THE IMPACT OF *SCHREMS II*: NEXT STEPS FOR U.S. DATA PRIVACY LAW

*Andraya Flor**

INTRODUCTION

Each time a person goes online they leave a digital footprint, but that does not mean they are aware of what that footprint contains. For example, some smartphone applications have location tracking set as a default, which requires the user to have knowledge of this default setting in order to turn it off.[1] In the case of Strava, a popular fitness application that allows members to share running routes with each other and compare fitness goals, the location-sharing feature also publicized heat maps of runners' routes that showed the positions of military service members on U.S. bases abroad.[2] Even where location sharing does not implicate national security by showing exact stations of servicemembers, it raises serious privacy concerns when it reveals information that the user did not know was accessible to others.[3] Design choices make it more difficult for users to become aware of what is happening with their personal information, and subsequently limit their ability to exercise meaningful control over data collection even where applications purport to give it to them. The European Union's comprehensive data privacy regulation, the General Data Protection Regulation (GDPR), acknowledges this defect in Article 25, titled "Data protection by design and by

* Candidate for Juris Doctor, Notre Dame Law School, 2022; Bachelor of Science in Commerce in Economics and Political Science, Santa Clara University, 2019. I would like to thank Professor Mark McKenna for his guidance and support in writing this Note and would also like to thank my colleagues on the *Notre Dame Law Review* for their diligent edits. Finally, I would like to thank my family for their love and support. All errors are my own.

1 Norway's Consumer Council (Forbrukarrådet) released a report that concluded that both Facebook and Google, as well as Microsoft, engage in deceptive design practices to "nudge users toward privacy intrusive options." FORBRUKARRADET, DECEIVED BY DESIGN 3 (2018), https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/. It found that Microsoft had the least privacy-intrusive settings of the three, albeit based on less monetization of user data in their business model, but that Google and Facebook had highly privacy-intrusive settings. *Id.* at 3, 11.

2 *Fitness App Strava Lights Up Staff at Military Bases*, BBC (Jan. 29, 2018), https://www.bbc.com/news/technology-42853072.

3 Harry Guinness, *How to Stop Strava from Making Your Home Address Public*, HOW-TO GEEK (June 26, 2020), https://www.howtogeek.com/678870/how-to-stop-strava-from-making-your-home-address-public/.

default," which requires companies to implement upfront data protection principles prior to processing personal data.[4]

Many in the United States also see comprehensive federal privacy legislation as necessary, including members of Congress who have introduced more than thirty total bills regarding federal data privacy since 2018.[5] The United States has yet to act on the issue on a federal level,[6] instead generally leaving it to individual companies and states to determine their own privacy policies. Generally, the U.S. approach to data collection is permissive with certain exceptions and prohibitions.[7] The EU took a different approach beginning with the Data Privacy Directive in 1995, which is now in force as the General Data Protection Regulation of 2018.[8] In the EU, data processing is unlawful unless the processor can first show one of the bases outlined in the GDPR as a reason for collecting it.[9]

Although starting from different viewpoints, both systems recognize that the companies who want to do business across their borders have to be permitted to engage in cross-border data transfers in order to operate. Under the GDPR, a country must be deemed to have adequate data protection laws before being allowed to receive data transfers from subjects located in the European Union.[10] The United States is not currently an adequate jurisdic-

4 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, art. 25, 2016 O.J. (L 119) 48 [hereinafter General Data Protection Regulation].

5 *See* Müge Fazlioglu, *Consolidating US Privacy Legislation: The SAFE DATA Act*, INT'L ASS'N OF PRIV. PROS. (Sept. 21, 2020), https://iapp.org/news/a/consolidating-u-s-privacy-legislation-the-safe-data-act/ (tracing the development of Republican-sponsored federal data privacy act proposals in the Senate); *see also* Cameron F. Kerry & Caitlin Chin, *How the 2020 Elections Will Shape the Federal Privacy Debate*, BROOKINGS INST. (Oct. 26, 2020), https://www.brookings.edu/blog/techtank/2020/10/26/how-the-2020-elections-will-shape-the-federal-privacy-debate/ (noting that reconciling the tensions between competing federal privacy bills is an ongoing endeavor).

6 Some states have passed or attempted to pass their own data privacy laws, modeled after the GDPR. *See* Sarah Rippy, *US State Comprehensive Privacy Law Comparison*, INT'L ASS'N OF PRIV. PROS., https://iapp.org/resources/article/state-comparison-table/ (last updated Feb. 19, 2021). For example, California passed the California Consumer Privacy Act (CCPA), which created a private right of action for California citizens to sue for certain violations of data privacy protections. *Id.*; CAL. CIV. CODE §§ 1798.100–.198 (West 2020).

7 *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

8 *See* Ernst-Oliver Wilhelm, *A Brief History of the General Data Protection Regulation*, INT'L ASS'N OF PRIV. PROS., https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/ (last visited Mar. 3, 2021).

9 *See* Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMMC'NS TECH. L. 65, 76 (2019); William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 967–79 (2016) (contrasting the European model of data protection with the American model based on consumer data privacy).

10 General Data Protection Regulation, *supra* note 4, art. 45(1).

tion, resulting in the need for other agreements to facilitate business between these markets.[11] The first agreement, the Safe Harbor Agreement,[12] and then its replacement, Privacy Shield,[13] both operated as voluntary self-certification programs for individual companies.[14] Due to Austrian data privacy activist Max Schrems, both agreements have been held invalid.[15] First, the 2015 case of *Maximillian Schrems v. Data Protection Commissioner* (*Schrems I*) invalidated the Safe Harbor Agreement,[16] and later the 2020 case of *Data Protection Commissioner v. Facebook Ireland Ltd.*[17] (*Schrems II*) did the same to Privacy Shield, again casting uncertainty on the ability of companies to engage in cross-border data transfers. Privacy Shield had increased protections for EU data subjects and addressed some of the criticisms that led to Safe Harbor's collapse: for example, a Privacy Ombudsperson was created to allow for additional oversight of data processing in the United States, and it also broadened the remedies available in the United States for violations.[18] Neither of these changes was enough to save it from being invalidated. Now, transfers of data from subjects located in the European Union to entities in the United States are by definition unlawful if made solely in reliance on Privacy Shield.[19] Even if a third replacement agreement is reached soon, there is no reason to believe it would not be subject to another challenge from Schrems.

After *Schrems II*, standard contractual clauses (SCCs) remain a mechanism for entities to transfer data across borders, referring to sets of specific

11 Currently, the European Commission has ruled that only twelve jurisdictions provide "adequate" data protection. *See Adequacy Decisions*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Oct. 2, 2020) (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay).

12 Commission Decision 2000/520 of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issues by the US Department of Commerce, 2000 O.J. (L 215) 7.

13 Commission Implementing Decision 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 1 [hereinafter Privacy Shield Decision].

14 *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 793–95 (2019).

15 *See* Max Schrems, Foreword, *The Privacy Shield Is a Soft Update of the Safe Harbor*, 2 EUR. DATA PROT. L. REV. 148, 148–49 (2016) (arguing that the proposed Privacy Shield is "an outright affront to the highest court of the European Union" and it "does not even regulate the vast majority of processing operations by US controllers").

16 Case C-362/14, ECLI:EU:C:2015:650, ¶ 98 (Oct. 6, 2015).

17 Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020).

18 Privacy Shield Decision, *supra* note 13, ¶¶ 116–17, 139.

19 *See* Joseph J. Lazzarotti & Mary T. Costigan, *EU-U.S. Privacy Shield Program for Transfer of Personal Data to U.S. Found Invalid*, JACKSONLEWIS (July 22, 2020), https://www.jacksonlewis.com/publication/eu-us-privacy-shield-program-transfer-personal-data-us-found-invalid.

contractual language issued by the European Commission.[20] Entities have the option to enter into these agreements, which apply to only the signatories and require the receiver of data, if outside the European Union, to comply with the GDPR.[21] Because many companies, especially multinational corporations, have relied on Privacy Shield with SCCs as a backstop in specific dealings, it is probable that in the short term many business relationships may continue relatively unaffected.[22]

Schrems II invalidated Privacy Shield because the court found that it did not provide an "essentially equivalent" level of protection compared to the guarantees of the GDPR.[23] The National Security Agency (NSA) operated surveillance programs that had the potential to infringe on the rights of EU subjects, and there was a lack of oversight and effective judicial remedies to protect rights of EU data subjects, which undermined Privacy Shield as a mechanism for data transfers.[24] This Note sets aside the surveillance and national security issue, which would require resolution through a shift in overall U.S. national security law, and instead focuses on the other problems raised by *Schrems II*: how can the United States be considered an adequate jurisdiction for GDPR purposes in order to facilitate cross-Atlantic data transfers?

The most complete solution for the United States is a federal data privacy law that will lead the United States to be deemed an adequate jurisdiction. Standard contractual clauses are insufficient as the sole basis of reliance for data transfers across the Atlantic for two reasons. First, *Schrems II* implicates the adequacy of data protection laws of jurisdictions even in the context of SCCs, placing the burden on individual companies to assess the relative adequacy of data privacy laws. Second, SCCs bind only the individual signatories such that they cannot create "adequacy" for the United States as a whole.

Part I provides context for the approach to data privacy in the United States compared to the system in the European Union. Part II analyzes why *Schrems I* invalidated Safe Harbor and how it created the standard that *Schrems II* later applied to also invalidate Privacy Shield. Part II also outlines

20 General Data Protection Regulation, *supra* note 4, art. 46; *Schrems II*, ECLI:EU:C:2020:559, ¶¶ 132–35. Along with standard contractual clauses, binding corporate rules remain another option for companies and were not directly addressed in *Schrems II*. Binding corporate rules are internal policies that must be approved by the supervisory authority. General Data Protection Regulation, *supra* note 4, art. 47. Binding corporate rules are designed to allow multinational companies to transfer data among their own affiliates that are located outside of the European Union. *Binding Corporate Rules (BCR)*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en (last visited Mar. 26, 2021).

21 *See* Claude-Étienne Armingaud, Laure Comparet & Violaine Selosse, *EU Data Protection: Standard Contractual Clauses May Have Been Confirmed by the CJEU, But at What Price?*, K&L GATES HUB (July 17, 2020), https://www.klgates.com/eu-data-protection-standard-contractual-clauses-may-have-been-confirmed-by-the-cjeu-but-at-what-price-07-17-2020.

22 *See id.*

23 *Schrems II*, ECLI:EU:C:2020:559, ¶ 181.

24 *Id.* ¶ 191.

the risks of future use of standard contractual clauses as a means to transfer data between the United States and the European Union without a U.S. federal privacy law. Part III takes a step back to address how the pace of technological development and nature of the internet require that data privacy be addressed at the federal level while also discussing easing the path toward adequacy. Lastly, Part IV presents possible solutions to the lack of harmony among data privacy laws in the U.S. and argues that a federal U.S. data privacy law is the best solution for businesses because it will provide a centralized standard on which to base their operations.

Before examining the impact of *Schrems II* on the data privacy framework, it is necessary to define a few key terms as used in the rest of this Note. Data privacy law is separate from cybersecurity law. Broadly, data privacy law seeks to provide rights centered around the use of personal data by companies, while cybersecurity law deals with unauthorized access of data and the consequences of large-scale data breaches.[25] Though distinct, both areas address the accessibility of personal data and, in addition, having strong data privacy regimes can help reduce the negative impacts of data breaches.[26]

Although California's influence is growing,[27] the General Data Protection Regulation functions as the current standard for global data privacy law.[28] Therefore, the use of the term "personal data" throughout this Note means the definition provided by the GDPR. "Personal data" under the GDPR "means any information relating to an identified or identifiable natural person ('data subject')" including indicators "such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[29] The GDPR also provides further restrictions for special categories of personal data in Article 9, which prohibits all processing of these types of information with a more limited scope of potential exceptions for collecting it.[30] The GDPR takes an expansive view of the term "personal data," where virtually any identifier could conceivably come under that definition.[31]

25 *See What Does Privacy Mean?*, INT'L ASS'N OF PRIV. PROS., https://iapp.org/about/what-is-privacy/ (last visited Dec. 7, 2020).

26 *See id.*

27 *See* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1734 (2021).

28 *See id.* 1735–36.

29 General Data Protection Regulation, *supra* note 4, art. 4.

30 *Id.* art. 9 (prohibiting collection of data regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning health, or data concerning sexual orientation).

31 *See* Hoofnagle, et al., *supra* note 9, at 72–73 ("[E]very datum that identifies a person or could identify a person in the future is personal data.").

I. THE UNITED STATES APPROACH TO DATA PRIVACY IS FRAGMENTED COMPARED TO THE COMPREHENSIVE GDPR

The rights of a data subject in the European Union are approached from a fundamentally different framework than in the United States.[32] The United States starts from the presumption that data collection and processing are permitted with industry-specific regulation, and the European Union presumes that data processing is unlawful unless certain conditions are met upfront. First, this Part will provide an overview of the state of data privacy law in the United States with a focus on the California Consumer Privacy Act as the first comprehensive attempt at data privacy regulation in the United States, and second, it will move to the EU's approach.

A. The United States and the "Right to Privacy"

In the United States, data protection is segmented by industry and closely related to consumer protection. Under the Health Insurance Portability and Accountability Act ("HIPAA"), for example, healthcare data of individuals is strictly regulated.[33] The Family Educational Rights and Privacy Act ("FERPA") governs student education data and imposes restrictions on outside access to a student's school records without the student's consent, and the Children's Online Privacy Protection Act (COPPA) provides protections for collection of information from children under age thirteen.[34] Outside of these sector-specific areas, the Federal Trade Commission acts as the federal agency that enforces data privacy violations.[35] However, there is no unifying or comprehensive U.S. federal data privacy law and no federal private right of action.[36]

Because of this fragmented approach, there is a question of where a right to any level of data privacy might originate. Some have theorized that there may be a right to data privacy as part of the Fourth Amendment's right to reasonable expectation of privacy, or at least in the right against unlawful

32 *But see* Schwartz, *supra* note 14, at 773 (noting that after the passage of the GDPR, industry experts in the United States began to adopt the language of the EU regarding rights to data privacy).

33 Michael D. Kummer & Kristin M. Hadgis, *Data Privacy at a Crossroads*, 71 TAX EXEC., Nov./Dec. 2019, at 48, 50.

34 *See id.*

35 The Department of Health and Human Services is authorized under HIPAA to promulgate privacy rules, and the Department of Education is authorized under FERPA to regulate student records. *See* McGeveran, *supra* note 9, at 997. Tying the FTC to data privacy reinforces the consumer-based market approach to data regulation that the United States has thus far followed. *See id.* at 998–99.

36 *See* Chander et al., *supra* note 27, at 1737; Cameron F. Kerry & John B. Morris, Jr., *In Privacy Legislation, a Private Right of Action Is Not an All-or-Nothing Proposition*, BROOKINGS INST. (July 7, 2020), https://www.brookings.edu/blog/techtank/2020/07/07/in-privacy-legislation-a-private-right-of-action-is-not-an-all-or-nothing-proposition/.

search and seizure.[37] However, this line of inquiry is tenuous and there are many exceptions to the prohibition on unlawful search and seizure.[38] Even if a right to data privacy is found to originate there, it is unlikely to have robust implications because of the already weak status of the general right to privacy; these rights only arise in response to criminal charges and are not generally otherwise enforceable against the state.[39] Although the United States does not have a federal data privacy right, several states have begun to fill the gap with legislation that confers certain rights to consumers regarding the management of their personal information. California enacted the California Consumer Privacy Act (CCPA), which went into effect in 2020 and at the time of passage was the first state effort toward a comprehensive data privacy regime.[40] The CCPA is loosely modeled after the GDPR and brings some of the same principles into its own framework, although it maintains a consumer protection perspective.

For example, the CCPA defines personal information as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[41] The Act goes on to list types of information that would fall within that definition, such as biometric information, geolocation data, and other identifiers, as well as inferences drawn from that data to create a profile about the consumer.[42] Similar to the GDPR's definition of personal data, the CCPA defines the scope of the provision broadly and encompasses a wide spectrum of information. Based on the text alone, the CCPA may go farther than the GDPR and include personal information at the household or device level, and not just the individual.[43] However, the CCPA is more limited in its enforcement ability. It regulates a narrower set of entities and confers a different scope of rights to consumers compared to

37 *See* McGeveran, *supra* note 9, at 976 (noting United States cases that outline broad Fourth Amendment jurisprudence of a right to privacy and contrasting those with cases where the Supreme Court declined to read a broader right to data protection into this right of privacy).

38 *See* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. Rev. 1511, 1536 (2010). *See generally* Gavin Skok, *Establishing A Legitimate Expectation of Privacy in Clickstream Data*, 6 Mich. Telecomms. & Tech. L. Rev. 61 (2000) (describing the history of Fourth Amendment jurisprudence within the context of clickstream data collection and advocating a nuanced approach as technology continues to evolve).

39 *See* Solove, *supra* note 38, at 1521–26 (advocating a reassessment of Fourth Amendment jurisprudence).

40 California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–.199 (West 2020); *see also* Kummer & Hadgis, *supra* note 33, at 50 (noting that the passage of the California Consumer Privacy Act "reflects a developing trend toward regulating personal data and protecting the privacy of residents").

41 Cal. Civ. Code § 1798.140(o)(1) (West 2020).

42 *Id.* § 1798.140(o)(A)–(K).

43 *See* Laura Jehl & Alan Friel, CCPA and GDPR Comparison Chart, Practical Law Chart w-016-7418 2 (2018), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf.

the GDPR.[44] Notably, both contain a private right of action although the CCPA's is much narrower.[45]

The CCPA provides a limited private right of action for California citizens "[t]o recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater" or injunctive relief.[46] Consumers may exercise this right if their nonredacted personal information is "subject to an unauthorized access . . . or disclosure" as a result of the business's failure to implement reasonable security practices.[47] This action is based on a narrower definition of personal information than that set out in the CCPA, instead using the definition from the California Customer Records Act that requires a first and last name in combination with another data element to constitute personal information.[48] Although it exists, the CCPA private right of action is restrictive and has yet to be tested extensively in court.[49]

In November 2020, California voters approved an update to the CCPA called the California Privacy Rights Act (CPRA).[50] The CPRA makes substantial changes to the enforcement structure of data privacy in the state and will take full effect on January 1, 2023.[51] The most significant change is the creation of the California Privacy Protection Agency, which has the authority to create additional data privacy regulations and will replace the California Attorney General's office in enforcing them.[52] The Attorney General's office will retain the ability to bring civil enforcement actions, but the other administrative powers will move to the new agency.[53] This change makes Califor-

44 *Id.* at 1, 5–7. The GDPR has a "much broader" scope and territorial reach and stronger right to erasure than the CCPA. *Id.* at 1. The CCPA has no right to restrict processing and no right to object to automated decisionmaking, where the GDPR allows it under certain circumstances. *Id.* at 5. Finally, the GDPR establishes a private right of action for "material or non-material damage caused by . . . data processors[']breach of the GDPR" while the CCPA has a narrower right for breaches involving a "sub-set of personal information." *Id.* at 6. However, though "[s]ubstantially different in scope," violations of either law can result in "significant economic liability." *Id.*

45 *Id.*

46 CAL. CIV. CODE § 1798.150(a)(1)(A)–(B) (West 2020).

47 *Id.* § 1798.150(a)(1).

48 *Id.* § 1798.81.5(d)(1).

49 Cathy Cosgrove, *CCPA Litigation: Shaping the Contours of the Private Right of Action*, INT'L ASS'N OF PRIV. PROS. (June 8, 2020), https://iapp.org/news/a/ccpa-litigation-shaping-the-contours-of-the-private-right-of-action/#:~:text=section%201798.150(a)(1,and%20maintain%20reasonable%20security%20procedures.

50 *See California Voters Adopt the California Privacy Rights Act*, JONES DAY INSIGHTS (Nov. 2020), https://www.jonesday.com/en/insights/2020/11/california-voters-approve-cpra.

51 *Id.*

52 *See id.*; *California Officials Announce California Privacy Protection Agency Board Appointments*, CA.GOV (Mar. 17, 2021), https://www.gov.ca.gov/2021/03/17/california-officials-announce-california-privacy-protection-agency-board-appointments/ [hereinafter *California Officials Announce*] (listing the new members of the CPPA board).

53 *California Officials Announce*, *supra* note 52.

nia's data privacy scheme more closely reflect the GDPR by creating a separate enforcement agency. CPRA also expands the private right of action definition of personal information to include the combination of an email or username and password (i.e., login credentials to an online account), although it still does not use the actual CCPA definition.[54]

One possible consequence of the CCPA/CPRA is that it becomes the equivalent of the GDPR in the United States and the de facto standard under which U.S. companies operate. Because it covers California citizens, which make up a significant consumer base in the United States, many companies will default to the CCPA standards across the United States.[55] Residents of other states will enjoy the benefit of a company that complies with the CCPA in all of its internal policies, although they will not be able to access the enforcement mechanisms because the CCPA only provides these rights to California citizens.[56] This outcome still has the benefit that other citizens in practice are afforded stronger data protection rights than they would have otherwise been able to access. Another outcome is that other states will follow suit and enact their own privacy laws: twenty-seven states introduced comprehensive data privacy regulation between 2018 and 2020.[57] The result will be data privacy laws that may be substantially similar but vary in certain details or requirements, contributing to the existing lack of harmony in data privacy law within the United States.[58]

B. European Union Approach to Data Privacy

Privacy rights in the European Union are rooted in "individual dignity" rather than consumer protections.[59] The EU Charter of Human Rights

54 Peter Hegel, Sundeep Kapur & Claire Blakey, *The California Privacy Rights Act (CPRA) Has Been Enacted into Law*, PAUL HASTINGS (Nov. 6, 2020), https://www.paulhastings.com/insights/ph-privacy/blog-the-california-privacy-rights-act-cpra-has-been-enacted-into-law.

55 *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1712 (2020).

56 *See id.* at 1692; *see also California Consumer Privacy Act (CCPA)*, OFF. OF THE ATT'Y GEN. OF CAL., https://oag.ca.gov/privacy/ccpa (last visited Jan. 10, 2021).

57 Rippy, *supra* note 6 (noting that Texas, Hawaii, and Louisiana are using task forces instead of considering a comprehensive bill). In addition to California, three states, Nevada, Maine, and Virginia, have already enacted their own state-wide data privacy legislation. *Id.* Washington state has introduced its own draft bill, and eight other states have data privacy bills in committee. *Id.*

58 *See id.* For example, almost all of the proposed and enacted state bills include a right for the consumer to opt out of the sale of their personal information to third parties—with exceptions, like Maine and Massachusetts, which reframe the process as requiring consumers to opt in to data sharing up front. *Id.* Although these states may not be large markets relative to the populations of other states like California, this example is illustrative of the potential discrepancies in privacy bills among states.

59 McGeveran, *supra* note 9, at 967.

includes an explicit right to data privacy.[60] Starting with this framework, the Data Privacy Directive, which later became the GDPR, requires a legitimate basis before data processing begins.[61] The GDPR continues this conception of data privacy in its principles of data minimization, data accuracy, and purpose-driven limits on controllers and processors to only collect and store what is necessary.[62] It prohibits broad data collection unless the data processor can show one of several legitimate bases for collection, in contrast to the initial U.S. presumption that data processing is permitted.[63] One of the key implications of the language of the GDPR is that it applies to the processing of data of any identifiable natural person located within the European Union—it is not limited to protecting only citizens of EU member states and instead operates based on the location of the person.[64]

The GDPR is built on expansive definitions that cover a wide scope of digital activity. Data "processing" means any operation, using automated or nonautomated means, "performed on personal data or on sets of personal data, . . . [such as] collection, . . . storage, . . . use, disclosure . . . or otherwise making [it] available."[65] A key aspect of this definition is that it includes both automated and nonautomated means of data collection, which encompasses a broad range of potential actions. A data "controller" is "the natural or legal person, public authority, agency or other body which . . . determines the purposes and means of the processing of personal data."[66] A data controller is not always the same as the processor, which is the "natural or legal person, public authority, agency or other body" that "processes personal data on behalf of the controller."[67] This distinction is meaningful because an entity that is not directly collecting or controlling the intake of personal data is still subject to the GDPR when it stores or otherwise uses data from a controller. Whether an entity functions as a processor or a controller does not result in a different standard of conduct in the context of cross-border trans-

60 Charter of Fundamental Rights of the European Union, art. 8, 2012 O.J. (C 326) 391, 397 ("Everyone has the right to the protection of personal data concerning him or her. . . . 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. . . . Compliance with these rules shall be subject to control by an independent authority."); *see also* G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.").

61 *See* General Data Protection Regulation, *supra* note 4, art. 5; *supra* note 9 and accompanying text.

62 General Data Protection Regulation, *supra* note 4, art. 5.

63 *See* McGeveran, *supra* note 9, at 977 (describing the dominant U.S. approach as assessing transactions for their unfairness rather than focusing on individual rights).

64 *See* Hoofnagle et al., *supra* note 9, at 74.

65 General Data Protection Regulation, *supra* note 4, art. 4(2).

66 *Id.* art. 4(7).

67 *Id.* art. 4(8).

fers: both types of operations still must comply with the terms of the GDPR when located outside of the European Union and receiving data from subjects in the European Union.[68]

Lastly, the GDPR defines "recipient" as "a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not."[69] This means that the GDPR applies not only directly to controllers and processors but also to third parties authorized by those entities to process the data. These definitions demonstrate the wide scope of potential entities that are subject to the GDPR, even if they are not engaging directly in economic activity in the European Union. The GDPR's potential application to data processors, controllers, and third parties increases the practical effect of these provisions and impacts the development of privacy law around the world, which is necessarily in response to this broad framework.[70]

In order to transfer personal data out of the European Union, a country must have an adequacy decision that certifies the data protection level of the country. If there is no adequacy decision, there are several options remaining for companies that are located in a jurisdiction that has yet to be deemed adequate.[71] Processing is "lawful" only if the data subject consents or if it is necessary for one of the following reasons: performance of a contract, to protect vital interests of the data subject or somebody else, to comply with a controller's legal obligations, for a task in the public interest, or in furtherance of legitimate interests to the extent the interest is not overridden by fundamental rights of the data subject.[72] The two bases of compliance with legal obligations and necessary for the public interest can only be predicated on European Union law or European Union Member state law "to which the controller is subject,"[73] meaning that companies cannot rely on their own national laws to show that processing is lawful. Enforcement under the GDPR is governed by independent national data protection authorities located in the individual member states.[74] The potential fines that companies may face for noncompliance are evaluated on a case-by-case basis and can reach up to four percent of the preceding year's global revenue.[75]

The GDPR's broad provisions further the goals of the EU approach to data privacy as rooted in individual dignity by requiring compliance with specific conditions before data processing becomes lawful, thus defining the context that informed both the *Schrems I* and *Schrems II* decisions.

---

68 *Id.* art. 3(2) ("This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union . . . .").

69 *Id.* art 4(9).

70 *See generally* Anu Bradford, *The Brussels Effect*, 107 Nw. U. L. Rev. 1 (2012).

71 *See* Hoofnagle et al., *supra* note 9, at 83–85 (discussing the GDPR's requirements for permitting cross-border data transfers where there is not an adequacy decision).

72 General Data Protection Regulation, *supra* note 4, art. 6.

73 *Id.* art. 6(3)(a)–(b).

74 *Id.* art. 51; *see also* McGeveran, *supra* note 9, at 970.

75 General Data Protection Regulation, *supra* note 4, art. 83(2)–(6).

II. MAX SCHREMS AND THE END OF SAFE HARBOR AND PRIVACY SHIELD

Because of these distinct approaches to regulating data privacy, the United States and European Union have negotiated agreements so that businesses can operate in both markets without incurring liability.[76] The first agreement, Safe Harbor, was enacted to facilitate these cross-border transfers in a legal regime that balanced the privacy interests of individuals with the needs of commerce.[77] This Part traces the timeline of the invalidation of Safe Harbor and its subsequent replacement, Privacy Shield, in the Court of Justice of the European Union based on the efforts of data activist Max Schrems.

A. Schrems I *Invalidates Safe Harbor*

In *Maximillian Schrems v. Irish Data Protection Commissioner* (*Schrems I*), decided in 2015, the Court of Justice of the European Union ("CJEU") found that the Safe Harbor Agreement did not ensure "an adequate level of protection" for data transfers under the Data Privacy Directive (now the GDPR) to the United States.[78] The CJEU held that the standard under the General Data Privacy Directive is that a country's level of data protection must be "*essentially equivalent* to that guaranteed within the European Union by virtue of Directive 95/46 read in light of the [EU Charter of Fundamental Rights]."[79] Schrems argued that Facebook Ireland's data transfers out of Ireland to Facebook in the United States should be prohibited because of evidence that the NSA had near unrestricted access to that information, which was revealed by Edward Snowden.[80] Schrems successfully argued that the Safe Harbor Agreement was an insufficient mechanism to protect the data of those located in the European Union.[81] The CJEU agreed with Schrems on the grounds that Safe Harbor had too many loopholes for United States surveillance operations and that public authorities were not required to comply at all.[82] While *Schrems I* was specifically concerned with the activities of U.S. mass surveillance operations by various branches of the government, it also was more broadly aimed at protecting the rights of EU data subjects when

76 *See* Hartzog & Richards, *supra* note 55, at 1706–09.

77 *Id.* at 1707; *see also* Daniel Alvarez, *Safe Harbor Is Dead; Long Live the Privacy Shield?*, BUS. L. TODAY, May 2016, at 1, 1.

78 Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650, ¶¶ 97–98 (Oct. 6, 2015); *see* Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post* Schrems, 18 GERMAN L.J. 881, 882 (2017).

79 *Schrems I*, ECLI:EU:C:2015:650, ¶ 73 (emphasis added). Currently, the European Commission has ruled that only twelve jurisdictions provide "adequate" data protection. *See Adequacy Decisions*, *supra* note 11.

80 *Schrems I*, ECLI:EU:C:2015:650, ¶¶ 85–86; Chander et al., *supra* note 27, at 1768; *see also* Kuner, *supra* note 78, at 890 (clarifying that the judgment did not explicitly rule that U.S. law was inadequate, but the discussion of U.S. intelligence gathering implies a strong condemnation of the effect of those practices on rights of EU data subjects).

81 *Schrems I*, ECLI:EU:C:2015:650, ¶ 106.

82 *See* Alvarez, *supra* note 77, at 1–2.

their data is transferred to private U.S. companies, and in its aftermath implicated an estimated five thousand companies and organizations.[83] Some have argued that the CJEU extended the meaning of the Directive (now GDPR) too far, such that it imputed EU law onto other sovereign states in violation of international law principles.[84]

In response to the invalidation of Safe Harbor, the European Union and United States negotiated the Privacy Shield Decision as a replacement agreement designed to answer the concerns outlined in *Schrems I*.[85] Privacy Shield contained significant changes to address the handling of Europeans' personal data, U.S. government access to that data, and general protection of EU citizens' rights.[86] These changes included representations that the U.S. national security programs would be limited and created a Privacy Ombudsperson designed to be an independent oversight mechanism for complaints against those programs.[87] Additionally, Privacy Shield required companies that chose to certify with the program to follow seven data privacy principles in all their transactions "to foster, promote, and develop international commerce" between the two jurisdictions.[88]

B. Schrems II *Invalidates Privacy Shield*

Max Schrems again triumphed over privacy agreements between the United States and European Union in 2020.[89] In *Data Protection Commissioner v. Facebook Ireland Ltd.* (*Schrems II*), the court addressed the adequacy of protection provided by the EU-U.S. Privacy Shield.[90] Schrems requested the data commissioner "prohibit or suspend the transfer by Facebook Ireland of his personal data to Facebook Inc., established in the United States, on the ground that that third country did not ensure an adequate level of protection."[91] In the judgment issued by the Commission, the court reiterated the goals of EU data protection based on safeguarding the fundamental rights and freedoms of persons in the European Union.[92] The court also discussed

83 *Id.*

84 *See* Christina Lam, Comment, *Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in* Schrems v. Irish Data Protection Commissioner, 40 B.C. INT'L & COMPAR. L. REV. ELEC. SUPPLEMENT 1, 10 (2017) (arguing that the meaning of "adequate level of data protection" should be "sufficient" instead of "essentially equivalent" to minimize the burden on other countries and maintain the spirit of the Data Privacy Directive). For a discussion of the "Brussels Effect" as a theory of how the European Union's actions in practical effect unilaterally regulate global markets, see generally Bradford, *supra* note 70.

85 *See* Lam, *supra* note 84, at 7; Alvarez, *supra* note 77, at 2–3.

86 Alvarez, *supra* note 77, at 2–3.

87 *Id.*

88 Privacy Shield Decision, *supra* note 13, annex II, at 48–52.

89 Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559 ¶ 203 (July 16, 2020).

90 *Id.* ¶ 68(9)–(10).

91 *Id.* ¶ 159.

92 *Id.* ¶ 8.

how U.S. intelligence operations undermined the principles of the GDPR, specifically in the context of an effective judicial remedy.[93]

The CJEU affirmed the requirement that data protection must be "essentially equivalent" to the GDPR to be considered an "adequate" level of protection, as first outlined in *Schrems I*.[94] According to the court, Privacy Shield allowed U.S. national security and public interest concerns to take primacy over the limiting principles in Privacy Shield.[95] The United States argued that Privacy Shield did provide adequate data protection because of the representations the United States made in the Privacy Shield Decision itself.[96] Both parties agreed to the initial Decision in spite of the national security concerns because the activity of United States surveillance operations was "limited to what is strictly necessary to achieve the legitimate objective in question."[97] The referring court questioned the adequacy of this limitation and the effectiveness of "judicial protection against such interferences" where the creation of a Privacy Shield Ombudsperson to ensure compliance still did not meet the GDPR requirements.[98]

Privacy Shield was held inadequate because it was not "essentially equivalent" to the level of data protection provided by the GDPR: the United States did not have effective and enforceable rights for data subjects in the European Union.[99] Similar to *Schrems I*, the court was concerned with the United States' ability to circumvent the protections in the GDPR through national security interests.[100] The practical effect of the decision renders data transfers between the European Union and United States uncertain. Because of *Schrems II* and the lack of an adequacy decision for the United States under the GDPR, data transfers between the two jurisdictions are unlawful unless companies utilize one of two other existing mechanisms: standard contractual clauses or binding corporate rules. And as the CJEU in *Schrems II* provides, standard contractual clauses entail an examination of the adequacy of the third country's level of data protection.

---

93 *Id.* ¶¶ 187–89, 191–92; *id.* ¶ 194 ("An examination of whether the ombudsperson mechanism which is the subject of the Privacy Shield Decision is in fact capable of addressing the Commission's finding of limitations on the right to judicial protection must . . . start from the premiss [sic] that data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data.").

94 *Id.* ¶ 94.

95 *Id.* ¶¶ 163–64.

96 Privacy Shield Decision, *supra* note 13, ¶¶ 125–34.

97 *Schrems II*, ECLI:EU:C:2020:559, ¶ 167.

98 *See id.* ¶¶ 168, 195–97 (noting that the Privacy Shield Ombudsperson reports to the Secretary of State and is not independent of the executive, and therefore is incapable of fully addressing the rights of data subjects).

99 *Id.* ¶¶ 64–65; *id.* ¶¶ 187–88 ("[L]egislation not providing for any possibility for an individual to pursue legal remedies . . . does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the [EU Charter of Fundamental Rights]."); *see also* Lam, *supra* note 84, at 13 (predicting that the European Union may invalidate Privacy Shield).

100 *See Schrems II*, ECLI:EU:C:2020:559, ¶¶ 191–92.

C. Schrems II *Undermines Reliance on Standard Contractual Clauses as a Sufficient Lawful Basis for Cross-Border Data Transfers*

The referring court in *Schrems II* also requested a ruling on whether standard contractual clauses provided adequate data protection. The referring court's belief was that the clauses did not rise to the "essentially equivalent" level of protection compared to the GDPR, but was uncertain as to whether the Commission could prohibit transfers that relied on these clauses based on the incompatible state of the law in the third country.[101] In particular, the referring court asked what factors should be considered for determining adequacy of protection with standard contractual clauses as the basis for the data transfer.[102]

In the *Schrems II* judgment, the CJEU affirmed the validity of the standard contractual clauses. It also stated that, although the GDPR was silent on this specific issue, that to assess the adequacy of the level of data protection in a country under these particular transfers the relevant question is whether data subjects are "afforded appropriate safeguards, enforceable rights and effective legal remedies."[103] The consequence of this inquiry is that where a country does not have an adequacy decision and is deemed so inadequate such that a company cannot be in compliance with the GDPR even using SCCs, a Data Protection Authority "is *required* to suspend or prohibit a transfer of data to [that] third country."[104]

Schrems II casts doubt on the long-term viability of reliance solely on SCCs for data transfers, especially in light of the referring court's doubts about the validity of these clauses that reflect general distrust of their effectiveness to secure data protection for EU data subjects. Even where SCCs are in place, a company is still subject to the adequacy level of the country to which they are transferring the personal data.[105] The court went on to conclude that because SCCs are only binding on the involved parties and create obligations for those parties only, "it may prove necessary to supplement the guarantees contained in those standard data protection clauses."[106] The European Data Protection Board (EDPB), which administers the GDPR, has

101 *Id.* ¶¶ 68, 90.

102 *Id.* ¶ 90.

103 *Id.* ¶¶ 103, 105 (noting that this inquiry includes assessment of the level of access by public authorities to the data and the legal system of the receiving country).

104 *Id.* ¶ 121 (emphasis added).

105 *See* Carol A.F. Umhoefer & Andrew Serwin, Schrems II*: Now What? New FAQs from EU Data Protection Supervisors Provide Guidance on Data Transfers*, DLA Piper (July 28, 2020), https://www.dlapiper.com/en/us/insights/publications/2020/07/schrems-ii-now-what-new-faqs-from-eu-data-protection-supervisors-provide-guidance-on-data-transfers/.

106 *Schrems II*, ECLI:EU:C:2020:559, ¶ 132. This determination is tempered by the court's decision not to extend the period of applicability for Privacy Shield to allow companies to find alternatives, instead finding that the decision would not create a "legal vacuum" because other mechanisms for data transfers would still allow them to proceed. *Id.* ¶ 202. By not creating an extension for Privacy Shield, the court signaled that reliance on procedures such as standard contractual clauses could be a sufficient lawful basis alone in certain cases for data transfers, even without supplements.

published recommendations for comment on supplementary measures to help companies if they are unsure about the level of data privacy in their jurisdiction.[107] These recommendations include technical measures, additional contractual measures, increased transparency, and other organizational suggestions.[108]

Setting aside the national security concerns that were part of the CJEU's rationale, *Schrems II* has two key findings. First, the court's judgment not only permits but requires data protection authorities to suspend the data transfer if they determine the transfer did not take place under an "essentially equivalent" process as guaranteed by the GDPR. Second, companies are not able to escape an adequacy inquiry into the laws of the country they are located in based on their use of standard GDPR contractual clauses and must still evaluate the overall context of the transfer—the level of privacy safeguards of their jurisdiction—and determine if supplements to the standard contractual clauses are necessary.[109] The CJEU declined to create a grace period for enforcement as had occurred when Safe Harbor was eliminated, and as of the judgment all data transfers based solely on Privacy Shield are unlawful.[110] Consequently, the United States is now in a position to reevaluate its data privacy governance mechanisms to continue to facilitate cross-border transfers of personal data and should take advantage of it, or continue to have its adequacy evaluated on a case-by-case basis in EU courts.

III. Rapid Technological Development Is a Reason to Enact Centralized Protections

Schrems II created uncertainty with regard to the state of data privacy transfers between the United States and European Union and continues to elevate the GDPR as a prominent data privacy governance mechanism in the international community. However, it also created an opportunity to evaluate the role of the GDPR compared to the sectoral approach of the United States. The United States' approach to privacy promotes flexibility and industry-specific standards that may be more easily updated with the fast pace of technological development. An example of rapid technological development is seen in the area of location tracking, where recent lawsuits include the City of Los Angeles's suit against the Weather Channel for passing its users' location data on to outside entities.[111] The reality is that GDPR is in

107 Eur. Data Prot. Bd., Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data 2 (2020), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

108 *Id.* at 21–37.

109 *See* Lazzarotti & Costigan, *supra* note 19 ("SCCs may not be an adequate transfer mechanism in every case, or they may require the negotiation of additional provisions to satisfy these obligations.").

110 *Schrems II*, ECLI:EU:C:2020:559, ¶ 203.

111 *See* Kirsten Martin & Helen Nissenbaum, *What Is It About Location?*, 35 Berkeley Tech. L.J. 251, 260–61 (2020).

force and its current effect is the de facto governing international standard for data privacy law, rendering private companies located in the United States subject to its provisions if they want to transfer personal data out of the European Union.[112]

Because the internet lacks territorial bounds, it is difficult to conceptualize a national law in this area that functionally could be limited to certain borders, given the multinational operations of most companies. The fast-paced development of technology means that regulators are often playing catch-up, and the GDPR's starting premise forces those innovations to consider the effect on an individual's personal data.[113] While states may implement laws that conflict and differ, the internet is distinctive because of its significant position in facilitating commerce and requires a centralized regulation.[114] The growing number of state data privacy bills reveals a trend that the United States should take advantage of to institute a centralized federal data privacy regulation, rather than continuing with the segmented approach. The proliferation of "mini-GDPRs"[115] is overall a detriment to the system of cross-border commerce, including across state borders within the United States.

In order to be deemed "adequate," the European Commission must issue an adequacy decision based on the examination of the following factors in the third country: rule of law, respect for human rights, national security, existence of independent supervisory authorities, and other international commitments the country has entered into.[116] Standard contractual clauses are also insufficient to deem the United States or other jurisdictions adequate because they bind only the individual signatories and do not relate to the factors laid out in GDPR Article 45. Either a third country, a territory or one or more specific sectors within that third country, or an international organization may be deemed to have an adequate level of data protection, although thus far only countries and their dependencies have been deemed adequate.[117] Because of the "essentially equivalent" standard established in *Schrems I* and *II*, the EU has set a high standard for other jurisdictions.

In the aftermath of *Schrems II*, and taken in the context of state-level developments of privacy law in the United States, the need for the United States to address the issue on the federal level becomes much stronger.

IV. The United States Should Enact a Federal Data Privacy Law

Schrems II leaves open only two mechanisms for lawful cross-border transfers of personal data into the United States: using either standard contractual clauses or binding corporate rules.[118] As discussed in Part II, even though

112 *See* Bradford, *supra* note 70, at 3–4.
113 *See* Martin & Nissenbaum, *supra* note 111, at 255–57, 265–66.
114 *See* Hartzog & Richards, *supra* note 55, at 1737.
115 *Id.* at 1712–13.
116 General Data Protection Regulation, *supra* note 4, art. 45.
117 *See Adequacy Decisions*, *supra* note 11.
118 *See supra* note 20 and accompanying text.

these devices remain in place (along with user consent) reliance on them entails increased costs for businesses through implementation of individual contracts or creates only a limited scope of binding corporate rules. By evaluating standard contractual clauses on a case-by-case basis and in light of the laws of the jurisdiction in which the company operates, *Schrems II* narrows even the use of these options to facilitate lawful transfers of personal data into the United States. A company that believed it followed the lawful use of SCCs may still find cross-border transfers that it relies on terminated by data protection authorities, reinforcing the need for the United States to address this issue.

The first Section of this Part addresses why data privacy governance is necessary at all, through ex ante regulation and principles of privacy by design and increased user control over personal data. The second Section applies these theories to the current state of privacy law in the United States and addresses why federal action is the better route than both a third iteration of a framework similar to Privacy Shield and continued state-by-state legislation.

A. The Burden to Safeguard Data Privacy Should Be on Those in the Best Position to Address It: The Controllers and Processors

Personal data is accessible and for sale in almost any online transaction.[119] It should be protected through centralized regulation rather than leaving it to individual parties to safeguard it because there is a "larger social value" to defending privacy.[120] Individual decisions regarding consent to data collection may "not collectively yield the most desirable social outcome," and the future of data processing does not show signs of slowing down.[121] Furthermore, reliance on consent and control of the user is undermined by the user's lack of information relative to the data collector and deceptive design practices when asking for user consent, reinforcing the value of having legislated protections at all.

1. Upfront Data Privacy Protection Will Address the Social Value of Safeguarding Personal Data

Some U.S. technology companies advocate a control-based theory of privacy regulation.[122] Scholars have argued that reliance solely on user control is misplaced and an ineffective means to address access to personal data, instead advocating a model with "a baseline, fundamental level of protection

119 *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1881, 1888–89 (2013).

120 *Id.* at 1881.

121 *Id.*; *see* Hartzog & Richards, *supra* note 55, at 1725 ("We are only beginning to assess the human and social costs of platform dominance and massive-scale data processing.").

122 *See* Woodrow Hartzog, Opinion, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423, 423–24 (2018). Both Facebook and Microsoft contain language in their privacy statements that reference user control. *Id.*

regardless of what they choose."[123] Most people do not want to micromanage their data due to the problem of scale in the thousands of online interactions that occur each day.[124] A 2008 study estimated that the opportunity cost in time spent to actually read the privacy policy once for each website visited in a year would be about $781 billion,[125] reinforcing the view that the burden to address these concerns should not be on the individual consumer. The additional problem with relying on user exercise of control is that the choice is not freely made because technology companies use design mechanisms to incentivize certain decisions; thus, laws curated to user choice are "deficient because [they] ignore[ ] design."[126] By regulating through design rather than user control, there is increased ability to have effective protection for consumers.

Proponents of the user control and transparency approach rely on consumers exercising their data privacy rights and on those rights being effective.[127] This approach places lower weight on the information asymmetry between the user and the company and argues that stronger enforcement mechanisms and routes for private individuals to obtain control will maximize the value of personal data for everyone.[128] Rather than making the judgment that a user's choice to prioritize a short-term gain over long-term potential adverse privacy impacts is a negative one, this model argues that the person who values the data more is able to exercise control where they want to, and ignore it when they do not and simply access the service.[129] Companies that value the personal information because of their monetization efforts will expend more effort to get it, and each person's willingness to enforce their data privacy rights accurately reflects how much they value this data.

However, reliance on user consent does not address the informational asymmetry between the company and the consumer, meaning that the choice to allow a company to collect personal information is based on an inaccurate assessment. Even users of Google that turn off their location ser-

123 *Id.* at 431.

124 *See* Hartzog & Richards, *supra* note 55, at 1735–36; Solove, *supra* note 119, at 1901.

125 Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J.L. & Pol'y for Info. Soc'y 543, 544 (2008).

126 Woodrow Hartzog, *Are Privacy Laws Deficient?*, 2 Int'l J. for Data Prot. Officer, Priv. Officer & Priv. Couns., no. 10, 2018, at 17, 17 (2018) ("While major privacy failures grab the headlines, the most significant corrosive force on our privacy is often barely noticeable, like death from a thousand cuts."); *see also* Hartzog & Richards, *supra* note 55, at 1735.

127 *See* Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. Rev. 1327, 1328–29, 1350 (2012) (discussing how consumers both are the product and help create the product, their digital profiles, in the market for personal data).

128 *See id.* at 1329 (arguing that the "right to rescind enrollment in [a social networking service], triggering a deletion of information shared with the service, and an ability to export information shared with the service are appropriate given the skewed aspects of personal information transactions.").

129 *See* Solove, *supra* note 119, at 1896, 1899–900.

vices are still tracked by Google using triangulation from cell towers.[130] Still, those in favor of this model suggest that the commodification of personal information is necessary to facilitate transnational commerce.[131] As the following report illustrates, companies have a profit motive to collect as much personal data as possible and will use deceptive design tactics to induce consumers to consent to the use, sale, or collection of their personal data. This reinforces one of the benefits of enacting a federal data privacy act focused on design at all, namely, that companies will be left to less self-regulation and forced to implement baseline protections for consumer data before turning to user controls.

2. Google, Facebook, and Microsoft as Case Studies in Undermining User Control

The Norwegian Consumer Council's (Forbrukarrådet's) report issued in 2018 analyzed the privacy protections for users of Facebook, Google, and Microsoft.[132] The report demonstrates the information asymmetry between the companies and their consumers and shows that the consumer begins with a disadvantage because they are asked to share personal information without a true understanding of how it will be used.[133] Users tend to trade short-term gains, such as access to a website, for potentially longer term loss of privacy and these efforts to nudge consumers to allow access to their personal information can become "ethically problematic . . . and deprive [consumers] of their agency."[134] This renders the user's "consent" to the use and collection of their personal data meaningless due to deceptive design practices.

To illustrate what is meant by deception in design, after the GDPR went into effect, companies notified their users of new privacy policies using pop-up windows. In the Norwegian Consumer Council's report, using screenshots from Facebook's GDPR notification to its users, the two options presented to users were "Manage Data Settings" in faded gray font next to "Accept and Continue" in bright blue.[135] If a user wanted to control their settings regarding personalized advertising based on Facebook's use of third-party data, they needed to select "Manage Data Settings"—the less prominent option. But, clicking "Accept and Continue"—standing out in a bright color—resulted in the automatic activation of the setting and authorized Facebook to use data from third parties to show them personalized advertisements.[136] Users who chose "Accept and Continue" did not get to see what

130 *See* Martin & Nissenbaum, *supra* note 111, at 303.

131 *See* Solove, *supra* note 119, at 1896 (noting that some view restrictions on businesses that rely on sale of data to provide their online content as "paternalistic").

132 FORBRUKARRADET, *supra* note 1, at 3; *see also* Martin & Nissenbaum, *supra* note 111, at 301–03 (finding that people have definite and nuanced expectations of privacy depending on the context of the platform being used).

133 FORBRUKARRADET, *supra* note 1, at 6.

134 *Id.* at 7.

135 *Id.* at 14.

136 *Id.*

the default setting was before they selected it, which the report calls "hidden defaults."[137]

Additionally, the choice presented to users was whether Facebook would use data from third parties to show them personalized ads, which is a limited scope of control when compared to other ways Facebook processes and collects data from third parties and does not inform the consumer of other ways third-party data may be used.[138] Even after choosing to restrict this setting, the pop-up continued with a disclaimer that if the user has given their contact information to a third party and Facebook matches it to their Facebook profile, Facebook may still use that data to show the user personalized advertisements.[139] This example illustrates how design choices influence both whether users exercise control at all and how effective those choices really are. These types of design choices may remain overlooked by basing regulation on illusory consent mechanisms and undermine their effectiveness.

B. Federal Regulation Will Provide a Minimum Standard of Data Privacy Safeguards

In his opening remarks to the House Energy and Commerce Committee in the wake of the Cambridge Analytica and Facebook data disclosures, Representative Frank Pallone stated, "We need comprehensive privacy and data security legislation. We need baseline protections that stretch from internet service providers to data brokers to app developers and to anyone else who makes a living off our data."[140] Implementing a federal regulation that requires companies to comply with specific minimum standards of data processing provides a baseline from which to address the growing industry of processing personal data.[141] The benefits to providing a minimum centralized standard within the United States include harmonization of internal policy and reduced costs for businesses that operate in multiple states. These outweigh the costs of decreased ability for states to experiment and lowered ability to tailor regulations to certain sectors; by implementing a minimum, it will preserve room for states' laws to build on the protections.[142] Because of its different approach to data privacy, a U.S. federal data privacy act will not

137 *Id.* at 14–15 (noting that Google also frequently has these "hidden default" mechanisms to prime users to make specific choices and maximize data sharing with third parties).

138 *Id.* at 33 ("Facebook is an enormous ecosystem for collecting and processing data about the user. Therefore, the option to stop only the use of data from third parties for personalised ads is a far cry from switching off personalisation of ads.").

139 *Id.* at 33–34.

140 *Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy & Com.*, 115th Cong. 6 (2018) (statement of Rep. Frank Pallone, Jr., Ranking Member, H. Comm. on Energy & Com.).

141 *See* Hartzog, *supra* note 122, at 431–32.

142 *See* Hartzog & Richards, *supra* note 55, at 1716; *cf.* Chander et al., *supra* note 27, at 1797–99 ("New federal privacy law could provide a nationwide floor, permitting states to intervene only to the extent that they raise privacy standards further. This allows state innovations and experimentation."); *see also supra* Part III.

reflect the same protections as the GDPR.[143] This leads to the external benefit of placing the United States in the global conversation surrounding data privacy and increases debate surrounding the best way to regulate these issues, leading to broader consensus in the future.

1. A Third Agreement Between the United States and European Union Will Likely Also Be Struck Down

The market pressures on both jurisdictions to facilitate cross-border data transfers mean that they will have to come to some sort of agreement. If its framework incorporates different principles than those in the GDPR, which is likely, the United States' approach will compete with the GDPR in the global sphere.[144] This will force the parties to negotiate and compromise or risk losing out on large segments of the global market if businesses choose to operate in only one economic area. The surveillance issues present in both Safe Harbor and Privacy Shield can only be resolved with a shift in U.S. national security policies, making a third agreement unlikely to succeed. With a federal law, the United States is better positioned to establish its adequacy because, although the *Schrems II* standard is "essentially equivalent," the CJEU clarified that it did not need to be identical so long as there are effective and enforceable rights for data subjects in the EU.[145]

2. Reliance on the CCPA/CPRA Is Not Enough to Certify the United States as Adequate

An unanswered question that remains after *Schrems II* is whether a single U.S. state could be deemed an adequate jurisdiction alone—for example, California and the CCPA/CPRA could potentially be evaluated independently of any federal U.S. framework. The consequence of this would be that by complying with the CCPA/CPRA, businesses located in California would be treated as complying with the GDPR. Because the CCPA/CPRA is already likely to become the de facto governing standard for businesses in the United States due to California's outsized market share,[146] this raises questions about the consequences of that adequacy decision for companies operating in other states and the interaction of state and federal legal systems. The idea of an end run around a federal privacy framework is appealing for its avoidance of the drawn-out process involved in enacting federal law.[147] The passage of the CPRA strengthens this argument because it creates a separate enforcement agency to oversee the provisions and expands the private right

143 *See* Hartzog & Richards, *supra* note 55, at 1692; Kerry & Chin, *supra* note 5.

144 *See* Chander et al., *supra* note 27, at 1737 ("California has emerged as a kind of privacy superregulator. . . . [California r]ather than the supernational EU . . . is now driving privacy in a significant part of the world. . . ."); Hartzog & Richards, *supra* note 55, at 1692 ("The GDPR has called the U.S. government's hand.").

145 *See supra* Sections II.B–C.

146 Hartzog & Richards, *supra* note 55, at 1712.

147 *See* Chander et al., *supra* note 27, 1797–99.

of action outlined in the CCPA.[148] However, even if the European Commission considered certifying a sector or state rather than an entire country, the private right of action is only available to California residents—it lacks an effective and enforceable remedy that *Schrems II* requires for a jurisdiction to be "essentially equivalent" to the GDPR because EU citizens and citizens of other states cannot access the mechanism.[149] The definition of personal information that can provide the basis for the action is also far narrower than that in the GDPR, making it unlikely that the European Commission would certify the jurisdiction as adequate even if companies followed the CCPA/CPRA.

By creating an independent data protection agency, one of the reasons that both Safe Harbor and Privacy Shield were invalidated in the *Schrems* cases, the CPRA's impact on the continued development of U.S. privacy law relative to the EU remains to be seen.

Conclusion

The current uncertainty that businesses located in the United States face regarding the lawfulness of cross-border data transfers between the United States and European Union stems from a different approach to regulation of data privacy. States in the United States have further complicated the situation—with California passing the CCPA/CPRA and as other states follow suit, the varied approaches to data privacy will only increase. The invalidation of Privacy Shield has reduced the mechanisms available to share data across the Atlantic and subjected the use of standard contractual clauses to a case-by-case inquiry. This domestic and global patchwork imposes costs and potential liability on businesses.

Moving forward in the sphere of data privacy regulation, the United States might value maintaining the sectoral approach as it allows for flexibility and meeting the needs of each industry on its own terms, allowing self-regulation where appropriate. However, *Schrems II* illustrates that despite attempts to self-regulate and allow private companies to contract among themselves in using standard contractual clauses, the GDPR compliance inquiry will entail an evaluation of the country's overall level of data protection in each cross-border transfer that takes place even with SCCs. Private companies face a high degree of uncertainty in their contract negotiations, regarding whether they need supplemental clauses beyond the SCCs and what form supplemental materials should take. Large corporations that engage in business around the globe may find themselves facing negotiations for massive numbers of individual contracts.

148 *California Voters Adopt the California Privacy Rights Act*, *supra* note 50.

149 *See, e.g.*, European Commission Press Release IP/19/421, European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows (Jan. 23, 2019) (explaining that two of the key reasons for the adequacy decision were a "complaint-handling mechanism" for European citizens supervised by an independent data authority and additional safeguards for companies to follow, also enforced by an independent data authority).

Generally, separate jurisdictions have an ability to enact contradictory or potentially confusing legislation, regardless of the compliance costs it may impose on businesses. The case for data privacy is distinct from the general ability to merely regulate differently. In an increasingly interconnected world, global commerce is driven by and dependent on the use of the internet. Uniformity, or at the least consistency and centralization, is key to the continuation of international trade. The European Union has already enacted the GDPR to govern the personal data of its data subjects, and its influence on the global market has resulted in most businesses complying out of necessity. Its framework and application in *Schrems I* and *Schrems II*, which deems other jurisdictions "adequate" if they are "essentially equivalent" to the GDPR, means that the European Commission will shut off a massive segment of world consumers to private businesses after evaluating another country's domestic policies and finding them inferior to their own.

Schrems II implies that a third workaround using a self-certification agreement between the United States and the European Union would be struck down for similar reasons as Safe Harbor and Privacy Shield. Having a centralized U.S. federal data privacy law provides a baseline for evaluating the United States as a potentially "equivalent" jurisdiction to the GDPR in level of data protection. Although the U.S. version of a data privacy law is unlikely to be substantively similar to the GDPR, recent proposed bills indicate reliance on similar principles of data governance that could provide common ground in the future.[150] The United States should use this opportunity to bring the benefits of a different history of data privacy to the global conversation on data privacy.

150 *See* Kerry & Chin, *supra* note 5 (noting that proposed federal data privacy bills promote "data minimization, individual privacy rights, transparency, and discriminatory uses of personal data."). For a suggested federal data privacy bill that draws from several prior bills, see generally CAMERON F. KERRY, JOHN B. MORRIS, JR., CAITLIN T. CHIN & NICOL E. TURNER LEE, BROOKINGS. INST., BRIDGING THE GAPS: A PATH FORWARD TO FEDERAL PRIVACY LEGISLATION (2020), https://www.brookings.edu/wp-content/uploads/2020/06/Bridging-the-gaps_a-path-forward-to-federal-privacy-legislation.pdf.