security*, which requires organizations to take reasonable precautions to safeguard personal information from loss, misuse, unauthorized access, disclosure, alteration, and/or destruction.[35] Sixth, *data integrity*, which requires the personal data to be relevant for the purposes it is being used for.[36] Seventh, *enforcement*, which requires the organization to have recourse mechanisms available to investigate and resolve complaints and disputes, procedures for verifying organizations'

---

[28] *Federal Trade Commission Enforcement of the U.S.–EU and U.S.–Swiss Safe Harbor Frameworks*, FED. TRADE COMM'N (July 25, 2016), https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor.

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id.*

commitments to adherence to the Safe Harbor Principles, and remedies for failure to comply with the Principles.[37]

In 2000, the Commission of the European Communities decided the so-called "Safe Harbor Decision," upholding the adequacy of the Safe Harbor Principles and framework in protecting data being transferred from the E.U. to the U.S.[38] The Commission also recognized that these Principles could be limited to the extent necessary to ensure national security, public interest, or law enforcement requirements.[39] In 2013, unauthorized data transfers of the National Security Agency ("NSA") surveillance programs and allegations of other U.S. intelligence activity in Europe exacerbated European concerns over the adequacy of U.S. data protection.[40]

In 2015, the Court of Justice of the European Union (the "CJEU" or "Court") invalidated the Safe Harbor framework in *Maxmillian Schrems v. Data Protection Commissioner and Digital Rights Ireland, Ltd.*—also known as "*Schrems I*."[41] Maximillian Schrems, the applicant, objected to the transfer of his personal data from Facebook Ireland to the U.S.,[42] arguing that the U.S. did not offer adequate protections to E.U. citizens.[43] The Court held that "adequate" levels of protection require the U.S. to "ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union…"[44] In ensuring these adequate levels of protection, the Court is entitled—and, in fact, obligated—to revisit previous decisions and findings relating to such adequacy and "check" that the decision and/or finding is "still factually and legally justified."[45] The Court thus revisited the Safe Harbor Decision of 2000.

In finding that the Safe Harbor Decision was invalid, the Court established that the Decision merely decided the adequacy of protection in the U.S. under the Safe Harbor Principles without any sufficient findings in relation to measures by which the U.S. actually *ensures* adequate levels of protection by way of domestic law or international commitments.[46] The Court

---

[37] *Id.*

[38] Commission Decision 2000/520, art. 1, 2000 O.J. (L 215) 7, 8 (EC) [hereinafter Safe Harbor Decision].

[39] *Id.* ¶¶ 50–52; MARTIN A. WEISS & KRISTIN ARCHICK, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 5 (Cong. Rsch. Serv. ed., 2016) [hereinafter CRS PRIVACY SHIELD].

[40] CRS PRIVACY SHIELD, *supra* note 39, at 8.

[41] Case C–362/14, Maximillian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶ 107 (Oct. 6, 2015).

[42] Maximillian Schrems v. Data Prot. Comm'r, 2015 ECLI ¶¶ 2, 28.

[43] *See id.* ¶¶ 28, 67.

[44] *Id.* ¶ 73.

[45] *Id.* ¶ 76.

[46] *Id.* ¶ 83.

states the Decision is also deficient in that it allows the U.S. to disregard the Safe Harbor Principles where they conflict with "national security, public interest, or law enforcement requirements," which have primacy over such Principles.[47] This means that where Safe Harbor Principles conflict with U.S. law, U.S. organizations must comply with domestic law, thereby allowing derogation from the Principles.[48] This level of protection clashes with E.U. standards whereby "protection of the fundamental right to respect for private life at [E.U.] level requires *derogations and limitations* in relation to the protection of personal data to apply *only in so far as is strictly necessary*."[49] That is, the E.U. imposes a much stricter standard than the U.S.

This decision was likely a result of the fact that the Safe Harbor Principles and the Safe Harbor Decision were implemented and decided in 2000, when the internet was still in its infancy stages.[50] Since 2000, various technological advancements have been made, including the spectacular rise of social media sites like Facebook (discussed in *Schrems I*) and others like Instagram, Twitter, etc., all of which obtain and retain users' personal information for their own use and for the use of advertising.[51] Concerns have thus, understandably, changed, and with that standards for data protection and privacy have also changed.

In 2016, in response to *Schrems I*, U.S. and E.U. officials announced the replacement of the Safe Harbor Principles and framework with the U.S.-E.U. Privacy Shield.[52]

B. The U.S.-E.U. Privacy Shield

The U.S.-E.U. Privacy Shield framework was more extensive and more robust than Safe Harbor.[53] It maintained the seven Safe Harbor Principles but added provisions on "sensitive data, secondary liability, the role of data protection authorities, human resources data, pharmaceutical and medical products, and publicly available data."[54] Unlike Safe Harbor, the Privacy Shield contained specific commitments from the U.S. concerning protections afforded to data obtained from the E.U.[55] and had a model for arbitrating

---

47 *Id.* ¶ 86.

48 *Id.* ¶ 85.

49 *Id.* ¶ 92 (emphasis added).

50 *See* CRS PRIVACY SHIELD, *supra* note 39, at 1.

51 Kalev Leetaru, *What Does It Mean For Social Media Platforms To "Sell" Our Data?*, FORBES (Dec. 15, 2018, 3:56 PM), https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=5c301dc22d6c.

52 CRS PRIVACY SHIELD, *supra* note 39, at 1.

53 *Id.* at 9.

54 *Id.*

55 *Id.* at 9–10.

disputes.[56] Essentially, the U.S. and the E.U. addressed the CJEU's concerns by enhancing commitments from the U.S., creating stronger enforcement mechanisms, establishing clear safeguards and transparency obligations, and protecting E.U. citizens' rights with several redress possibilities.[57]

In 2016, the European Commission issued an Implementing Decision whereby it stated that the U.S. had rules in place to limit interference on individuals' right to privacy for law enforcement or public interest purposes to what is strictly necessary to achieve legitimate objectives and ensure legal protection.[58] Because these limits and protections were in place, the Commission found that the U.S. *did* ensure adequate levels of protection for E.U. citizens' personal data being transferred there.[59]

The Privacy Shield was written and promulgated with the GDPR in mind and was designed to preemptively ensure that U.S. companies comply with GDPR requirements.[60] Although all seemed well for a period of time, the CJEU once again turned data privacy on its head with its 2020 decision in *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems* ("*Schrems II*").

IV. *SCHREMS II* AND THE UNCERTAINTY LEFT IN ITS WAKE

In 2015, after *Schrems I* was decided, Maximillian Schrems relodged his complaint against Facebook Ireland for transferring data to Facebook Inc., which then made the data available to U.S. authorities like the NSA and Federal Bureau of Investigation ("FBI").[61] Schrems argued for the prohibition or suspension of transfers of his personal data to the U.S. due to the inadequacy of data protection.[62] The CJEU assessed the validity of the Privacy Shield Decision and the adequacy of U.S. levels of protection in light of Article 47 of the GDPR as it pertains to Articles 7, 8, and 47 of the Charter of Fundamental Rights of the European Union (the "Charter").[63]

---

[56] *Id.* at 10.

[57] *Id.*

[58] Commission Decision 2016/1250, 2016 O.J. (L 207) ¶ 135 (EU) [hereinafter Privacy Shield Decision].

[59] *Id.* ¶ 136.

[60] *FAQs – General*, INT'L TRADE ADMIN.: PRIV. SHIELD PROGRAM, https://www.privacyshield.gov/article?id=General-FAQs (last visited Oct. 21, 2021).

[61] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., ECLI:EU:C:2020:559, ¶¶ 55, 57 (July 16, 2020).

[62] *Id.* ¶ 55.

[63] *Id.* ¶ 138.

A. GDPR and Charter Rights and Protections

Article 47 of the GDPR—under Chapter 5, which governs "[t]ransfers of personal data to third countries or international organisations"—states that companies may enact "binding corporate rules" ("BCRs") to allow data transfers from the E.U., provided that they comport with certain requirements.[64] The adequacy of these BCRs may be assessed by a "competent supervisory authority" to ensure consistent implementation across the E.U.[65]

Article 7 of the Charter reads: "Everyone has the right to respect for his or her private and family life, home and communications."[66] Article 8 of the Charter reads:

> Protection of personal data
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for *specified purposes* and *on the basis of the consent of the person concerned or some other legitimate basis laid down by law*. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall *be subject to control by an independent authority*.[67]

Article 47 of the Charter governs the right to a fair trial and effective remedy.[68]

The Court asserted that communication, retention, and access of personal data to a third party "constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter…"[69] The Court further recognized, however, that the rights set forth in Articles 7 and 8 of the Charter are not absolute and must be considered in light of their function in society.[70] To that end, as laid out in Article 8, personal data must be processed for "specified purposes and on the basis of the consent… or some other legitimate basis laid down by the law."[71] This means that limitations on the right of privacy are only valid where they are proportionate; specifically, limitations must be "necessary and genuinely meet objectives of general interest

---

64 *See* GDPR, *supra* note 19, at 60, 62–65.

65 *Id.* at 63.

66 Commission Regulation 2000/C, art. 7, 2000 O.J. (C 364) 1, 10 (EU) [hereinafter E.U. Charter].

67 *Id.* at 10.

68 *Id.* at 20.

69 Data Prot. Comm'r v. Facebook Ireland Ltd., 2020 ECLI ¶¶ 170–71.

70 *Id.* ¶ 172.

71 E.U. Charter, *supra* note 66, at 10.

recognized by the Union or the need to protect the rights and freedoms of others."[72] Because limitations on these fundamental rights to privacy must only apply in so far as strictly necessary, any legislation imposing such limitation must clearly and definitively convey the rules on the scope and application of the limitation, including the circumstances and conditions under which such limitation may apply.[73]

The Court, therefore, questioned the legitimacy of the Commission's Privacy Shield Decision on the grounds that the U.S. was not limiting interference on the right to privacy to the extent strictly necessary, as required by the principle of proportionality.[74]

B. Privacy Shield Invalidated but SCCs Upheld

The CJEU ultimately held that the Privacy Shield Decision, or hereby the Privacy Shield framework, was invalid because surveillance programs in the U.S. that were obtaining E.U. citizens' data were not tailored to what was strictly necessary under the proportionality doctrine.[75] These surveillance programs did not prescribe the precise rules on the scope and application of their limitations on the right to privacy, and otherwise fell short of guaranteeing a level of protection essentially equivalent to that guaranteed under the GDPR and Charter.[76]

The Court also found that there was no effective and sufficient remedy—equivalent to that of the E.U.—for people whose data was transferred to the U.S.[77] As set forth in Article 47 of the Charter, those whose rights and freedoms are violated have the right to an effective remedy before an independent and impartial tribunal.[78] Surveillance programs in the U.S. afforded no such redress in U.S. courts,[79] and the Ombudsperson Mechanism suggested by the U.S. was found to be imperfect because the Ombudsperson may not be independent and impartial.[80] The Ombudsperson is appointed by the Secretary of State, reports directly to the Secretary of State, and serves as an integral piece of the U.S. State Department, which suggests they may not

---

[72] Data Prot. Comm'r v. Facebook Ireland Ltd., 2020 ECLI ¶ 174.

[73] *Id.* ¶ 176.

[74] *Id.* ¶ 178; *see generally* E.U. Charter, *supra* note 66, at 21 ("Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.").

[75] Data Prot. Comm'r v. Facebook Ireland Ltd., 2020 ECLI ¶¶ 179–84.

[76] *See id.* ¶¶ 179–81.

[77] *See id.* ¶¶ 186–97.

[78] *Id.* ¶ 186; E.U. Charter, *supra* note 66, at 20.

[79] Data Prot. Comm'r v. Facebook Ireland Ltd., 2020 ECLI ¶ 192.

[80] *Id.* ¶¶ 193–95; *see generally* Privacy Shield Decision, *supra* note 58, ¶ 116 (providing information on the Ombudsperson Mechanism between the U.S. and E.U.).

be entirely independent from the Executive branch.[81] Additionally, the Ombudsperson is unable to issue binding decisions in regards to law enforcement and intelligence activity.[82] Because the U.S. fails to provide adequate redress essentially equivalent of that guaranteed in the E.U., the level of protection once again fails to pass muster.[83]

However, the U.S. is not left completely in the lurch. The Court upheld the validity of so-called "standard contract clauses" ("SCCs"), previously validated by the European Commission as potentially adequate to ensure U.S. compliance with E.U. data privacy protections.[84] With these SCCs, two or more entities engaging in transfers of data guarantee the receiving party will protect the personal data it is obtaining.[85] The U.S. also has the BCRs mentioned in Article 47 of the GDPR, which are considered the "gold standard" of international data transfers.[86] The main benefit of using BCRs is that a supervisory authority decides on the adequacy of the protection whereas SCCs require the user to decide (and they are thus responsible if they happen to be wrong).[87]

C. Reactions, Consequences, and Future Implications

After *Schrems II*, U.S. companies that previously relied on the Privacy Shield are left scrambling to figure out alternative mechanisms for ensuring protection of data flowing from the E.U.[88] The implications are far-ranging, thus impacting E.U.-U.S. and other global data transfers.[89] There may be effects on trade and data localization because the E.U.'s stringent standards

---

[81] Data Prot. Comm'r v. Facebook Ireland Ltd., 2020 ECLI ¶¶ 195–96.

[82] *Id.* ¶ 196.

[83] *Id.* ¶ 197.

[84] Commission Decision 2010/87, art. 1, 2010 O.J. (L 39) 5, 8 (EU) [hereinafter SCC Decision]; GDPR, *supra* note 19, at 62; *see* Data Prot. Comm'r v. Facebook Ireland Ltd., 2020 ECLI ¶ 203.

[85] Robert B., *Using Standard Contractual Clauses*, TERMSFEED (Jan. 18, 2021), https://www.termsfeed.com/blog/using-standard-contractual-clauses/.

[86] Lukas Feiler & Wouter Seinen, *BCRs as a Robust Alternative to Privacy Shield and SCCs*, THE INT'L ASS'N OF PRIV. PROS. (Jul. 23, 2020), https://iapp.org/news/a/binding-corporate-rules-as-a-robust-alternative-to-privacy-shield-and-sccs/; *see generally* GDPR, *supra* note 19.

[87] *Id.*

[88] Hunton Andrews Kurth, *BREAKING: Unexpected Outcome of Schrems II Case: CJEU Invalidates EU-U.S. Privacy Shield Framework but Standard Contractual Clauses Remain Valid*, PRIV. & INFO. SEC. L. BLOG (July 16, 2020), https://www.huntonprivacyblog.com/2020/07/16/breaking-unexpected-outcome-of-schrems-ii-case-cjeu-invalidates-eu-u-s-privacy-shield-framework-but-standard-contractual-clauses-remain-valid/.

[89] Rezzan Huseyin, *The CJEU's Hearing on Schrems II Signals Potential Chaos Ahead*, 19 PRIV. & DATA PROT. J. 2, 17 (2019).

preclude transfers to countries like the U.S., whose data protection frameworks are more relaxed.[90]

With little to no guidance from the Commission or CJEU, countries are left to determine how to ensure compliance with E.U. standards on their own.[91] Some have pinpointed lawful grounds for data transfer such as GDPR Article 49 derogations, BCRs, consent or necessity, and certification or codes of conduct.[92] Others have issued guidance on analysis of compliance, suggesting a step-by-step evaluation such as (1) identifying data flows and uses, (2) verifying GDPR applicability, (3) determining if data use is GDPR-compliant, (4) checking if the data remains within GDPR-compliant locations, and (5) evaluating the risk associated with the collected data.[93]

Taking these steps allows companies to identify and mitigate gaps in GDPR compliance, thereby reducing the risk of penalties.[94] However, until the U.S. enacts sweeping policy changes and a singular federal framework on data privacy and protection, U.S. companies are, for the most part, still at relatively significant risk.

V. CRITICISM AND SUGGESTIONS

The E.U. is performing its due diligence by ensuring that wherever its citizens' data is being sent has processing and protection standards that are as stringent as E.U. standards. This is how nations can ensure the increasing data flows do not endanger those whose data is being collected and shared. The outcome of *Schrems II* and the language of the GDPR tracks with the language of various international treaties as well as internal European treaties. For example, Article 8 of the E.U. Charter, discussed above, bestows upon all Europeans the right to protection of their personal data. Article 17 of the International Covenant on Civil and Political Rights ("ICCPR")—an

---

[90] Elisabeth Meddin, *The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade Violation of Articles XVI and XVII of the General Agreement on Trade in Services*, 35 AM. U. INT'L L. REV. 997, 1016–18 (2020); H. Jacqueline Brehmer, *Data Localization: The Unintended Consequences of Privacy Litigation*, 67 AM. U. L. REV. 927, 956 (2018); *see* Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 J. INT'L ECON. L. 771, 777 (2020).

[91] *See* Brian Hengesbaugh, et al., *Guidance Notes for Responding to 'Schrems II'*, THE INT'L ASS'N OF PRIV. PROS, https://iapp.org/resources/article/guidance-notes-for-responding-to-schrems-ii/ (last visited Oct. 21, 2021) (compiling a list of guidance notes on what to do and how to comply with the GDPR in light of Schrems II).

[92] *E.g.*, Chander, *supra* note 90, at 775–76; Jessica Shurson, *Data Protection and Law Enforcement Access to Digital Evidence: Resolving the Reciprocal Conflicts Between the EU and US Law*, INT'L J. L. & INFO. TECH. 167, 173 (2020).

[93] Zak Rubinstein, *Maintaining GDPR Compliance in the Wake of Schrems II*, CPO MAG. (Nov. 6, 2020), https://www.cpomagazine.com/data-protection/maintaining-gdpr-compliance-in-the-wake-of-schrems-ii/.

[94] *Id.*

international treaty to which the U.S. is a party—states: "[no] one shall be subjected to arbitrary or unlawful interference with his privacy…"[95] While this imposes a less stringent standard on the U.S. as the E.U. Charter and GDPR impose on the E.U., the ICCPR restricting data transfers to the U.S. that are at risk of abuse or misuse is still well within the E.U.'s rights. The onus is thus on the U.S. to rise to that standard in order to maintain international data flows.

Although the two previous frameworks have been deemed insufficient, the U.S. may still want to maintain the same seven key Principles from the Safe Harbor and Privacy Shield frameworks but elaborate on how to comply with E.U. standards now that they have been more clearly articulated in *Schrems II*. While there has been general silence and obscure guidance on how to achieve GDPR compliance,[96] it is clear that the U.S. needs to perform a complete overhaul of data protection and guarantees of privacy, including the establishment of better mechanisms for redress where these rights have been violated or impinged—an issue highlighted by the CJEU in *Schrems II*.

In performing this overhaul, the U.S. may want to take stock of what types of companies or entities are seeking to obtain E.U. citizens' data and what they are using it for. By compiling this data, the U.S. will be able to work backwards to ensure the ability to achieve their goals while meeting the E.U. standards. In the last few months, for example, users in the U.S. have no doubt seen an uptick in notifications on websites about Cookies and the requirement to opt-in or opt-out of data tracking in order to even view the whole website. The U.S. appears to be cracking down on its data privacy and protection, but more needs to be done.

Moreover, other countries have taken steps to increase their data privacy and protection laws and comply with the GDPR. Brazil has modeled its General Data Protection Law after the GDPR, containing similar scope and applicability, but with lower fines for non-compliance.[97] Japan has entered into a "reciprocal adequacy" agreement with the E.U., whereby there are whitelisted companies in each that are sufficiently cautious and provide adequate protections for personal data.[98] This agreement also provides E.U. citizens with a method of recourse for violations of data privacy rights by these Japanese companies (and vice versa).[99] India has modeled its Personal

---

[95] *See* International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, T.I.A.S. No. 92–908, 999 U.N.T.S. 171.

[96] *See* Andrea Jelinek, *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*, EUR. DATA PROT. BD. (July 23, 2020), https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.

[97] Dan Simmons, *12 Countries with GDPR–like Data Privacy Laws*, COMFORTE BLOG (Jan. 12, 2021), https://insights.comforte.com/12-countries-with-gdpr-like-data-privacy-laws

[98] *Id.*

[99] *Id.*

Data Protection Bill after the GDPR, although it has built in more leeway for the government to decide on its enforcement and when exceptions are permitted.[100] The U.S. may take any one (or more than one) of these approaches and strategies when deciding what to do to comply with the GDPR while retaining a certain level of autonomy.

Within the U.S., although there is no federal data privacy law applicable to all industries in the U.S., states have enacted their own laws, and California has made its data privacy laws such that they overlap with the GDPR.[101] The California Consumer Privacy Act ("CCPA") is one of the strictest state regulations in the U.S. and focuses on consumers' rights rather than the requirements organizations must abide by.[102] Some of these overlapping rights include the right to access, data portability, and deletion.[103]

Some scholars have offered reasons why the U.S. is loath to enact and enforce a GDPR-like instrument.[104] These reasons include the fact that there is no agency to enforce such an instrument, the instrument would be exceedingly difficult to get it through Congress, and there appears to be insufficient public demand for such data privacy overhaul.[105] While these reasons are valid, they are not insurmountable. For example, Facebook was recently in trouble for its transfers of user data between entities like Amazon, Yahoo, Spotify, and Bing.[106] Especially now, in light of the Facebook/Cambridge Analytica debacle, users are starting to delete their Facebook and Instagram accounts to prevent data misuse.[107]

While users may have been uninformed—and even unaware how uninformed they were—in the early days of internet literacy, users now know

---

[100] *Id.*

[101] *Id.*

[102] Jonathan Deveaux, *CCPA: Data Privacy like GDPR; Data Security like PCI DSS*, COMFORTE BLOG (Oct. 16, 2019), https://insights.comforte.com/ccpa-data-privacy-like-gdpr-data-security-like-pci-dss.

[103] *Id.*

[104] Derek Hawkins, *The Cybersecurity 202: Why a Privacy Law like GDPR Would Be a Tough Sell in the U.S.*, WASH. POST (May 25, 2018, 8:14 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/.

[105] *Id.*

[106] Gabriel J.X. Dance et al., *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html.

[107] Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html; *see* Kate O'Flaherty, *Facebook Users Have 3 Superb Reasons to Quit in 2021*, FORBES (Jan. 10, 2021, 9:17 AM), https://www.forbes.com/sites/kateoflahertyuk/2021/01/10/facebook-users-have-3-superb-reasons-to-quit-in-2021/?sh=365746f62119.

that many of the websites and apps they use on a daily basis are, in one way or another, collecting their data. Furthermore, these websites and apps are even sharing the data with each other.[108] Users search the internet for a garden hose once, and within minutes they are confronted with advertisements for garden hoses on all other sites or applications they open. This is not a coincidence.

Companies collect and use user data—whether it be personal data or data related to how the users engage with a website including behavioral information such as transactional details and history—to improve how their websites operate, enhance their consumer experience, and refine their marketing and advertising strategies.[109] Companies rely on data mining corporations like Oracle to compile and use user data to target users with relevant advertisements.[110] However, a new feature on Oracle's site is the following message on the corporation's Privacy page:

> Pursuant to the E.U. General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and other applicable laws and regulations, individuals in the EU/EEA and other jurisdictions may have data subject rights enabling them to request to access, delete, correct, remove or limit the use, or receive a copy of their personal information in Oracle's possession or for which Oracle is otherwise responsible. View instructions on how to exercise these rights.[111]

This is a new development, and the development is no doubt in response to the *Schrems II* decision. However, this message remains hidden, similar to most privacy policies, as it was accessible via a link in small font, hidden amongst other links, at the very bottom of Oracle's website, which is a place consumers normally would not think to look. Therefore, while this may be an effort to provide "protection" sufficient to stand up to the GDPR, it is crafted in a way that U.S. companies can still claim they have given consumers the option of opting out of data collection while simultaneously deterring consumers from taking part in that option.

The U.S. undoubtedly has a tough road ahead, especially considering the different ideologies and philosophies behind protecting citizen data between the U.S. and the E.U. The path to adopting GDPR-like data privacy and protection laws may be an arduous one. Especially now, during the COVID-

---

[108] *E.g.*, O'Flaherty, *supra* note 107.

[109] Max Freedman, *How Businesses Are Collecting Data (and What They're Doing with It)*, BUS. NEWS DAILY (Jun. 17, 2020), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[110] *See Oracle Audiences*, ORACLE, https://www.oracle.com/cx/advertising/audiences/ (last visited Oct. 22, 2021).

[111] *Legal Notices*, ORACLE, https://www.oracle.com/cx/advertising/audiences/ (last visited Oct. 22, 2021).

19 pandemic, social media is more important than ever in ensuring families and friends can remain connected. The use of these social media sites and apps will likely remain steady or even increase as more are developed. However, the tide appears to be changing when it comes to users wanting to protect their personal data. More people are becoming aware of data collection and use, and they are taking steps to ensure their data is safeguarded.

In this era of oversharing and social media, there may be some resistance to an overarching federal framework to protect Americans' data, but as the collection and trading of personal data continue to grow, a day of reckoning will come for those companies misusing this data. Due to the nature of the internet's ubiquity and omnipresence, it is inevitable that data will be collected from various websites and apps that people visit and use every day. So, why not protect that data? The U.S. only stands to benefit from stronger safeguards, especially if other countries take the same approach as the E.U. and begin to restrict data transfers to the U.S. due to insufficient protections. Ultimately, if the U.S. wants to continue obtaining and using personal data from the E.U., it will have to fall in line and strike a sufficient balance between U.S. and E.U. ideals of freedom and privacy.

VI. CONCLUSION

Although the last two decades have seen incredible leaps in the recognition and protection of data privacy, much remains to be done. As technology advances, ever-more problems with data privacy continue to arise. Naturally, some countries will approach data privacy and protection with more exacting and stringent standards while others will take a more lax approach. This inevitably leads to issues with how that data is thus shared amongst countries or entities with differing views on such privacy and protection. It remains to be seen just how these varying philosophies and standards will reach any sort of equilibrium, but with the recent developments of the GDPR and *Schrems II* decision, the U.S. will need to drastically improve its protections if it wishes to continue dealing in global personal data.