Boston College Law Review

Volume 62 | Issue 7 Article 9

10-26-2021

Using State-Based Adequacy Now, National Adequacy Over Time to Anticipate and Defeat *Schrems III*

Emily A. Ivers
Boston College Law School, emily.ivers@bc.edu

USING STATE-BASED ADEQUACY NOW, NATIONAL ADEQUACY OVER TIME TO ANTICIPATE AND DEFEAT *SCHREMS III*

Abstract: Consequent to their incongruous developments of data privacy law, the European Union and United States have struggled to lawfully trade data with one another. Both nevertheless aspire to make the transfers occur. Therefore, they have negotiated two agreements for lawful data trade: (1) Safe Harbor and (2) Privacy Shield. But the European Union has also required the United States to guarantee nearly "equivalent" protections to its own. Given the Court of Justice of the European Union's decisions in *Schrems v. Data Protection Commissioner* (*Schrems I*) and *Data Protection Commissioner v. Facebook Ireland Ltd.* (*Schrems II*) to invalidate the agreements, achieving the equivalency requirement will be demanding. This Note contends that the upcoming successor agreement should allow well-suited states in the United States to obtain "adequacy" determinations for themselves, rather than trying to adapt the structurally dissimilar federal legislation to meet European Union standards. This approach is the only realistic way to anticipate and defeat an inevitable "*Schrems III*" court challenge.

INTRODUCTION

Today's hottest commodity on the transatlantic trade market, personal data, has all but eliminated the greatest concern faced by its predecessors: getting from the shore of one continent to another.[1] But the resolution to this problem has merely sowed the seed of a new hurdle.[2] Although recent advances in technology have made trading personal information via data more effortless and immediate, its transfer poses an unsettling question—what can happen to the information once it has arrived?[3]

---

[1] *See* Daniel Alvarez, *Safe Harbor Is Dead; Long Live the Privacy Shield?*, A.B.A. (May 20, 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/05/09_alvarez/ [https://perma.cc/B5V5-K8UZ] (commenting on the history of transatlantic travel); Václav Janeček, *Trade in Data: Constructive Limits of Personal Data Ownership*, OXFORD BUS. L. BLOG (May 31, 2018), https://www.law.ox.ac.uk/business-law-blog/blog/2018/05/trade-data-constructive-limits-personal-data-ownership [https://perma.cc/VK4P-NYDV] (commenting on the economic viability of trading personal data). Centuries ago, it could take several months for a traded good to travel between Europe and the United States (US). Alvarez, *supra*. In contrast, a data point can travel from one side of the Atlantic to the other at the "speed of light." *Id.*

[2] *See* DEBORAH HURLEY, POLE STAR: HUMAN RIGHTS IN THE INFORMATION SOCIETY 12–13 (2003) (connecting the advances in modern technology with the concern for their ability to spread the information they collect).

[3] *See id.* at 12, 19 (describing technology, and thus the data it produces, to be "ubiquitous" and increasingly troublesome); Alvarez, *supra* note 1 (admiring just how fast transatlantic trade has become).

The European Union (EU) and United States (US) have been embroiled in a conflict to determine the best answer to this question for decades.[4] Although both agree that personal data is private, and thus deserves protection, they disagree about the measures necessary to guarantee individuals this right.[5] Consequently, they have had to negotiate a middle ground to allow personal data to remain on the transatlantic trade market.[6]

Despite both governments' attempts to reach a compromise, Austrian privacy activist Maximillian Schrems has twice thwarted their efforts.[7] Finding victory before the Court of Justice of the European Union (CJEU) both in 2015, in *Schrems v. Data Protection Commissioner* (*Schrems I*), and in 2020, in *Data Protection Commissioner of Ireland v. Facebook Ireland Ltd.* (*Schrems II*), Schrems wiped out two agreements that previously allowed the EU and US to trade data, Safe Harbor and Privacy Shield.[8] Left without a valid transatlantic agreement, companies have had to implement unpredictable and potentially inapplicable "mechanisms" to make such transfers.[9] Unfortunately for businesses, even an unknowingly improper use of European data can result in extremely harsh financial backlash.[10] Although the Department of Commerce

---

[4] *See* Owen McCoy, *A Legislative Comparison: US vs. EU on Data Privacy*, EUR. INTERACTIVE DIGIT. ADVERT. ALL. (Mar. 31, 2020), https://edaa.eu/a-legislative-comparison-us-vs-eu-on-data-privacy/ [https://perma.cc/7T3A-3QZ9] (contrasting the way that the European Union (EU) and US have developed privacy legislation to best protect personal information and its transfers).

[5] *EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce*, PRIV. SHIELD FRAMEWORK, https://www.privacyshield.gov/servlet/servlet.FileDownload?file015t00000004qAg [https://perma.cc/U2DS-HMLK].

[6] *See* MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RSCH. SERV., R44257, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 1, 4 (2016) (explaining the need for the two governments to negotiate a way to continue data trade between themselves).

[7] *See* Case C–311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶ 201 (July 16, 2020) (invalidating the Privacy Shield framework); Case C–362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650, ¶ 106 (Oct. 6, 2015) (invalidating the Safe Harbor framework). Maximillian Schrems originally grew concerned with data privacy as a law student in California. Interview by James Jacoby with Max Schrems, Priv. Advoc. (Mar. 28, 2018) (transcript available at https://www.pbs.org/wgbh/frontline/interview/max-schrems/ [https://perma.cc/TVU6-EHF3]). During one of his classes, a Facebook, Inc. (Facebook) representative commented that, although the EU had privacy regulations, the company did not follow them because the EU did not actually prosecute the laws. *Id.* This sparked Schrems to examine EU privacy law and data practices of the popular social media platforms he used. *Id.* Deeply disturbed with the results of his inquiries, Schrems chose to act and eventually sued Facebook. *Id.*

[8] *See Schrems II*, ECLI:EU:C:2020:559, ¶ 201 (ending the applicability of the Privacy Shield mechanism); *Schrems I*, ECLI:EU:C:2015:650, ¶ 106 (terminating the Safe Harbor mechanism).

[9] *See* Davide Szép, *America's Tech Giants: It's Back to the Drawing Board on European Data*, 92 N.Y. STATE BAR J. 45, 46 (2020) (commenting that any US organization that still seeks to collect data from the EU must do so via an "alternative mechanism[]"). The most common alternative mechanisms that businesses use to obtain data from the EU are "Standard Contractual Clauses (SCCs)" and "Binding Corporate Rules (BCRs)." *Id.*; *see also infra* notes 144–147 and accompanying text (summarizing how to use SCCs and BCRs to make lawful data transfers).

[10] *See* Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the

commented in August 2020 on the possibility of developing a new and more compliant agreement with the EU, it remained silent on how it could accomplish this goal.[11] Thus, with *Schrems III* being not only predictable but inevitable, how can the US guarantee the success of the third transatlantic data transfer agreement?[12]

This Note contends that the reason for the invalidation of both Safe Harbor and Privacy Shield is inherent in the inability to disguise the US's sectoral data privacy system as one comparable to the EU's omnibus legislation.[13] It remains imperative to quickly find a balance between the strict standards of the EU and the sectoral structure of US law to fulfill the economic needs of both parties.[14] But it is unlikely that they can achieve a meaningful degree of equiv-

---

Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 83(2)(b), 2016 O.J. (L 119) 1, 82 (considering, but not excluding, the awareness that the business had when calculating fines for a misuse of EU data); *GDPR Fines Database—List of Fines*, INT'L NETWORK OF PRIV. L. PROS., https://gdpr-fines.inplp.com/list/ [https://perma.cc/9BP9-YHUJ] (listing General Data Protection Regulation (GDPR) fines that range from several hundred euros to several million). For example, an individual in Austria was fined €2,200 for use of a personal security camera which recorded public entry ways to a residential building. *GDPR Fines Database—List of Fines*, *supra*.

Acknowledging that not all European countries belong to the EU, this Note uses the word "European" to refer only to EU countries and their citizens. *Compare Countries*, EUR. UNION, https://europa.eu/european-union/about-eu/countries_en [https://perma.cc/FB8D-Z2ZC] (listing the countries belonging to the EU), *with Countries of Europe*, NATIONS ONLINE, https://www.nationsonline.org/oneworld/europe.htm [https://perma.cc/CYE4-3R9L] (listing all European countries).

[11] *See* Press Release, U.S. Dep't of Com., Joint Press Statement from U.S. Secretary of Commerce Wilbur Ross and European Commissioner for Justice Didier Reynders (Aug. 10, 2020), https://useu.usmission.gov/joint-press-statement-from-u-s-secretary-of-commerce-wilbur-ross-and-european-commissioner-for-justice-didier-reynders/ [https://perma.cc/D56L-TJ52] (detailing the collective and public response made by the EU and US in response to the *Schrems II* decision). The parties stated that they had merely begun to consider replacing Privacy Shield. *Id.* The released statement suggested that the world's economic environment might play a role in the necessity to find a new way to lawfully trade data. *See id.* (referencing the importance of finding "prosperity" during a time of significant struggle).

[12] *See* HENDRIK MILDEBRATH, EUR. PARL. RSCH. SERV., PE 652.073, THE CJEU JUDGMENT IN THE *SCHREMS II* CASE (2020), https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf [https://perma.cc/6BQR-M38P] (acknowledging that Schrems' proposed course of action is not likely to occur before a replacement to Privacy Shield is made). Schrems suggested that the US must change its surveillance law to continue to trade data with the EU. *Id.* That result, nevertheless, is unlikely to happen. *See id.* (claiming there was not enough time to accomplish this feat). Although it remains unclear when to expect a new agreement, making the changes that Schrems proposes would require a complete "overhaul" of current US law that would take a considerable amount of time and effort. *Id.*

This Note does not use the term "*Schrems III*" to reference or suggest the current existence of such a case, but rather to predict the likelihood of such a case upon the development of a new transatlantic data privacy transfer mechanism. *See generally Schrems II*, ECLI:EU:C:2020:559, ¶ 201 (ending the validity of the Privacy Shield mechanism); *Schrems I*, ECLI:EU:C:2015:650, ¶ 106 (voiding the Safe Harbor mechanism).

[13] *See infra* notes 22–260 and accompanying text.

[14] *See* Cassandra Liem et al., *The Economic Value of Personal Data for Online Platforms, Firms and Consumers*, RUEGEL (Jan. 14, 2016), https://www.bruegel.org/2016/01/the-economic-value-of-

alence at a national level before a potential *Schrems III* challenge.[15] This Note suggests that the US should draft an adequacy agreement that is state-specific, focusing on the individual states with privacy standards most similar to those in the EU.[16] In this way, the US could take a piecemeal approach that could effectuate a nationwide mechanism for transatlantic personal data trade over time.[17] Allowing a state like California to obtain individual adequacy might incentivize the US as a whole to raise its privacy standard and achieve nationwide adequacy over time.[18]

Part I of this Note introduces the conflicting privacy protection approaches taken by the EU and US that led to the ultimate demises of the previous two transatlantic data transfer agreements, Safe Harbor and Privacy Shield.[19] Part II contemplates the current strive for a future privacy agreement and surveys US privacy laws on the state level.[20] Part III proposes that negotiating multiple state-specific adequacy determinations, rather than a single nationwide one, is necessary to a new agreement's success and the continued trade of data between the EU and US.[21]

I. Harbor Drained, Shield Lowered: Schrems Makes Developing a Transatlantic Data Privacy Agreement a Losing Battle

Privacy is a long-recognized right that is necessary to the global community.[22] But privacy concerns have recently grown as individuals more regularly

---

personal-data-for-online-platforms-firms-and-consumers/ [https://perma.cc/3QLK-VG66] (showing the monetary benefit that data brings to different stakeholders). The economic advantages of data trading may be reflected in the revenue that advertising brings to businesses. *See id.* (explaining the "advertising revenues per user" calculation and its significance). Businesses can use personal data to better tailor advertisements to users of a platform, and in turn, the users are more likely to click on the advertisement. *Id.* As a result, data trading is a lucrative venture for the business. *See id.* (giving the example of Facebook's extreme growth in advertising-based revenue over time).

[15] *See* Mildebrath, *supra* note 12 (recognizing that what might be the best course of action for the US is not necessarily a practical one); *see also infra* notes 22–260 and accompanying text (showing that national adequacy is unlikely to occur in the near future because the US's privacy structure is deeply incompatible with the EU's). Schrems recently developed an organization, aptly named "noyb," an abbreviation for "none of your business," to pursue data privacy cases like *Schrems I* and *Schrems II*. *Max Schrems Launches a New NGO That Is None of Your Business*, GDPR Informer (Jan. 25, 2018), https://gdprinformer.com/news/max-schrems-launches-new-ngo-none-business [https://perma.cc/B6ZF-XJ4T]; *Our Detailed Concept*, NYOB, https://noyb.eu/en/our-detailed-concept [https://perma.cc/5SFS-XMGA] (explaining the organization's goals and practices).

[16] *See infra* notes 216–260 and accompanying text.

[17] *See infra* notes 232–260 and accompanying text.

[18] *See infra* notes 232–260 and accompanying text.

[19] *See infra* notes 22–154 and accompanying text.

[20] *See infra* notes 155–215 and accompanying text.

[21] *See infra* notes 216–260 and accompanying text.

[22] *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948) (recognizing that a person has a natural-born right to withhold certain information from others); Deborah Hurley, *Taking the Long Way Home: The Human Right of Privacy*, *in* Privacy in the Modern

divulge their personal information, called "personal data."[23] "Personal data" refers to any statistic or detail that pertains to the identity of a person.[24] This

AGE: THE SEARCH FOR SOLUTIONS 70, 72 (Marc Rotenberg et al. eds., 2015) (explaining the global acknowledgement of privacy as a human right over seventy years ago); *see also* Hurley, *supra*, at 72 (stating that the safekeeping of private information promotes "autonomy, self-determination, and dignity"). In the mid-twentieth century, two international documents declared a fundamental right to not have one's privacy unjustifiably invaded. *See* Hurley, *supra*, at 72 (referencing the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights). In 1993, the World Conference on Human Rights made clear that "human rights" were absolute and applicable to the entire human population. *World Conference and the Vienna Declaration*, BBC WORLD SERV., http://www.bbc.co.uk/worldservice/people/features/ihavearightto/four_b/treaties_vienna.shtml [https://perma.cc/ZJ48-YXK4]. During this conference, a significant majority of recognized sovereign countries signed a commitment to further these human rights globally. *See id.* (stating that 171 nations were party to the Vienna Declaration and Programme of Action); *see also Growth in United Nations Membership*, UNITED NATIONS, https://www.un.org/en/about-us/growth-in-un-membership [https://perma.cc/QEJ8-V3JX] (recognizing the existence of 184 member states in 1993). Advances in technology have also changed the nature of privacy concerns over time. *Compare* Katz v. United States, 389 U.S. 347, 349 (1967) (providing a Fourth Amendment privacy case that questioned the legality of police using wiretap technology to obtain information without the individual's knowledge), *with* Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (exemplifying an older Fourth Amendment privacy case that focused on the marital privacy rights of a married woman and her ability to use birth control). In *Katz*, the Supreme Court extended Fourth Amendment protection beyond the previous requirement that "physical intrusion" was necessary to be a violation. 389 U.S. at 360 (Harlan, J., concurring). It, thus, forbade the abuse of wiretap technology to breach an individual's private conversations. *Id.* at 359 (majority opinion). As the Court noted, individuals have a "*general* right to privacy" and a "right to be let alone." *Id.* at 350.

[23] *See* HURLEY, *supra* note 2, at 19, 24 (explaining that data is omnipresent). By 2020, there was more data than visible stars. Branka Vuleta, *How Much Data Is Created Every Day? [27 Staggering Stats]*, SEEDSCIENTIFIC (Jan. 28, 2021), https://seedscientific.com/how-much-data-is-created-every-day/ [https://perma.cc/76FU-FG4T]; *Data Never Sleeps 8.0*, DOMO, https://www.domo.com/learn/infographic/data-never-sleeps-8 [https://perma.cc/YZ3G-TCLF] (claiming that the world produces millions of different data records in just one minute).

Although people should decide what they do or do not share with outsiders, recent innovations have reduced the ability to safekeep personal data. *See* HURLEY, *supra* note 2, at 19, 24 (describing the ability of technology to dissipate information). For example, without the existence of technology, much of an individual's personal information remains relatively private, unless the individual directly chooses to share it. *See* Mary Atamaniuk, *20 Years in Digital Privacy: How the Definition Has Evolved*, CLARIO (July 3, 2020), https://clario.co/blog/privacy-definition-over-years/ [https://perma.cc/XJ6U-JFGJ] (explaining that for much of history, privacy protection was as straightforward as not telling others your secrets). Thus, individuals acted as the gatekeeper to their own privacy. *Id.* The decision to reveal any such information, therefore, inherently reduced the expectation to it remaining private. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (explaining that the willing disclosures made to a phone company delegitimized the individual's claim to privacy over his telephone history). This is far less applicable in today's technology-dominated environment, wherein personal information can be collected and disseminated without the individual's knowledge. *See* Carpenter v. United States, 138 S. Ct. 2206, 2261–63 (2018) (Gorsuch, J., dissenting) (claiming that newer technology has become so integrated into our daily lives and holds such deeply personal information that it limits the practicality of older privacy doctrines); *see also* HURLEY, *supra* note 2, at 19 (acknowledging the sheer amount of data collection); Atamaniuk, *supra* (noting that, over time, companies have become increasingly skilled at using their customers' personal information). Even people who do not intend to create personal data do so. *See* Atamaniuk, *supra* (commenting that the infamous Facebook-Cambridge Analytica data abuse involved many individuals who were oblivious to data practices).

broad category of information has a vast range of uses that have proven to be incredibly lucrative.[25] Nevertheless, the incentives to expansively use personal data strain against the potential risks it poses to human rights.[26] To uphold their

---

Everyday actions like turning on a lightbulb or using a car's navigation service generate data related to that individual. *See, e.g.*, Geoffrey A. Fowler, *What Does Your Car Know About You? We Hacked a Chevy to Find Out.*, WASH. POST (Dec. 17, 2019), https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out/ [https://perma.cc/WU2U-S8H2] (explaining that a car's internal computer, like any other computer, can and does collect information on the driver); *These LED Smart Lights Are Tracking Your Moves*, CBS NEWS (June 30, 2014), https://www.cbsnews.com/news/technology-in-led-smart-lights-raises-privacy-concerns/ [https://perma.cc/9HXT-5NEF] (providing an example of a lightbulb that was praised for its energy-saving capabilities and was also collecting data on its users).

[24] INFO. COMM'R'S OFF., GUIDE TO THE GENERAL DATA PROTECTION REGULATION (GDPR) 9–10 (2021), https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf [https://perma.cc/E85E-6CYG]. *See generally* Regulation (EU) 2016/679, *supra* note 10 (laying out the provisions of the EU's omnibus GDPR legislation). Many different types of information concerning an individual can be used to ascertain their identity. Regulation (EU) 2016/679, *supra* note 10, art. 4, at 33. For example, personal data includes information like: a "name," government "identification number," "location," and even biometric information. *Id.*

[25] *See* MATTHEW NORTH, DATA MINING FOR THE MASSES 13 (2012) (ebook) (listing everyday activities like buying food, filling the gas tank, going out to dinner, or picking up mail that can all create a digital footprint of an individual); Liem et al., *supra* note 14 (stating that data and its use is a multi-billion-dollar industry and is growing). On a macroscopic level, an aggregate of data can predict general patterns and trends. *See* NORTH, *supra*, at 14 (examining how a business can amass data to generate profiles for the preferences of different demographics of its customers). By connecting data points, retailers can determine which products are most popular and where to sell certain products. *See id.* (exemplifying how a grocery store might benefit from requiring shoppers to provide their location and sex when they acquire a membership card for discount eligibility). Simultaneously, it can give incredibly detailed insight to the preferences and demographics of a single individual. *See id.* (commenting that the same information can be used to tailor an advertisement to an individual).

[26] *See* G.A. Res. 217 (III) A, *supra* note 22, art. 12 (claiming privacy protection to be fundamentally important); Kari Paul, *Americans' Data Is Worth Billions—and You Soon Might Be Able to Get a Cut of It*, MARKETWATCH (Oct. 9, 2018), https://www.marketwatch.com/story/americans-data-is-worth-billions-and-you-soon-might-be-able-to-get-a-cut-of-it-2018-10-09 [https://perma.cc/AU99-NZBZ] (claiming that corporations like Instagram and Twitter can sell their users' personal information to advertisers for billions of dollars each year). Although many processors and collectors are likely well-intentioned, the inherent nature and sheer volume of information welcomes the possibility for misuse. *See* Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, FORBES (May 21, 2018), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=2d19600660ba [https://perma.cc/AH3G-P76K] (commenting on the extremely large amount of data that an individual person creates). Some breaches of personal information may be potentially more detrimental than others. *See, e.g.*, *Consumer Financial Protection Bureau Fines Wells Fargo $100 Million for Widespread Illegal Practice of Secretly Opening Unauthorized Accounts*, CONSUMER FIN. PROT. BUREAU (Sept. 8, 2016), https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-fines-wells-fargo-100-million-widespread-illegal-practice-secretly-opening-unauthorized-accounts/ [https://perma.cc/AT2Q-8NFL] (presenting the extreme abuse made by a financial agency when it opened unauthorized accounts by using data that it had collected on its members). *See generally* Jim Zarroli, *Wells Fargo's Unauthorized Accounts Likely Hurt Customer's Credit Scores*, NPR (Sept. 26, 2016), https://www.npr.org/2016/09/26/495501008/wells-fargos-unauthorized-accounts-likely-hurt-customers-credit-scores [https://perma.cc/DY5J-J5GK] (criticizing

commitment to the fundamental right to privacy, countries have developed legislation to offset dangerous data abuses.[27] Although most countries have promulgated strong privacy legislation for their constituents, they have not necessarily done so in similar ways.[28]

While developing their own personal data privacy protection systems, the EU and US diverged into two incongruous systems that have since throttled transatlantic data transfer.[29] As a result, they have struggled to find a mechanism that allows seamless and lawful transfers of EU data to the US.[30] Section

---

the company's privacy violation for the damage done to its customers by deteriorating their personal financial leverage).

[27] *See generally* World Conference on Human Rights, *Vienna Declaration and Programme of Action*, U.N. Doc. A/CONF.157/23 (June 25, 1993), (providing the agreement of nations to guarantee human rights across the globe); *Data Protection and Privacy Legislation Worldwide*, UNCTAD, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide [https://perma.cc/RCE2-MMJV] (demonstrating that two-thirds of countries in the world have privacy legislation in place and another tenth that have initiated legislation to come). National privacy laws purport to safeguard the integrity of personal data far beyond its initial disclosure. *See Fair Information Practice Principles*, IAPP, https://iapp.org/resources/article/fair-information-practices/ [https://perma.cc/Z2J6-WPF4] (listing eight nonbinding Fair Information Practice Principles (FIPPs) that reflect several best practices for data before and after collection); *FIPPs*, NIST, https://csrc.nist.gov/glossary/term/FIPPs [https://perma.cc/647K-839W] (defining FIPPs as a set of exemplary concepts that promote better privacy legislation across the world). The FIPPs first gained traction in the 1970s. *FIPPs*, *supra*. They suggest that entities: (1) minimize the amount data that they collect, (2) maintain only high caliber data, (3) divulge their reason to collect data accurately, (4) obtain user consent, (5) secure the personal information, (6) be forthcoming about their data practices, (7) provide individuals with rights to their own information, and (8) meaningfully adhere to the preceding practices. *Fair Information Practice Principles*, *supra*.

[28] *See What's Data Privacy Law in Your Country?*, PRIV. POL'YS, https://www.privacypolicies.com/blog/privacy-law-by-country/ [https://perma.cc/7YVG-ETZB] (Sept. 4, 2019) (providing information about the status of various countries' current regulations). For example, in New Zealand, data collectors must gather personal information straight from the user and provide reciprocal information about the collector. *Id.* Meanwhile, India requires websites to include a privacy policy that details what type of information they collect and where that information may go after collection. *Id.*

[29] *See* W. Gregory Voss, *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, 2019 U. ILL. J.L. TECH. & POL'Y 405, 407, 410 (bringing attention to the lack of similarity between the EU's and US's frameworks); *EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce*, *supra* note 5 (acknowledging that, by developing a "sectoral" data privacy framework, the US has distinguished itself from the EU). Notably, the lack of conformity between privacy laws at any level can cause issues or obstruct the free flow of data. *See* Voss, *supra*, at 410 (claiming that the success of data trade depends on the analogousness of privacy regulations); *see also* Nicholas Blackmore, *Feeling Inadequate? Why Adequacy Decisions Are Rare (and May Get Rarer) in Asia-Pacific*, KENNEDYS (Mar. 26, 2019), https://kennedyslaw.com/thought-leadership/article/feeling-inadequate-why-adequacy-decisions-are-rare-and-may-get-rarer-in-asia-pacific/ [https://perma.cc/2ETE-SG5U] (commenting on the struggle faced by Asian-Pacific countries, with the sole exception of Japan, to obtain adequacy determinations given their privacy regimes).

[30] *See* Case C–311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶ 201 (July 16, 2020) (making the Privacy Shield agreement inoperable); Case C–362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650, ¶ 106 (Oct. 6, 2015) (demonstrating the similar result in the court challenge to the Safe Harbor agreement). Although alternative mechanisms do exist, it is not necessarily clear how to properly or uniformly use them. *See* MILDEBRATH, *supra* note 12 (noting that there is no universally applicable answer to the usability of SCCs made in the *Schrems*

A of this Part discusses the tension between personal freedoms and economic interests that is inherent to data privacy regulation.[31] Section B juxtaposes the EU's omnibus approach to privacy law with the US's sectoral one.[32] Section C provides background to the development and demise of the first agreement aimed to resolve the tension, Safe Harbor.[33] Section D introduces its most recent successor, Privacy Shield, and chronicles its similar fate.[34]

A. Perfectly Private? Governments Weigh Individual Privacy Rights with National Economic Proclivities

In the twenty-first century, data collection has become common in the average person's life and a token of the global economy.[35] The ability to collect and use data does not have any natural physical restrictions.[36] Likewise, the enormous amount of data that exists only continues to grow.[37] Thus, without

---

II decision); Ruth Boardman et al., *Safe Harbor Invalid: FAQs*, BIRD & BIRD (Nov. 2015), https://www.twobirds.com/en/news/articles/2015/global/safe-harbor-invalid-faqs [https://perma.cc/JN42-FK9V] (suggesting that the alternatives are merely "short term" solutions).

[31] *See infra* notes 35–73 and accompanying text.

[32] *See infra* notes 74–111 and accompanying text.

[33] *See infra* notes 112–130 and accompanying text.

[34] *See infra* notes 131–154 and accompanying text.

[35] *See* Daniel J. Grimm, *The Dark Data Quandary*, 68 AM. U. L. REV. 761, 763 (2019) (recognizing that people are generally aware of the abundance of data in their daily lives); Dennis D. Hirsch, *The Glass House Effect: Big Data, the New Oil, and the Power of Analogy*, 66 ME. L. REV. 373, 374–75 (2014) (reiterating the worldwide impact of data with the commonly-used comparison "data is the new oil"); *see also* Kenneth Cukier & Viktor Mayer-Schoenberger, *The Rise of Big Data: How It's Changing the Way We Think About the World*, 92 FOREIGN AFFS., May/June 2013, at 28, 28 (commenting on the impressive growth of data practices since 2000).

[36] *See* D. Daniel Sokol & Roisin Comerford, *Antitrust and Regulating Big Data*, 23 GEO. MASON L. REV. 1129, 1137 (2016) (observing that the use of a specific piece of data by one entity does not preclude another from using the same information). When multiple people can indulge in the same resource contemporaneously, it is called a "non-rivalrous good." *Non-Rivalrous Goods*, CFI, https://corporatefinanceinstitute.com/resources/knowledge/economics/non-rivalrous-goods/ [https://perma.cc/4AZP-NJPH]. In contrast, the classic legal example of a rivalrous resource comes from *Pierson v. Post*. *See* 3 Cai. 175, 177 (N.Y. Sup. Ct. 1805) (questioning which hunter had the right to a fox that was killed during a simultaneous hunt). In *Pierson,* only one of the two hunters could have property rights in the animal because the possession of the fox by one man necessarily barred the other's possession. *See id.* at 179–80 (finding that only he who actually holds the fox has a right to it).

[37] *See* OPENVAULT, BROADBAND INSIGHTS REPORT (OVBI): 1Q 2020, at 2 (2020), https://openvault.com/NEW-SITE-OV3/wp-content/uploads/2021/02/Openvault_Q120_DataUsage_FINAL.pdf [https://perma.cc/HNR9-BDYE] (calculating the 47% growth in data utilization between the first fiscal quarters of 2019 and 2020); *State of BI & Analytics Report*, SISENSE, https://www.sisense.com/whitepapers/state-of-bi-analytics-report-2020/ [https://perma.cc/4YR5-W327] (detailing the increased application of data practices in a broad range of corporate functions, such as productivity and customer assistance). In 2020, the amount of data used and produced rapidly surged in tandem with the flux of individuals working and socializing from their devices at home. *See* Autumn Molay & Ryan Williams, *In-Home Data Usage Increases During Coronavirus Pandemic*, COMSCORE (Mar. 24, 2020), https://www.comscore.com/Insights/Blog/In-Home-Data-Usage-Increases-During-Coronavirus-

external regulation, the potential for its accrual is limitless, and the incentive to do so is large.[38]

And yet, there is no obvious or commonly accepted standard for personal data regulation.[39] Legislatures face the difficult challenge of balancing corporate profitability with the individual privacy concerns of their citizens.[40] Strict privacy regulations decrease the amount of data that a corporation can collect and sell.[41] Alternatively, weak privacy regulations leave peoples' personal information at risk.[42] Thus, data regulation necessarily puts national economic success at odds with the rights of individuals.[43] Subsection 1 of this Section assesses the commercial potential for personal data on the trade market.[44] In contrast, Subsection 2 considers the personal privacy concerns that are also tied to the sale of data.[45]

Pandemic [https://perma.cc/GW3J-UU47] (noting the impact that COVID-19 restrictions had on the incidence of data production).

[38] *See* ALBERT OPHER ET AL., THE RISE OF THE DATA ECONOMY: DRIVING VALUE THROUGH INTERNET OF THINGS DATA MONETIZATION 2 (2016), https://www.ibm.com/downloads/cas/4JROLDQ7 [https://perma.cc/3SY7-7GP9] (noting that data practices are becoming more straightforward); Angela Byers, *Big Data, Big Economic Impact?*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 757, 759–60 (2015) (highlighting the monetary implications of efficient data manipulation); Sokol & Comerford, *supra* note 36, at 1137 (commenting on the ability of many entities to control the same data at once). Efficient data application can propagate billions to trillions of dollars for the US's corporate economy. *See* Byers, *supra*, at 759–60 (cumulating studies to suggest that the American retail and manufacturing industries can conserve massive sums of money just by properly leveraging data).

[39] *See Data Protection Laws of the World*, DLA PIPER, https://www.dlapiperdataprotection.com [https://perma.cc/ZM4U-TJ8X] (depicting the vigorousness of privacy protection across the globe). Despite their differences, EU countries and the US both have strong privacy regulation when compared with countries like Botswana, Kenya, and Paraguay. *See id.* (categorizing countries into four levels of privacy standards, and placing the EU nations and the US in the strongest regulatory category).

[40] *See* Hirsch, *supra* note 35, at 375 (acknowledging the concurrent advantages and disadvantages of trading personal data).

[41] *See id.* (presenting privacy and profitability as a sliding scale of interests). Thus, as privacy rights increase, the profitability of data can decrease. *See id.*

[42] *See* Frank Pasquale, *7 Ways Data Currently Being Collected About You Could Hurt Your Career or Personal Life*, HUFFPOST https://www.huffpost.com/entry/data-collected-hurt-career-personal_b_6110682 [https://perma.cc/Y8A3-3WSH] (Dec. 6, 2017) (describing a wide range of privacy misuses that might occur but are rarely considered by the individual). In addition to more classic and predictable misuses of data, there are some more zany examples of its abuse as well. *Id.* For example, data misrepresentation can lead to improper implications in a drug crime, or even nefarious actors collecting disposed coffee cups to gather genetic information from its long-gone drinker. *Id.*

[43] *See* Hirsch, *supra* note 35, at 375 (linking the quantity of data to its potential danger).

[44] *See infra* notes 46–59 and accompanying text.

[45] *See infra* notes 60–73 and accompanying text.

1. Economic Incentives Favor the Broad Sale of Data

Data is incredibly lucrative and can holistically increase the wealth of its constituents.[46] Throughout history, merchants have used the personal preferences of their customers to drive their economic success in the market.[47] Today, modern businesses can even manipulate individualized data to better develop, peddle, and sell goods, all while evading the costs of generalized mass marketing.[48] As consumer information has become digitally discernable and more easily acquired, the associated riches have likewise grown.[49] Therefore, many companies have focused an increasing amount of their resources on processing more data and leveraging it for profit.[50] Both large and small businesses have begun to accrue massive amounts of revenue from doing so in recent years.[51] Personal data currently approaches a multi-trillion dollar industry.[52]

---

[46] *See* Byers, *supra* note 38, at 761 (explaining that data can benefit individuals, even in obscure ways like decreasing the time and cost associated with travel); Mat Travizano, *The Tech Giants Get Rich Using Your Data. What Do You Get in Return?*, ENTREPRENEUR (Sept. 28, 2018), https://www.entrepreneur.com/article/319952 [https://perma.cc/658T-JSL9] (claiming that Google alone can earn over $3 billion from data each quarter). Information that can be leveraged for profit can come from many sources, including geographic location, energy production, car sensors, pulse trackers, and spatial comparisons. *See* OPHER ET AL., *supra* note 38, at 6–7 (giving examples of different areas of data that a business might utilize to make money).

[47] *See Big Data Analytics: What It Is and Why It Matters*, SAS, https://www.sas.com/en_us/insights/analytics/big-data-analytics.html [https://perma.cc/P47K-J5K3] (claiming that retailers used data as a marketing tool in the 1950s). Over half a century ago, before data was a digital concept, vendors analyzed personal data to stay in tune with their consumers' preferences. *See id.* (explaining that retailers compile data in ledgers and manipulate it to keep in vogue).

[48] *See* ALESSANDRO ACQUISTI, THE ECONOMICS OF PERSONAL DATA AND THE ECONOMICS OF PRIVACY 8 (2010), https://www.oecd.org/sti/ieconomy/46968784.pdf [https://perma.cc/BQQ7-W53P] (noting that a business can scrutinize a collection of personal data to forecast the future of its industry and meet the desires of its consumers). In 2009, the sale of goods using web-based marketing accounted for a $300 billion revenue in the US alone. *Id.* From analyzing the data that they collect, retailers can learn how to target their advertisements to those most likely to purchase the item and determine which products or improvements the market desires most. *See id.* at 8–9 (explaining several ways that a business can use the data to alter its behavior). It can, thus, reduce the overhead costs that might elsewise counteract its profit. *See id.* (concluding that these changes are economically prudent).

[49] *See Big Data Analytics*, *supra* note 47 (claiming that businesses can find success from the newfound momentum of personal data collection). Two ways that a company can discern valuable information from data are through prognostic analyses and self-teaching artificial intelligence. *See id.* (defining the practices of "predictive analytics" and "machine learning"). Both practices use informational input to develop more suitable output for future transactions. *Id.*

[50] *See* Byers, *supra* note 38, at 757 (flagging data as a primary concern for many businesses, especially those in the tech space); Sokol & Comerford, *supra* note 36, at 1129 (recognizing that businesses gather significantly more data via the internet than ever before).

[51] *See* Joseph Kennedy, *Big Data's Economic Impact*, COMM. FOR ECON. DEV., https://www.ced.org/blog/entry/big-datas-economic-impact [https://perma.cc/S97A-495J] (citing that US data utilization could earn upwards of $1.3 trillion just from seven fields of business). Businesses that use data to guide their practices work better and faster than their non-data using counterparts. *See* Andrew McAfee & Erik Brynjolfsson, *Big Data: The Management Revolution*, HARV. BUS. REV. (Oct. 1, 2012), https://hbr.org/2012/10/big-data-the-management-revolution [https://perma.cc/JW8H-URDM] (concluding that decisions based in collected information were at least 5% more effective).

Although its global trade is already incredibly lucrative, the market for data sales expects nearly to double in the upcoming years.[53] National borders do not limit the sale of data.[54] Thus, a country's ability to exchange data extra-territorially can have a significant impact on the profitability of its corporate economy.[55]

In addition to the corporate advantage, individuals can also reap the economic benefits of personal data analysis.[56] Customers may benefit from seeing only ads that they might want or need, paying lower costs for the services they use, and having better products at their disposal sooner.[57] Additionally, several companies have adopted models that allow customers to participate actively and make money off of the collection of their own data.[58] The personal data trade, nevertheless, is not limitlessly beneficial.[59]

2. Individual Privacy Incentives Favor the Restricted Sale of Data

Although personal information is valuable, it can come at a cost to the individual.[60] Data collectors often amass more data than they are capable of put-

---

[52] Kennedy, *supra* note 51.

[53] *See Big Data Market—Global Forecast to 2025*, MARKETSANDMARKETS (Mar. 2020), https://www.marketsandmarkets.com/Market-Reports/big-data-market-1068.html [https://perma.cc/9R9F-39FN] (projecting the expected increase in data revenue between 2020 and 2025). Global data exchange revenues will likely increase from $138.9 billion in 2020 to $229.4 billion by 2025, reflecting an increase in profitability of over 65%. *Id.*

[54] *See* RACHEL F. FEFER, CONG. RSCH. SERV., R45584, DATA FLOWS, ONLINE PRIVACY, AND TRADE POLICY 1 (2019) (reflecting on international trade practices for personal data); Brad McDonald, *Why Countries Trade*, FIN. & DEV., Dec. 2009, at 48, 48 (commenting that countries will decide to trade with each other for the sake of making money and allowing their economies to remain competitive).

[55] *See* Hirsch, *supra* note 35, at 374 (likening data to an asset that can correlate heavily with success in the market).

[56] *See* Sokol & Comerford, *supra* note 36, at 1133–35 (listing ways that individuals may benefit from their own data collection, including the cheapness, caliber, and novelty of the goods that they receive in return). Once data collectors collect and analyze the users' data, they then apply it to tailor their goods or services to the individual consumer. *See id.* at 1134 (explaining how data use can reciprocally help the customers).

[57] *See id.* at 1133 (claiming why highly-tailored data is better).

[58] *See* ACQUISTI, *supra* note 48, at 10 (noting that some businesses will reward customers that disclose their information); *see, e.g.*, *Earn Rewards,* GOOGLE OP. REWARDS HELP, https://support.google.com/opinionrewards/answer/7378183?hl=en#zippy= [https://perma.cc/SP3U-R3TH] (describing their survey-based rewards system). For example, Google Opinion Rewards provides users with data analyst-operated questionnaires. *Earn Rewards*, *supra*. In turn, the program pays users a nominal value for their responses. *See id.* (claiming that a user can earn up to a dollar for each survey).

[59] *See* Hirsch, *supra* note 35, at 378 (continuing the comparison between data and oil to suggest that data is likewise prone to messy complications).

[60] *See* ACQUISTI, *supra* note 48, at 3 (suggesting that over-intrusive data collection can produce a highly accurate record of an individual's life-story that, in turn, creates significant risk).

ting to use.[61] The more information that a corporation collects or trades on a person, the closer the digital fingerprint parallels the individual's actual life experience.[62] In turn, that person becomes increasingly identifiable and subject to inherent risk.[63] Moreover, today's data practices involve far more than just consumer preferences.[64] The average data collector or processor can generate information relating to an individual's geographic location, spending habits, and physical descriptors.[65]

Yet colossal data breaches and nefarious use are common, and the broad collection and trade of data can have serious implications for people's security.[66] Breaches reveal private information to unintended recipients.[67] That information may be used to harm the individual in most, if not all, aspects of life.[68] Most often, ill-intentioned recipients will use the misappropriated data to

---

[61] *See* Grimm, *supra* note 35, at 768 (contending that the vast majority of data that collectors gather then goes unused). Unused and unprocessed data is called "dark data." *Id.* By one estimate, over 90% of all data that exists is dark data. *Id.* at 768–69. In addition to being wasteful, dark data implicates legal concerns because businesses cannot regulate the quality and safety of personal data that they do not know needs protection. *Id.* at 780.

[62] *See* ACQUISTI, *supra* note 48, at 3 (likening a person's data profile to a "dossier").

[63] *See, e.g.*, Khaled El Emam et al., *Evaluating the Risk of Re-identification of Patients from Hospital Prescription Records*, 62 CANADIAN J. HOSP. PHARMACY 307, 307–08, 313–15 (2009) (testing the possibility to pinpoint an individual from their medication-related data and concluding that the probability of identification was high and put the individual's privacy at significant risk).

[64] *See* OPHER ET AL., *supra* note 38, at 6–7 (showing the range of data that a business might wish to collect about a person).

[65] *Id.* at 5–7 (giving examples of ways that a business might collect information and the types of information they may look for).

[66] *See* Hirsch, *supra* note 35, at 378 (predicting that the amount of personal data violations is even higher than the thousands reported); RISK BASED SEC., 2021 MID YEAR REPORT: DATA BREACH QUICK VIEW 2 (2021), https://pages.riskbasedsecurity.com/hubfs/Reports/2021/2021%20Mid%20Year%20Data%20Breach%20Quick View%20Report.pdf [https://perma.cc/UW5S-3BVJ] (stating that the US had at least 1,767 breaches in the first half of 2021); Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling a Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/UD72-8FU5] (detailing that most Americans are deeply worried about the ways that the government and companies use their data to gain information about them). In one of the more significant data breaches, hackers accessed the information of approximately one hundred million Target Corp. customers in December 2013. Hirsch, *supra* note 35, at 378.

[67] *How Data Breaches Happen*, KASPERSKY, https://usa.kaspersky.com/resource-center/definitions/data-breach [https://perma.cc/5757-PA3S]. Breaches are not necessarily malicious. *See id.* (explaining that data breaches can be both purposeful and accidental). And they can occur several different ways. *See id.* (commenting that sometimes data hackers will trick users into sending them private data, while others force their way into sensitive databases). Breaches that do involve malintent are often called "hacks" and the bad actors called "hackers." *See* Jenny Knafo, *Data Breach vs. Data Hack*, DEVOLUTIONS (May 23, 2019), https://blog.devolutions.net/2019/05/data-breach-vs-data-hack [https://perma.cc/X9XW-XCQG] (differentiating a "breach" from a "hack" by the underlying objective).

[68] *How Data Breaches Happen*, *supra* note 67 (claiming that personal data may be leveraged to cause political, financial, and social injury). Unfortunately, people do not always realize that their information has been compromised for a significant amount of time. *See* Rob Sobers, *Data Breach*

make valuable transactions at the individual's expense.[69] But some use it for other purposes, like blackmail.[70] In just the last decade, breaches at popular US businesses have compromised billions of peoples' information.[71] Although a large number of breaches have occurred in corporate settings, personal data is always vulnerable and becomes a target regardless of where it gets stored.[72] Thus, privacy risks serve as an inherent caveat to unlimited data collection.[73]

Response Times: Trends and Tips, VARONIS, https://blogvaronis2.wpengine.com/data-breach-response-times/ [https://perma.cc/FN8Z-GE36] (June 17, 2020) (lamenting that companies take nearly seven months to recognize that a breach has happened).

[69] *See What Happens to Your Personal Information Once You've Been Hacked?*, SELFKEY (Nov. 21, 2019), https://selfkey.org/what-happens-to-your-personal-information-once-youve-been-hacked/ [https:/perma.cc/2U98-NCRF] (claiming that financial data is among the most lucrative types of data). Hackers can steal financial data to make purchases on the bank accounts of another individual. *Id.* They can also use medical data to obtain care on another's insurance. *Id.* Alternatively, a hacker could steal another's intellectual property to avoid incurring development or licensing fees. *Id.*

[70] *Id.* Some hackers will use personal data to force individuals into choices that they would otherwise not make. *See, e.g.*, *id.* (providing one example where a news reporter used stolen data about the CEO of Amazon.com, Inc., Jeff Bezos, and his adultery for blackmail).

[71] *See* Michael Hill & Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (July 16, 2021), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html [https://perma.cc/A2XG-MDNR] (highlighting some of the largest breaches in history, including Yahoo! Inc. (Yahoo) in 2013 and 2014, LinkedIn Corp. in 2012 and 2021, and Facebook in 2019). The breach at Yahoo in 2013 exemplifies how complicated they can be. *See id.* (explaining that the breach eventually resulted in a reduced acquisition price of the business years later). Yahoo failed to disclose the breach for three years, and even then, underreported the affected users by two billion. *See id.* (noting that the original claim to one billion affected persons in 2016 was increased to three billion by 2017). Despite the frequency and severity of large breaches, the US judicial system does not always provide an accessible remedy to the victims of a hack. *See generally* Nicolas N. LaBranche, Note, *The Economic Loss Doctrine & Data Breach Litigation: Applying the "Venerable Chestnut of Tort Law" in the Age of the Internet*, 62 B.C. L. REV. 1665, 1665–88 (2021) (proposing that many data breach victims are unable to seek redress in court because they cannot surpass "procedural hurdles").

[72] *See* Dmitry Dontov, *What Businesses Are the Most Vulnerable to Cyberattacks?*, FORBES (Jan. 19, 2021), https://www.forbes.com/sites/theyec/2021/01/19/what-businesses-are-the-most-vulnerable-to-cyberattacks/?sh=2a313e3d3534 [https://perma.cc/72SB-SXNQ] (explaining that businesses small and large alike may become targets to data breaches); *see, e.g.*, RISK BASED SEC., *supra* note 66 (commenting on an unexpected and seemingly random breach in 2021 at Ducks.org). Data breach analysts were surprised by the May 2021 breach of Ducks.org because the business was a nonprofit and solely works to protect duck species. *See* RISK BASED SEC., *supra* note 66 (acknowledging that large, popular, and profitable entities are the normal targets to a data attack). Although Ducks.org has a more obscure and smaller database, the breach revealed the private data of 474,000 people. *Id.*

[73] *See* DELOITTE, *Managing Data Risks for Value Creation*, *in* FUTURE OF RISK IN THE DIGITAL ERA 14, 14–15 (2019), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-rfa-future-of-risk-in-the-digital-era-report.pdf [https://perma.cc/M6G5-VLJB] (juxtaposing the monetary advantages to data trade with the danger it causes to suggest ways that a business may balance the two).

B. The EU Versus US Data Privacy Frameworks: A Conflict Between Omnibus and Sectoral Legislation

Despite having similar stances on privacy as a fundamental human right, the centralization of the EU's privacy legislation is structurally antithetical to the patchwork system developed in the US.[74] Subsection 1 of this Section details the broad personal data protections afforded by centralized privacy law in the EU.[75] In contrast, Subsection 2 describes the specific protections afforded by sectoral laws in the US and the subsequent incompatibility with EU privacy law demands.[76]

1. The EU Takes an "Omnibus" Approach to Privacy Legislation

For decades, the EU strived to expand upon very few data protection laws that could simultaneously encompass the wide range of privacy concerns.[77] To accomplish this goal, the EU developed "omnibus" laws.[78] This type of umbrella legislation purports to protect all European constituents from the wide range of personal data abuses that they may encounter.[79] The laws have continued to liberally define both the subjects and scope of their protection.[80]

---

[74] *See* Gabe Maldoff & Omer Tene, *"Essential Equivalence" and European Adequacy After* Schrems*: The Canadian Example*, 34 WIS. INT'L L.J. 211, 221 (2016) (contrasting the many components of US privacy law with the localized "omnibus" law in the EU). Like the EU, Canada opted to develop umbrella data privacy legislation. *Id.* at 218–20. This law, the Personal Information Protection and Electronic Documents Act (PIPEDA), broadened the protections of Canadians' personal information that the government and private entities collect. *Id.* at 218–19.

[75] *See infra* notes 77–95 and accompanying text.

[76] *See infra* notes 96–111 and accompanying text.

[77] *See* Ben Wolford, *What Is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ [https://perma.cc/8ZD9-HM63] (giving a history of the legislation and practices leading up to the EU's adoption of the GDPR); *Data Protection in the EU*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en [https://perma.cc/E2AU-Z97W] (overviewing the omnibus privacy structure that the EU developed through two pieces of legislation and a few oversight authorities).

[78] *See* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1973–74 (2013) (stating that the Data Protection Directive (DPD), which emphasized the need to maintain open channels for safe data trading, perpetuated the development of an omnibus regime in the EU). An "omnibus" law covers data coming from any type of commerce. Voss, *supra* note 29, at 421. Although omnibus privacy frameworks do not preclude the state from having additional sectoral regulations, those additions are subordinate law. *See* Schwartz, *supra*, at 1974 (claiming that a nation may include supplementary legislation that can provide additional regulations for individual areas that may require more protection).

[79] *See* Schwartz, *supra* note 78, at 1975 (noting that omnibus legislation protects data, irrespective of the collector or the type of information that the data holds).

[80] *See, e.g.*, Regulation (EU) 2016/679, *supra* note 10, art. 4(1), at 33 (defining "personal data" to include any information that could relate to or pinpoint an individual).

The broad privacy rights of European citizens have expanded and solidified over time.[81] Since 1950, the EU has sought to spearhead the global movement toward strong and all-encompassing legislation to protect the right to privacy.[82] In 1995, the EU passed its first directive aimed to safeguard its constituents from the threat that new advances in technology posed to privacy.[83] Two decades later, it enacted the General Data Protection Regulation (GDPR), what many consider to be the world's strongest and most ancillary privacy legislation.[84] This document has proven to be a formidable and fortifying culmination of many rights regarded as necessary to protect the personal data of Europeans.[85]

---

[81] *See* MILDEBRATH, *supra* note 12 (noting that the *Schrems II* Court of Justice of the European Union (CJEU) decision was a continuation of its trajectory towards stronger data privacy protections). The CJEU has played a significant role in securing and enhancing privacy rights for Europeans. *Id.* For example, in 2006, it voided an unrelated privacy agreement that regulated the transfer of travel-related data. *Id. See generally* Commission Decision 2004/535, of 14 May 2004 on the Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the United States' Bureau of Customs and Border Protection, 2004 O.J. (L 235) 11 (EC) (allowing for passenger data collected at the border to be transferred between the EU and US). The court also protested the enactment of an equivalent agreement with Canada in 2017. MILDEBRATH, *supra* note 12. *See generally* SHARA MONTELEONE, EUR. PARL. RSCH. SERV., PE 608.673, CJEU OPINION ON EU-CANADA PNR AGREEMENT (2017), https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/608673/EPRS_ATA(2017)608673_EN.pdf [https://perma.cc/J2ZT-XM9X] (providing an overview of the Canadian version of the Passenger Name Record Agreement that the CJEU likewise rejected).

[82] Wolford, *supra* note 77. *See generally Complete Guide to GDPR Compliance*, GDPR.EU, https://gdpr.eu [https://perma.cc/Z6KS-T5TV] (offering a wide range of resources to better understand the development and implementation of the GDPR).

[83] *See generally* Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (providing standards to safeguard the collection of personal data), *repealed by* Regulation (EU) 2016/679, *supra* note 10; Voss, *supra* note 29, at 420 (offering a brief introduction to Directive 95/46/EC).

[84] Wolford, *supra* note 77. The GDPR replaced the DPD. Regulation (EU) 2016/679, *supra* note 10, art. 94, at 86. The six major updates from the DPD to the GDPR were: (1) expanding the definition of "personal data" to encompass more of a comprehensive profile of information; (2) empowering individuals with control over their information; (3) regulating "processors" in addition to "controllers"; (4) demanding that data security be fundamental to businesses organization; (5) standardizing the disclosure of and punishment for violations; and (6) adding provisions for extraterritorial regulation by the EU. *See The Main Differences Between the DPD and the GDPR and How to Address Those Moving Forward*, SEEUNITY, https://britishlegalitforum.com/wp-content/uploads/2017/02/GDPR-Whitepaper-British-Legal-Technology-Forum-2017-Sponsor.pdf [https://perma.cc/9ZMN-D4AV] (comparing the 1995 DPD with the 2016 GDPR).

[85] *See* Wolford, *supra* note 77 (recognizing the extreme toughness of the GDPR and its requirements). The monetary penalties associated with the GDPR's enforcement have been massive. *See* Ben Swagerman, *The Biggest GDPR Fines to Date*, LEXOLOGY (June 15, 2020), https://www.lexology.com/library/detail.aspx?g=ac77a2a3-b19c-4c7d-8031-4021e5fc90f4 [https://perma.cc/4KLD-7SYD] (giving examples of GDPR-related fines). Google L.L.C. accrued a $57 million fine from France based on one violation alone. *Id.* Amazon.com, Inc. was recently hit with the largest GDPR penalty of all time, totaling in at a massive $888 million. Stephanie Bodoni, *Amazon Gets Record $888 Million EU Fine Over Data Violations*, Bloomberg (July 30, 2021), https://www.bloomberg.com/news/

One data privacy privilege that the EU gave to its residents and citizens, called "extraterritoriality," allows them to bootstrap their rights to wherever they or their data go in the world.[86] Thus, privacy legislation enacted in the EU can nonetheless have legal implications for organizations seeming to act exclusively outside of the EU.[87] Although data trade limitations may negatively impact its economy, the EU chose to actively prioritize the safekeeping of personal data by restricting the flow of identifiable information to parties which can safeguard it competently.[88]

The EU has required, by law, that all foreign recipients of European data must be "adequate[ly]" prepared to receive and protect it.[89] An entity may be "adequate" if either (1) its home country receives nationwide approval or (2) it receives approval of its own privacy measures.[90] The EU determines a country's aptitude to protect personal data at the European Commission (the Commission) by scrutinizing the ability of the local regulations to protect fundamental privacy rights.[91] Foreign countries have the burden to show the Com-

---

articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach [https://perma.cc/5HDS-ZMUS].

[86] *See* Regulation (EU) 2016/679, *supra* note 10, art. 3(1), at 32 ("This Regulation applies . . . whether the processing takes place in the Union or not.").

[87] *See id.* (providing for the law's extraterritorial scope). For example, a company that believes itself to be fully situated in the US, and only intends to process the data of US citizens, might unknowingly become subject to the provisions of the GDPR. *See id.* (showing that a European could migrate into the US with his or her data privacy rights, possibly making this hypothetical corporation, despite its intentions, a processor of that European's data).

[88] *See* Charter of Fundamental Rights of the European Union, arts. 7, 8, 47, 2012 O.J. (C 326) 391, 397, 405 (providing redress for any violations to an individual's right to private life and information); Directive 95/46/EC, *supra* note 83, art. 1, at 22–24 (emphasizing that the EU would take active steps to guarantee the personal liberties and privacy rights of individuals). The Charter of Fundamental Rights of the EU provides Europeans with rights to: (1) self-respect; (2) personal liberties; (3) fairness; (4) safe social and professional conditions; (5) individual rights; and (6) legal protection. *See generally* Charter of Fundamental Rights of the European Union, *supra* (providing Europeans with a plethora of rights in all walks of life).

[89] Directive 95/46/EC, *supra* note 83, arts. 25–26, at 45–46.

[90] *See* Regulation (EU) 2016/679, *supra* note 10, recital 108, at 20 (explaining that without a national approval, businesses must take additional steps to ensure the legality of their data-related business with the EU). Although individual approval is possible through mechanisms like SCCs and BCRs, it is far more complicated than a nationwide transatlantic agreement would be. *See* Claude-Étienne Armingaud et al., *EU Data Protection: Standard Contractual Clauses May Have Been Confirmed by the CJEU, but at What Price?*, K&L GATES (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 [https://perma.cc/8X8Z-PSAX] (noting that SCCs may be difficult to apply because they depend on the state's additional safeguards to be valid); Natalie Whitney, *GDPR: Standard Contractual Clauses vs Binding Corporate Rules*, GRCI L., https://www.grcilaw.com/blog/international-data-transfers-model-contract-clauses-vs-binding-corporate-rules [https://perma.cc/8V3Y-R7NP] (Apr. 8, 2021) (explaining that BCRs are less applicable than other mechanisms because they are only relevant for larger entities).

[91] Charter of Fundamental Rights of the European Union, *supra* note 88, art. 8(1), at 397; Directive 95/46/EC, *supra* note 83, arts. 25–26, at 45–46. The European Commission (the Commission)

mission their own suitability to receive data from the EU.[92] The Commission may decide based on its consideration of the requesting country's ability to protect the personal information of European citizens.[93] When the Commission finds that a country has sufficient data security in place, it publishes its approval through an "adequacy decision."[94] If a country does not have such a decision, individual entities may only transfer data if they implement their own protection measures to comply with EU standards.[95]

2. Meanwhile, the US Takes a "Sectoral" Approach to Privacy Legislation

Unlike the EU, the US privacy framework consists of a hodgepodge of state and federal laws that regulate individual categories of privacy protection.[96] Due to this divided structure, the US has "sectoral" privacy legislation.[97] This approach allows the US to develop highly-tailored laws that focus specifically on the privacy concerns that come from a specific sector of business.[98] Each piece of legislation has the flexibility to define whom it will regu-

---

is an administrative directorate with the authority to decide whether a country has "adequate . . . data protection" to receive data from the EU. *Adequacy Decisions*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/3EDL-KMXH]. Although Directive 95/46/EC does not expressly define "adequate," the CJEU ruled that its language demands that the country: (1) have regulations that will guarantee the data is sufficiently safeguarded; and (2) have those safeguards be evaluated to make certain they "protect[] . . . the private lives and basic freedoms and rights" of Europeans. Case C–362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650, ¶¶ 70–72 (Oct. 6, 2015) (quoting Directive 95/46/EC, *supra* note 83, art. 25(6), at 46) (confirming that adequacy may be evaluated with consideration to many factors and invoking the requirements of Article 8(1)).

[92] Directive 95/46/EC, *supra* note 83, recital 57, at 37, art. 25(6), at 46. Non-member countries must provide legally binding evidence to show the EU, via the Commission, that it deserves to continue their international trade. *Id.* art. 25(6), at 46.

[93] *See id.* recital 56, at 36 ("[T]he adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer . . . .").

[94] *Id.* art. 25(6), at 46; *see* WEISS & ARCHICK, *supra* note 6, at 12 (discussing the necessity for the CJEU to approve of data-transfer mechanisms).

[95] *See* Regulation (EU) 2016/679, *supra* note 10, recital 108, at 20 (recognizing that an individual business can use SCCs and/or BCRs to exchange data with the EU if their nation does not have the required privacy standards).

[96] *See* Maldoff & Tene, *supra* note 74, at 221 (describing the culmination of all US privacy laws to be like an ill-constructed "quilt," rather than a singular cohesive piece of legislation). Some of the sectors that US privacy law regulates concern information relating to health, finances, education, and electronic communication. *Id.*

[97] Voss, *supra* note 29, at 418.

[98] STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 7–39 (2019) (demonstrating the ability of a sectoral approach to have very specific laws that can explicitly regulate the exact abuses it wishes to protect Americans from); *see* Schwartz, *supra* note 78, at 1974 (providing Professor David Flaherty's claim that sectoral laws react to distinct issues with strong and customized protection). There is no individual agency tasked with overseeing the enforcement of federal privacy regulations. Maldoff & Tene, *supra* note 74, at 222. Instead, different agencies are responsible for overseeing different sectoral laws. *See id.* (listing multiple federal agencies that collectively substitute for having a localized "regulator"). For example,

late and what data it will embrace.[99] New data privacy laws in a given sector can, and often do, define their protections differently from those dealing in another sector.[100] Collectively, these laws regulate personal data use by all public and private entities that are within the realm of a specific law.[101] Certain data or businesses, however, may potentially go unregulated if no sectoral law covers them.[102]

In addition, individual states have also developed vastly differing and conflicting standards of protection.[103] These laws are supplementary to federal data privacy regulations.[104] Therefore, states may differ on the breadth of the

---

the Federal Trade Commission (FTC) is tasked with the enforcement of the CAN-SPAM Act, a privacy law that regulates certain electronic communications. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 §§ 6–7, 15 U.S.C. §§ 7704–7705. On the other hand, the Office for Civil Rights (OCR) acts as the regulator for HIPAA, which sets standards for medical data. Off. of Civ. Rts. (OCR), *Enforcement Highlights*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html [https://perma.cc/JNS8-9GAL] (Aug. 11, 2021). *See generally* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191 110 Stat. 1936 (detailing the provisions of the Act).

[99] MULLIGAN & LINEBAUGH, *supra* note 98, at 7–8.

[100] *See* Voss, *supra* note 29, at 410 (describing the lack of continuity between data privacy legislation within the US).

[101] Maldoff & Tene, *supra* note 74, at 221. The Privacy Act of 1974 regulates the standards that all federal agencies must meet in their interaction with personal data. 5 U.S.C. § 552a. This legislation purported to "balance" federal agencies' demand for personal data with an individual's fundamental right not to have their privacy unnecessarily violated. *Overview of the Privacy Act of 1974*, U.S. DEP'T OF JUST., https://www.justice.gov/opcl/policy-objectives [https://perma.cc/GKC6-TMMB] (Feb. 24, 2021). Congress enacted the law in response to the infamous "Watergate scandal," whereby a federal agency used wiretapping technology to illicitly spy on the political opponents of sitting President Richard Nixon. *Id.*; *see Watergate Scandal*, HIST., https://www.history.com/topics/1970s/watergate [https://perma.cc/6HPG-TR54] (June 16, 2021) (chronicling the actions taken by the Committee to Re-Elect the President in the office of the Democratic National Committee on June 17, 1972). Suspicion surrounding President Nixon's personal involvement led to his eventual resignation. *See Watergate Scandal*, *supra* (detailing the President's departure from office in 1974).

[102] *See* Maldoff & Tene, *supra* note 74, at 221 (noting the gap in US privacy law that may exist for an organization that is not specifically regulated). Unlike in omnibus legislation, there is no catch-all engrained into the US data privacy structure. *Id.*; *see* Voss, *supra* note 29, at 421 (defining an "omnibus" law by its broad reach). Although it has continued to carve out distinct areas of concern, there is an inherent possibility for abuse of personal data to slip through the cracks. *See* Maldoff & Tene, *supra* note 74, at 221 (explaining that an organization may "fall outside of" federal protection).

[103] Voss, *supra* note 29, at 410.

[104] *See* Maldoff & Tene, *supra* note 74, at 221 (discussing the US's multi-level sector-based web of privacy legislation); Lesley Daunt, *State vs. Federal Law: Who Really Holds the Trump Card?*, HUFFPOST, https://www.huffpost.com/entry/state-vs-federal-law-who-_b_4676579 [https://perma.cc/3XMD-V4AW] (Mar. 30, 2014) (noting that state regulations can add to but not contradict federal legislation). As provided by its Constitution, the US has a two-tiered government, with legislative powers at both the federal and state levels. CONG. RSCH. SERV., RL30315, FEDERALISM, STATE SOVEREIGNTY, AND THE CONSTITUTION: BASIS AND LIMITS OF CONGRESSIONAL POWER 1 (2013). The interrelation between these tiers is called "federalism." *Id.* States have certain power, called "sovereignty," to regulate themselves individually. *Id.* But there are restrictions to that power as well. *See id.* (commenting that states do not have certain self-regulatory powers, including the power to wage war).

additional protections that they afford to their constituents.[105] Similar to the approach of federal data privacy, some states have introduced more category-specific laws.[106] Conversely, other states have recently opted to develop more generalized pseudo-omnibus legislation.[107] Although states have the autonomy to expand their privacy protections, the laws of one state have the ability to affect an entity conducting business in another state because technology and data permeate state borders.[108]

Because the US takes a sectoral approach and has varying standards, the EU has never deemed the US "adequate" to receive personal data from the EU.[109] Instead, the Department of Commerce has twice negotiated a mechanism to allow certified and compliant American entities to trade data between the EU and US lawfully.[110] The agreements borne from those negotiations pur-

---

Many of the powers not held by state governments are held by the federal government instead. *See, e.g.*, *id.* at 2 (noting that the power to "coin money" is that of the federal government alone). State governments must also defer to and obey any laws promulgated by the federal tier. U.S. CONST. art. VI, cl. 2 ("This Constitution, and the Laws of the United States . . . shall be the supreme Law of the Land . . . .").

[105] *See 2020 Consumer Data Privacy Legislation*, NAT'L CONF. OF STATE LEGISLATURES, https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx [https://perma.cc/SZ83-TSSN] (Jan. 17, 2021) (providing updates on various types of privacy legislation that each state added or failed to add to their state laws in 2020).

[106] *See, e.g.*, Biometric Information Privacy Act (BIPA) of 2018, 740 ILL. COMP. STAT. 14/15 (2020) (protecting Illinois residents from the collection and use of data derived from their bodily measurements). Illinois provides additional regulation for data relating to a "biometric identifier." *Id.* This information can include a broad range of details, such as fingerprints, voice data, or facial structure. *Id.* at 14/10.

[107] *See, e.g.*, California Consumer Privacy Act (CCPA) of 2018, CAL. CIV. CODE §§ 1798.100–.194 (Supp. 2021) (providing Californians with a wide range of protections to safeguard their personal data). *See generally* Carol A. F. Umhoefer, *CCPA vs. GDPR: The Same, Only Different*, DLA PIPER (Apr. 11, 2019), https://www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1-2019/ccpa-vs-gdpr/ [https://perma.cc/C64Q-YFFG] (reflecting on the common comparison between the Californian law and EU omnibus law). The CCPA gives Californians a broad set of controls over their personal data. *See* CIV. §§ 1798.100–.120. Its provisions include many data rights, such as the "right to know," "right to delete," "right to opt out," and right to non-discrimination. *Id.* §§ 1798.105, .115, .120, .125. Although this is not necessarily true omnibus legislation, it does share many similarities to laws like the GDPR, and it is not necessarily sector specific. *See generally id.* § 1798.100–.120 (having similar provisions to the EU GDPR's rights to know, restrict, and prevent further data collection); Regulation (EU) 2016/679, *supra* note 10 (providing the EU's omnibus law).

[108] *See* CIV. § 1798.145(a)(6) (providing the possibility for the CCPA to have extraterritorial reach into the jurisdiction of other US states). Only a business that has no commercial relation or business in California or with Californians is absolutely excluded from the CCPA. *Id.*

[109] *See* Maldoff & Tene, *supra* note 74, at 223 (suggesting that the US has never even attempted to satisfy "adequacy" pursuant to its national privacy structure because it does not have an "omnibus" law).

[110] Anupam Chander, *Is Data Localization a Solution for* Schrems II?, 23 J. INT'L ECON. L. 771, 772–73 (2020); *see Privacy Shield Overview*, PRIV. SHIELD FRAMEWORK, https://www.privacyshield.gov/Program-Overview [https://perma.cc/5KBA-9XHU] (explaining the role of the Department of Commerce in finding a middle ground for data transfers to continue). The ability to make a legal

ported to balance the demand for legal transatlantic data transfers with the obligation to protect the more-stringent privacy rights of EU citizens.[111]

C. Schrems I *Invalidated the Data Transfer Mechanism Formerly Known as Safe Harbor*

The first personal data transfer mechanism that the EU and US negotiated was called "Safe Harbor."[112] It became effective in 2000 upon receiving its adequacy assessment from the Commission.[113] Under this agreement, the EU presumed that all entities participating in the Safe Harbor Program had "adequate" protections for lawful receipt and use of EU data.[114] In turn, participants in Safe Harbor were bound to uphold privacy standards that guaranteed that the rights of EU constituents be met.[115] Organizations could apply and join the program by "self-certify[ing]" their commitment to follow the requirements of Safe Harbor.[116] Specifically, the Safe Harbor agreement required member organizations to observe seven 'best practices' to protect personal data.[117]

---

transfer of data between the EU and US can be important to organizations in both places. *See Privacy Shield Overview*, *supra* (noting that these agreements affect compliance "on both sides"). Although a US company may suffer from its inability to make use of valuable EU data, European entities are likewise unable to sell it, and therefore, cannot profit from such a sale. *See* Dan Cooper et al., *Life After* Schrems II*: Practical Recommendations in an Uncertain Time*, COVINGTON (Sept. 4, 2020), https://www.insideprivacy.com/cross-border-transfers/life-after-schrems-ii-practical-recommendations-in-an-uncertain-time/ [https://perma.cc/U2L4-CF45] (recognizing the reciprocal economic impact faced by European companies trying to make the international trade); Liem et al., *supra* note 14 (explaining the importance of data trade in the global economy).

[111] *See* MILDEBRATH, *supra* note 12 (commenting on the compromise made to develop Privacy Shield); *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, https://2016.export.gov/safeharbor/eu/eg_main_018476.asp [https://perma.cc/P7K7-SB3F] (Dec. 18, 2013) (reflecting a similar process to develop Safe Harbor).

[112] *U.S.-EU Safe Harbor Overview*, *supra* note 111.

[113] 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 Issued by the US Department of Commerce, art. 1, 2000 O.J. (L 215) 7, 8 (EC). The US Department of Commerce arranged the Safe Harbor agreement during the Clinton Administration. Chander, *supra* note 110, at 773.

[114] *U.S.-EU Safe Harbor Overview*, *supra* note 111.

[115] *Id.*

[116] *Id.* The Safe Harbor Program required a participating organization to renew its self-assessment each year. *Id.*

[117] *See Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000*, EXPORT.GOV, https://2016.export.gov/safeharbor/eu/eg_main_018475.asp [https://perma.cc/3RP7-VL4Q] (Jan. 30, 2009) (presenting the use of several data protection principles to overcome EU requirements). The US Department of Commerce published these principles to ease some confusion that its constituents might have regarding what the Safe Harbor agreement actually required of them. *See id.* (providing context to the document). (1) Data collectors were obligated to tell individuals why the business collected the personal data. *See id.* (explaining the Safe Harbor Principle: "Notice"). (2) They were also required to allow individuals to decide whether their collected personal data could later be transferred or used for other reasons. *See id.* (explaining the Safe Harbor Principle: "Choice"). (3) Likewise, they had to provide the preceding opportunities to individuals again if the business ever

Over a decade after the agreement went into effect, Maximillian Schrems brought a complaint that would decimate Safe Harbor.[118] Schrems claimed that US privacy practices allowed for private data collectors to share his information to national security operations.[119] He argued that the initial transfer potentially endangered his privacy, rather than protecting it as legally required.[120] In October 2015, in *Schrems v. Data Protection Commissioner* (*Schrems I*), the CJEU agreed, holding that the Safe Harbor adequacy decision was "invalid" because it did not meet the EU's standard for "adequate" protection.[121]

In voiding Safe Harbor, the CJEU focused on the inherent conflict between the agreement and the privacy protections afforded by EU law.[122] Name-

---

transferred their data to another entity. *See id.* (explaining the Safe Harbor Principle: "Onward Transfer"). (4) Data collectors were responsible for properly securing the personal data they collected. *See id.* (explaining the Safe Harbor Principle: "Security"). (5) Additionally, they are limited to the use of data that was correct and used exclusively for pertinent objectives. *See id.* (explaining the Safe Harbor Principle: "Data Integrity"). (6) Individuals could "access" their collected personal data and rectify or erase it. *See id.* (explaining the Safe Harbor Principle: "Access"). (7) Lastly, there had to be a system to ensure the compliance of participating entities. *See id.* (explaining the Safe Harbor Principle: "Enforcement").

[118] *See* Case C–362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650, ¶ 28 (Oct. 6, 2015) (providing background to the case brought by Schrems in 2013); Commission Decision 2000/520, *supra* note 113, art. 1, at 8 (deeming the Safe Harbor mechanism to be "adequate"). Schrems took issue with a local Facebook subsidiary transferring the data it collected to its US corporate parent, Facebook Inc. *Schrems I,* ECLI:EU:C:2015:650, ¶ 28. He, thus, filed a complaint with the Data Protection Commissioner of Ireland (commissioner). *Id.* The commissioner denied Schrems' request, and was ultimately sued by Schrems for doing so. *Id.* ¶¶ 29–30. Although Schrems did not directly question the Safe Harbor adequacy determination, the High Court of Ireland concluded that its legal assessment was necessary to resolve the suit. *Id.* ¶ 35.

[119] *Schrems I*, ECLI:EU:C:2015:650, ¶ 28. The scrutiny of US privacy protection on a global stage began in 2013 when a Central Intelligence Agency employee, Edward Snowden, divulged the US National Security Agency (NSA)'s practices to reporters. *See* Dave Davies, *Edward Snowden Speaks Out: 'I Haven't and I Won't' Cooperate with Russia*, NPR (Sept. 19, 2019), https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia [https://perma.cc/3DPD-8W22] (recounting Snowden going to Hong Kong to reveal highly confidential NSA documents to three reporters); Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 11, 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [https://perma.cc/6F5Y-RCF7] (disclosing that Snowden was the "whistleblower" behind the unprecedented NSA scandal).

[120] *See Schrems I*, ECLI:EU:C:2015:650, ¶ 67 (addressing his suspicion that the US could not afford Europeans the "adequate . . . protection" required by law). Specifically, Schrems contended that the US lacked the legal foundation to guarantee rights afforded to him by Directive 95/46/EC. *See id.* In 1995, the European Parliament developed Directive 95/46/EC to better protect European data as it travelled between European countries. *EU Data Protection Directive*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/intl/eu_data_protection_directive.html [https://perma.cc/LE8G-C3LL].

[121] *See Schrems I*, ECLI:EU:C:2015:650, ¶ 106 (concluding that the Safe Harbor adequacy determination was not proper); *id.* ¶ 67 (implicating that the "validity" of Safe Harbor depended on its ability to properly protect European data). Specifically, the CJEU focused its attention on Articles 1 and 3 of the Safe Harbor adequacy determination. *Id.* ¶¶ 79, 99.

[122] *See id.* ¶¶ 3–9 (introducing the CJEU's decision to invalidate Safe Harbor with the provisions of Directive 95/46/EC and Commission Decision 2000/520). The CJEU referenced parts of the legis-

ly, the court took issue with the fact that a US corporation could ignore Safe Harbor requirements when transferring data to a potentially non-compliant public authority.[123] The US security authorities' overreach allowed their improper access to European data and contradicted the purpose of the Safe Harbor agreement.[124] More concerningly, EU citizens had no meaningful legal recourse.[125] Furthermore, the Safe Harbor adequacy decision itself failed to assert that US regulations or agreements would sufficiently protect the integrity of EU personal data.[126] Although the EU did not necessarily require foreign

---

lation to show the protective and broad nature of Directive 95/46/EC and Commission Decision 2000/520. *See, e.g.*, *id.* ¶¶ 3–4 ("[D]ata-processing systems are designed to serve man." (quoting Directive 95/46/EC, *supra* note 83, recital 2, at 31)); *id.* ¶ 4 ("Member States shall protect the fundamental rights and freedoms of natural persons . . . with respect to the processing of personal data." (quoting Directive 95/46/EC, *supra* note 83, art. 1, at 38)).

[123] *See id.* ¶¶ 82, 86 (outlining the possibility for a US business that participated in Safe Harbor to nevertheless transfer data that it collected from the EU to a non-compliant public entity). US "national security, public interest," and "law enforcement" took precedence to any requirement of Safe Harbor. *Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000*, *supra* note 117; *see Schrems I*, ECLI:EU:C:2015:650, ¶ 86 (emphasizing this caveat in its invalidation of the agreement). Additionally, "public authorities" that obtained the information would be under no obligation to comply with the agreement. *Schrems I*, ECLI:EU:C:2015:650, ¶¶ 82, 93. An organization could, thus, plausibly be obligated to make a transfer that was in direct violation of the Safe Harbor principles to an entity that was likewise not bound to meet EU standards. *See id.* at ¶¶ 82–86 (identifying US legislation to be at odds with actual "adequacy").

[124] *See Schrems I*, ECLI:EU:C:2015:650, ¶ 90 (claiming that national organizations in the US overindulged in their use of personal data); *U.S.-EU Safe Harbor Overview*, *supra* note 111 (explaining that Safe Harbor purported to balance personal privacy needs with economic ones). In 2013, the Commission assessed US security authorities to determine how they made use of their access to personal data. Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows, COM (2013) 846 final (Nov. 11, 2013); Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM (2013) 847 final (Nov. 11, 2013). It concluded that these organizations used data more than was "necessary and proportionate" to address actual security needs. *Schrems I*, ECLI:EU:C:2015:650, ¶ 22. The Commission further found that Europeans had no way to properly address potential abuses of their privacy rights. *Id.* ¶ 23.

[125] *See Schrems I*, ECLI:EU:C:2015:650, ¶¶ 89–90, 95 (expressing concern that neither the US government nor legal system would effectively address EU privacy complaints). The CJEU lamented that the FTC's oversight of mercantile litigation was inapplicable to individuals. *Id.* ¶ 89. Additionally, there was no way for Europeans to challenge potential abuses in court. *Id.* ¶ 90. The court concluded that the lack of redressability was inconsistent with EU legislation. *See id.* ¶ 95 ("[L]egislation not providing for any possibility . . . to pursue legal remedies . . . does not respect the essence of the fundamental right to effective judicial protection . . . .").

[126] *Id.* ¶¶ 96–97. The Safe Harbor adequacy determination lacked any explicit statement that the US "ensure[d]" that its regulations would properly protect personal data. *See* Commission Decision 2000/520, *supra* note 113, recitals 2, 5, at 7 (omitting such a provision). The CJEU claimed that this alone would have been sufficient to invalidate the agreement. *Schrems I*, ECLI:EU:C:2015:650, ¶ 98. The court, nevertheless, continued to assess the contents of the agreement to provide a more-detailed invalidation. *See generally id.* ¶¶ 99–106 (continuing to evaluate Article 3 of Commission Decision 2000/520).

countries to match its exact privacy standards, it demanded that they have "essentially equivalent" protections to those in the EU.[127]

Following this decision, US entities could no longer lawfully obtain data from the EU by participating in the Safe Harbor program.[128] The EU and US therefore worked to quickly renegotiate a new mechanism to provide another adequacy classification.[129] The heir to Safe Harbor began its reign in August of the following year.[130]

D. Déjà Vu All Over Again: Schrems II *Ends Privacy Shield and Diminishes the Strength of SCCs*

Privacy Shield, the successor mechanism to Safe Harbor, was operational several months after *Schrems I* in 2016.[131] The EU and US drafted this agreement on similar core principles of data protection to those of Safe Harbor.[132]

---

[127] *Schrems I*, ECLI:EU:C:2015:650, ¶ 73. The court conceded that, because the law required a foreign country's standards to be "adequate," it could not then demand them to be "identical" to the EU. *Id. Compare Adequate*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/adequate [https://perma.cc/5NER-9E35] (providing the term's degree of comparability to be "enough or satisfactory for a particular purpose"), *with Identical*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/identical [https://perma.cc/4W8Z-ZVH7] (showing the heightened requirement to be "exactly the same"). Essential equivalence requires: (1) clarity and accessibility; (2) minimization; (3) completely autonomous supervision; and (4) a means to rectify potential abuses in court. *See Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment*, CNIL (Feb. 5, 2016), https://www.cnil.fr/en/statement-article-29-working-party-consequences-schrems-judgment [https://perma.cc/URF9-8GDB] (assessing the *Schrems I* decision to hypothesize the requirements for a valid agreement after the decision).

[128] *Schrems I*, ECLI:EU:C:2015:650, ¶106; *see U.S.-EU Safe Harbor Overview*, *supra* note 111 (detailing the mechanism which, prior to *Schrems I*, allowed for data transfers between the EU and US). *See generally* Courtney M. Bowman, *US-EU Safe Harbor Invalidated: What Now?*, PROSKAUER (Oct. 6, 2015), https://privacylaw.proskauer.com/2015/10/articles/european-union/us-eu-safe-harbor-invalidated-what-now/ [https://perma.cc/Y9BC-C28L] (discussing the impact that *Schrems I* had on the EU when it ceased the availability of the only national data-transfer mechanism, Safe Harbor).

[129] *See* Chander, *supra* note 110, at 773 (stating that the EU and US developed Privacy Shield one year after *Schrems I* invalidated Safe Harbor).

[130] *See Privacy Shield Overview*, *supra* note 110 (referencing the Privacy Shield's adequacy determination on July 12, 2016); *see* Commission Implementing Decision (EU) 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, art. 1, 2016 O.J. (L 207) 1, 35 (EC) (finding Privacy Shield to be "adequate"); MILDEBRATH, *supra* note 12 (labeling Privacy Shield as a "replacement" to Safe Harbor).

[131] *Privacy Shield Overview*, *supra* note 110. Much like Safe Harbor, the Commission cleared Privacy Shield during its required adequacy determination. *See* Commission Implementing Decision 2016/1250, *supra* note 130, art. 1, at 35 (giving the Commission's accepting opinion of the updated framework). Privacy Shield was negotiated during the Obama Administration. Chander, *supra* note 110, at 773.

[132] *EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce*, *supra* note 5 (explaining the core Privacy Shield Principles: (1) "Notice," (2) "Choice," (3) "Accountability for Onward Transfer," (4) "Security," (5) "Data Integrity and Purpose Limitation," (6) "Access," and (7) "Recourse, Enforcement and Liability"); *see U.S.-EU Safe Harbor Overview*, *supra*

With Privacy Shield, the Department of Commerce restated the guiding standards while further emphasizing the legal responsibility of US data collectors to protect Europeans' personal information and minimize the data that they collect.[133] Additionally, in response to redressability concerns brought forth in the *Schrems I* decision, the Privacy Shield mechanism established an "[o]mbudsperson," responsible for arbitrating the US-based privacy concerns of those protected under EU law.[134] Despite some public disapproval, the Commission deemed Privacy Shield to be "adequate."[135] But Schrems remained unsatisfied with the new agreement and continued to bring legal challenges regarding the validity of data transfers between the EU and US.[136]

---

note 111 (overviewing the Safe Harbor agreement and its principles); *supra* note 117 and accompanying text (explaining the seven Safe Harbor principles).

[133] *See EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce*, *supra* note 5 (emphasizing the importance of compliance by participants to uphold the values of the Privacy Shield principles). For example, the FTC could pursue and enforce Privacy Shield against any organization that failed to adhere to its terms. *Id.* Section 5(a) of the FTC Act generally provides regulation to "unfair or deceptive acts" that may occur in the trade of business. *See* Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a)(1) (providing the legal standard for unfair practice). In addition to the main seven principles, Privacy Shield included sixteen additional requirements for its members. *See EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce*, *supra* note 5 (giving additional explanations for: (1) "Sensitive Data"; (2) "Journalistic Exceptions"; (3) "Secondary Liability"; (4) "Performing Due Diligence and Conducting Audits"; (5) "The Role of the Data Protection Authorities"; (6) "Self-Certification"; (7) "Verification"; (8) "Access"; (9) "Human Resources Data"; (10) Obligatory Contracts for Onward Transfers; (11) "Dispute Resolution and Enforcement"; (12) "Choice—Timing of Opt Out"; (13) "Travel Information"; (14) "Pharmaceutical and Medical Products"; (15) "Public Record and Publicly Available Information"; and (16) "Access Requests by Public Authorities").

[134] *See* Case C–311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶¶43, 45 (July 16, 2020) (explaining the implementation of the "Ombudsperson" in Privacy Shield); Commission Implementing Decision (EU) 2016/1250, *supra* note 130, annex A, at 72 (approving this addition as being sufficient to meet EU standards); Mark Young & Sam Jungyun Choi, *Privacy Shield Ombudsperson Confirmed by the Senate*, COVINGTON (June 25, 2019), https://www.insideprivacy.com/cross-border-transfers/privacy-shield-ombudsperson-confirmed-by-the-senate/ [https://perma.cc/YDC5-SBR7] (discussing the role that the first ombudsperson, Keith Krach, would play in enforcing Privacy Shield). The ombudsperson was designed to act as an entity that was separate from US national intelligence and surveillance. *Schrems II*, ECLI:EU:C:2020:559, ¶43. The role was to oversee any complaint that may be brought by a European concerning US data practices. *Privacy Shield Ombudsperson*, U.S. DEP'T OF COM., https://www.state.gov/privacy-shield-ombudsperson/ [https://perma.cc/4X5C-GRZ3]. EU constituents did not need to show that any person or entity had "accessed" or abused their personal data to file complaints. Maldoff & Tene, *supra* note 74, at 238.

[135] Commission Implementing (EU) Decision 2016/1250, *supra* note 130, art. 1, at 35.

[136] *See* MILDEBRATH, *supra* note 12 (describing the sequence of events that led to the *Schrems II* complaint). Notably, the original complaint for *Schrems II* was made prior to the enactment of Privacy Shield. *Id.* Initially, Schrems brought a challenge to the Irish Data Protection Authority based solely on Facebook Ireland's continued use of SCCs to transfer data to the US after *Schrems I*. *Id.* The Commission deemed SCCs "adequate" in 2010. Commission Decision 2010/87, of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC of the European Parliament and of the Council, art. 1, 2010 O.J. (L 39) 5, 8 (EU). By the time *Schrems II* reached the CJEU, Privacy Shield had received its own adequacy determination and was in full force. *See* MILDEBRATH, *supra* note 12 (noting the coinciding

In July 2020, in *Data Protection Commissioner v. Facebook Ireland Ltd.* (*Schrems II*), the CJEU invalidated Privacy Shield as a mechanism for transatlantic personal data transfers.[137] Similar to its *Schrems I* decision, the court focused on the US's failure to safeguard personal data in a manner that was "essentially equivalent" to the standard required by the EU.[138] It found that Privacy Shield was still insufficient for EU privacy requirements.[139] In part, the court reasoned that US surveillance laws fell short of the EU standard that the collection and use of personal data be both "necessary" and "proportional[]" to its objective.[140] This determination hinged on the lack of restrictions placed on national surveillance groups and their ability to meddle with personal data existing in the US.[141] The court further found the addition of an ombud-

---

rise and demise of Privacy Shield). Thus, the CJEU used this opportunity to assess both data-transfer mechanisms in one decision. *Id.*; *see Schrems II*, ECLI:EU:C:2020:559, ¶ 66 (addressing the choice to decide the validity of the adequacy determinations for both SCCs and Privacy Shield).

[137] *Schrems II*, ECLI:EU:C:2020:559, ¶ 201. Although Schrems and Facebook Ireland Ltd. were the primary parties to this decision, the US, the Electronic Privacy Information Centre, the BSA Business Software Alliance Inc., and Digitaleurope all acted as intervening parties during the proceeding. *See generally id.* (listing all relevant parties). In September 2020, the sister decision to *Schrems II* saw a similar outcome regarding the functional equivalent to Privacy Shield that existed between the US and Switzerland. FED. DATA PROT. & INFO. COMM'R, POLICY PAPER ON THE TRANSFER OF PERSONAL DATA TO THE USA AND OTHER COUNTRIES LACKING AN ADEQUATE LEVEL OF DATA PROTECTION WITHIN THE MEANING OF ART. 6 PARA. 1 SWISS FEDERAL ACT ON DATA PROTECTION 5–7 (Sept. 8, 2020), https://www.newsd.admin.ch/newsd/message/attachments/64261.pdf [https://perma.cc/BVT5-UNXX].

[138] *See Schrems II*, ECLI:EU:C:2020:559, ¶ 105 (referencing the requirement in EU privacy legislation that a country's standards must be "essentially equivalent" to the EU's to be sufficient).

[139] *Id.* ¶ 201. Unlike in *Schrems I*, the court in *Schrems II* relied on the GDPR to set benchmarks for EU standards. *Compare id.* ¶ 202 (expressly citing the provisions of Article 46 of the GDPR), *with* Case C–362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650 (Oct. 6, 2015) (containing no reference to the GDPR). Although the GDPR was far into its development at the time of the *Schrems I* decision, it was not fully implemented until three years later. Wolford, *supra* note 77. It was, thus, only applicable law for the *Schrems II* decision. *See generally Schrems II*, ECLI:EU:C:2020:559 (occurring in 2020, four years after the EU adopted the GDPR).

[140] *See Schrems II*, ECLI:EU:C:2020:559, ¶ 176 (describing the requirements of EU law). First, the use of personal data must be restricted to the minimum that is needed for some goal. *Necessity & Proportionality*, EURO. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en [https://perma.cc/7R2Y-U7QR]. Second, there must be an equilibrium between the extent to which data is collected and used and the reason that it was necessary. *Id.* In precise terms, data collection is only "proportional[]" if the "disadvantages" to the individual do not surpass the "advantages" to the authority. *Id.*

[141] *See Schrems II*, ECLI:EU:C:2020:559, ¶ 65 (commenting that US surveillance practices were especially concerning to the EU because Europeans were not privy to the constitutional protections an American citizen held to prevent or remedy privacy harms). In part, the CJEU looked to the broad abilities granted to the NSA in Executive Order 12,3333 (E.O. 12,333). *Id.* President Ronald Regan introduced E.O. 12,3333 in 1981 to provide US surveillance programs extensive abilities to act, collect, and use security intelligence in ways that would elsewise be unlawful. Exec. Order No. 12,333, 46 Fed. Reg. 59941 (Dec. 4, 1981); *see also Executive Order 123333*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/surveillance/12333/ [https://perma.cc/9PX5-YP6B] (giving additional background to the order). Although E.O. 12,3333 has been amended several times throughout history, these changes have only increased the power of surveillance programs and widened its role as a

sperson as an arbitrator to be an insufficient improvement from Safe Harbor, because the position's autonomy and ability to make compulsory decisions was questionable.[142] The court was especially concerned that this role's close tie with US intelligence compromised its ability to protect EU citizens.[143]

In the same opinion, the court affirmed a different adequacy decision, which stated that standard contractual clauses (SCCs) can be a valid mechanism for personal data transfers.[144] SCCs are set clauses that businesses can adopt into a contract to properly protect their data transfers.[145] EU and US companies can use them to require safeguarding of data transfers because SSCs are internally binding and enforceable on the parties.[146] And because the Commission must institute the SCCs, this mechanism can serve as an alterna-

---

catchall provision for government intelligence activity. *See, e.g.*, *Executive Order 12333*, *supra* (noting the 2008 amendment by President George Bush to augment the already significant capabilities of the Director of National Intelligence).

[142] *Schrems II*, ECLI:EU:C:2020:559, ¶ 195. The Privacy Shield framework instituted the ombudsperson position. *Id.* ¶ 43. This position purported to be an uninfluenced and self-authoritative entity that was separate from US intelligence programs. *Id.* Thus, any suspicion that the court had as to the position's independence was directly counter-intuitive to its purpose. *See id.* ¶¶ 43, 195.

[143] *Id.* ¶ 195.

[144] *Id.* ¶¶ 124, 149; *see* Commission Decision 2010/87, *supra* note 136, art. 1, at 8 (finding standard contractual clauses to be "adequate safeguards" for data transfers). The Commission determines which collections of SCCs are appropriate for businesses to adopt into their contracts to permissibly trade data through Commission decisions. *Standard Contractual Clauses (SCC)*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en [https://perma.cc/GWN6-W58F] (commenting on the Commission's role in approving SCCs); *see* Steve Vella, *Why Use the Standard Contractual Clauses?*, GTG ADVOCS. (July 26, 2019), https://www.gtgadvocates.com/why-use-the-standard-contractual-clauses/ [https://perma.cc/A2YY-UDQW] (introducing the various SCCs that the Commission has introduced). Prior to *Schrems II*, the Commission had approved three groupings of clauses. Vella, *supra*. *See generally* Commission Decision 2010/87, *supra* note 136 (providing for SCCs as an adequate mechanism); Commission Decision 2004/915, of 27 December 2004 Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, 2004 O.J. (L 385) 74 (EC) (offering an "alternative set of standard contractual clauses" to an earlier 2001 decision); Commission Decision 2001/497, 2001 O.J. (L 181) 19 (EC) (issuing, for the first time, a group of SCCs that would allow lawful transfers to foreign countries according to the requirements in Directive 95/46/EC). In light of the *Schrems II* decision, the Commission released a new decision updating the older SCCs. *See generally* Commission Implementing Decision (EU) 2021/914, of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/678 of the European Parliament and of the Council, 2021 O.J. (L 199) 31, 31–32 (broadening the applicability of SCCs to four different "module[s]" for international data transactions).

[145] Szép, *supra* note 9, at 46; *see* Whitney, *supra* note 90 (giving background to SCCs). SCCs are also called "model contractual clauses." Whitney, *supra* note 90.

[146] Vella, *supra* note 144 (outlining what SCCs are and how to use them); *see Schrems II*, ECLI:EU:C:2020:559, ¶ 124 (discussing the Commission's decision on the validity of SCCs). Immediately following the *Schrems I* decision, there was concern that the ruling would effectuate a complete standstill in transatlantic data transfers. *See* Boardman et al., *supra* note 30 (addressing several questions arising from the invalidation of Safe Harbor). There were, nevertheless, "other legal bases" for data to continue being transferred. *Id.* SCCs are one of those bases. Vella, *supra* note 144.

tive to establish "adequacy" for importing personal data from the EU to the US.[147]

In the absence of a country-wide negotiated transatlantic mechanism, SCCs have been the best alternative to make a lawful transfer.[148] Nevertheless, the CJEU was not receptive to the absolute legality of this mechanism, and made its lawful application incredibly stringent.[149] The adequacy of an SCC would depend on the requesting party's national standard.[150] The court, however, was unclear on how to ensure the validity of a data transfer when using SCCs.[151] Instead, the court required an individual evaluation to ensure the lawfulness of transfer.[152] This means that the utility of SCCs remains uncertain.[153]

---

[147] *See* Szép, *supra* note 9, at 46 (discussing the Commission's role in enacting SCCs); Alexander Zinser, *The European Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries: An Effective Solution?*, 3 CHI.-KENT J. INTELL. PROP. 24, 25 (2003) (explaining that the SCCs are mechanisms that may be used for "adequacy"). Successful SCCs will: (1) guarantee a substantial amount of protection that meets the standards of EU law; (2) support the needs of individuals whose data is used or processed; and (3) enforce any liability that may arise from provisional breaches. *Id.* There were, nevertheless, several exemptions to Directive 95/46. *See* Directive 95/46/EC, *supra* note 83, art. 26, at 46. For example, data could be lawfully transmitted to a country that is not "adequate" if the person gave unequivocal permission for it to occur. *Id.* art. 26(a), at 46.

Another popular and alternative mechanism is BCRs. Szép, *supra* note 9, at 46. BCRs are dissimilar to SCCs for several reasons. *Id.* Although SCCs are exclusively Commission-implemented, BCRs are more akin to "a code of conduct" that must be followed for sufficient protection to be met. Whitney, *supra* note 90. Further, BCRs are initiated by the individual entity and must thereafter be approved by the proper EU data privacy administration to be valid. *Id.*

[148] *See* Boardman et al., *supra* note 30 (discussing the viability of alternative mechanisms, such as SCCs and BCRs, and concluding that SCCs are likely better to use than BCRs).

[149] *See Schrems II*, ECLI:EU:C:2020:559, ¶¶ 125–126, 134 (commenting that the adequacy of SCCs may depend on a "case-by-case" evaluation that considers the sufficiency of law in the business's home-country).

[150] *Id.* The court concluded that SCCs are not "per se" valid or invalid. MILDEBRATH, *supra* note 12. Rather, the mechanism could have varying degrees of sufficiency. *See id.* (noting that SCCs' validity depends on the safeguards offered by the business in combination with the protections from the foreign country).

[151] *See Schrems II*, ECLI:EU:C:2020:559, ¶ 133 (explaining that SCCs may be insufficient to protect European data, but failing to describe what "supplementary measures" would be necessary to do so). SCCs are cookie-cutter agreements approved by the Commission that may effectively be copied and pasted into transatlantic data trade contracts. *See id.* (noting that SCCs do not vary from country to country). Thus, the court reasoned that the sufficiency of SCCs might depend on the nationality of the foreign entity and the degree of additional protection afforded by its home country's laws. *Id.* An entity based in a country with higher data privacy standards would thereby require less augmentation to be compliant with the EU. *See id.* (proposing that external national standards continue to play a role in individualized adequacy). The burden rests on the organizations to make sure that there is proper protection before trading the data. *See id.* at ¶¶ 134, 142 (obligating data "controller[s]" to "verify [that] . . . adequate protection" will be met "prior to any transfer" of data).

[152] Christopher Kuner, *The* Schrems II *Judgment of the Court of Justice and the Future of Data Transfer Regulation*, EUR. L. BLOG (July 17, 2020), https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/ [https://perma.cc/RK6G-RB4W]. Because the requirements for one organization to make transfers lawfully may be different from those of another, using SCCs requires "mini adequacy decisions" for each entity. *Id.*

Therefore, *Schrems II* created significant ambiguity for the EU and the US to clarify to guarantee the future of transatlantic data trading.[154]

II. Where Should We Begin: The *Schrems II* Decision Asks the EU and US to Re-strike the Balance Between Privacy and Profitability

The CJEU's invalidation of the Privacy Shield in *Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II)* in July 2020 re-opened the dialogue about the intricacy of privacy legislation and accentuated the international and intranational differences among data regulations.[155] Section A of this Part examines the incentives and deterrents that the EU and US face in light of the CJEU's invalidation of Privacy Shield in *Schrems II*.[156] Section B briefly surveys US states for privacy legislation that supplements the federal standard.[157] Section C considers the recent privacy regulations promulgated in California, which make it the strictest regulator of personal information in the US.[158]

A. Without Privacy Shield, the EU and US Must Determine What Comes Next

Since the CJEU struck down Privacy Shield in July 2020, both the EU and the US have been left to question the future of a new transatlantic data trading mechanism.[159] Subsection 1 of this Section presents the general sentiments of the EU and US governments towards renegotiation.[160] Subsection 2 discusses the alternative mechanisms used for data transfers in the absence of

---

When using SCCs, it is the duty of the organization to determine whether there is proper protection in place. *Schrems II*, ECLI:EU:C:2020:559, ¶ 134.

[153] *See Schrems II*, ECLI:EU:C:2020:559, ¶¶ 125–126 (limiting SCCs to situational applicability).

[154] *See* Ryan Chiavetta, *The Post-* 'Schrems II' *Road Isn't Clear, but Privacy Pros Can Still Take Steps Forward*, IAPP (Dec. 15, 2020), https://iapp.org/news/a/the-road-isnt-clear-but-privacy-pros-can-still-take-steps-forward-post-schrems-ii/ [https://perma.cc/NB43-GUZD] (commenting that businesses were perplexed and worried about what to do immediately following the *Schrems II* opinion).

[155] *See* Case C–311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶ 201 (July 16, 2020) (invalidating Privacy Shield in July 2020).

[156] *See infra* notes 159–197 and accompanying text.

[157] *See infra* notes 198–206 and accompanying text.

[158] *See infra* notes 207–215 and accompanying text.

[159] *Schrems II*, ECLI:EU:C:2020:559, ¶ 201; *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/ [https://perma.cc/WV6F-E23R] (calling the *Schrems II* decision confusing to process).

[160] *See infra* notes 163–175 and accompanying text.

Safe Harbor and Privacy Shield.[161] Subsection 3 addresses one of the largest concerns presented by the EU–US surveillance legislation.[162]

1. The EU and US Generally Desire a New Agreement

Schrems II left the corporate market with a significant burden that was instantly enforceable.[163] In quick response to the decision invalidating Privacy Shield, the US Department of Commerce and the Commission issued a joint statement pledging their intent to find and renegotiate an alternative agreement.[164] The declaration acknowledged the difficult balance between individual privacy protection and economic prosperity, but also committed to finding a viable replacement to the mechanism.[165]

The US has advocated for the expeditious renegotiation of a transatlantic data transfer mechanism.[166] The same day that the *Schrems II* decision was released, the US Secretary of Commerce published a statement acknowledging the agency's dissatisfaction with the invalidation of Privacy Shield.[167] It also stated that the US would learn from *Schrems II*.[168] The statement emphasized the department's concern over the sweeping ramifications that the decision would have on American businesses, as well as the need to find an alternative quickly.[169] In a similar statement, the US Secretary of State reaffirmed the De-

---

[161] *See infra* notes 176–186 and accompanying text.

[162] *See infra* notes 187–197 and accompanying text.

[163] *See* Edgar Hidalgo et al., *The EU-U.S. Privacy Shield Invalidated: What It Means for U.S. Companies*, JD SUPRA (July 17, 2020), https://www.jdsupra.com/legalnews/the-eu-u-s-privacy-shield-invalidated-74627/ [https://perma.cc/4TNM-KZAB] (commenting on the immediacy of the implications of *Schrems II*).

[164] *See* Press Release, U.S. Dep't of Com., *supra* note 11 (stating that the EU and US had already begun to consider the replacement for Privacy Shield shortly after the *Schrems II* decision).

[165] *See id.* (remarking on the significance of both an individual's ability to safeguard information and the economic struggles faced worldwide caused by COVID-19).

[166] *See* MILDEBRATH, *supra* note 12 (mentioning the urgency expressed by US officials in connection with the ongoing economic struggles faced by the US in 2020).

[167] *See* Press Release, U.S. Dep't of Com., U.S. Secretary of Commerce Wilbur Ross Statement on *Schrems II* Ruling and the Importance of EU–U.S. Data Flows (July 16, 2020), https://useu.usmission.gov/u-s-secretary-of-commerce-wilbur-ross-statement-on-schrems-ii-ruling-and-the-importance-of-eu-u-s-data-flows/ [https://perma.cc/ES7U-CNAH] (lamenting the CJEU's decision to strike down the Privacy Shield mechanism).

[168] *See id.* (assuring that the US Department of Commerce would work with the EU to minimize the repercussions of *Schrems II*).

[169] *See id.* (stating that all businesses and trades rely on their ability to sell information internationally). Notably, at the time of invalidation, the Privacy Shield program hosted and supported more than 5,300 US companies. *Id.* Ross also commented on the department's intention to carry on with Privacy Shield, despite its inapplicability to EU data transfers. *See id.* (allowing the program to proceed after the *Schrems II* decision).

partment of Commerce's apprehension toward the lasting effect that stifling international personal data trade would have on the economy.[170]

The EU expressed similar sentiments favoring the preservation of international data trade with the US.[171] The EU, however, simultaneously acknowledged that it would not compromise individual protection for the sake of economic viability.[172] Vice-President Vera Jourová of the Commission for Values and Transparency released a statement acknowledging the uncertainty caused by the *Schrems II* decision for both EU and US businesses alike.[173] She proposed that they could use the ruling as a resource to understand how best to move forward with a transatlantic agreement.[174] The Commissioner for Justice Didier Reynders furthered the Vice-President's remarks by suggesting that a focus on alternative mechanisms may be the most effective way to solidify the transatlantic data trade.[175]

2. The Feasibility of SCCs to Regulate the Transatlantic Data Trade

Without Safe Harbor or Privacy Shield, both European and American businesses have had to seek legal shelter in substitute structures.[176] One alternative that the EU and US could focus a future agreement on are SCCs.[177] *Schrems II* specifically upheld the possibility for an entity to make a lawful

---

[170] Press Statement, Michael R. Pompeo, Sec'y, Dep't of State, European Court of Justice Invalidates EU-U.S. Privacy Shield (July 17, 2020), https://ee.usembassy.gov/2020-07-20-1/ [https://perma.cc/JM3X-A4U7] (expressing concern over the millions of workers impacted). The transatlantic data trade is worth more than $7.1 trillion dollars. *Id.*

[171] *See* Press Statement, Eur. Comm'n, Opening Remarks by Vice-President Jourová and Commissioner Reynders at the Press Point Following the Judgment in Case C-311/18 Facebook Ireland and Schrems (July 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1366 [https://perma.cc/47VJ-PBWE] (attempting to calm the concerns from European and American businesses in the wake of *Schrems II* by assuring them that transatlantic data trade will proceed).

[172] *See id.* (stating Vice-President Jourová's claim that the *Schrems II* decision also reaffirmed the notion that the EU would fight to protect European data extraterritorially). Jourová claimed that the future of transatlantic data trade would need to be consistent with: (1) *Schrems II*; (2) EU legislation; and (3) the inherent human right to privacy. *See id.* (enumerating the Vice-President's guarantees to Europeans in any ensuing agreement).

[173] *See id.* (noting the confusing implications of *Schrems II* for businesses).

[174] *See id.* (claiming that the EU and US will be able to use the *Schrems II* dicta and holding to build a better arrangement moving forward).

[175] *See id.* (praising the court for allowing SCCs to stand after *Schrems II*).

[176] *See* Szép, *supra* note 9, at 46 (stating that, in the absence of Privacy Shield, businesses must use surrogate arrangements, like SCCs and BCRs); *see, e.g.*, Cooper et al., *supra* note 110 (acknowledging that after *Schrems II*, all businesses making data transfers from EU states to the US had to rely on other practices, such as SCCs, to continue).

[177] *See* Press Statement, Eur. Comm'n, *supra* note 171 (praising the court for allowing SCCs to stand after *Schrems II*); *see also supra* notes 144–147 and accompanying text (defining and explaining SCCs).

data transfer without Privacy Shield by using these provisions.[178] The Commission has shown great hope for SCCs as well.[179] Therefore, they are likely the best alternative and most reliable replacement.[180]

But there remains some suspicion about the viability of these alternative mechanisms in the absence of a broader transatlantic data trade agreement.[181] Shortly after *Schrems II*, the Commission acknowledged that the EU would need to update their SCCs if they were to continue as the substitute for a Privacy Shield agreement.[182] One major concern is that older SCCs only apply to data transfers from EU controllers to another controller and EU controllers to EU processors, meaning that US processors cannot use them.[183] And, updated SCCs that do provide for US processors are incredibly new, not yet required, and their success remains unproven.[184] Moreover, no SCCs necessarily ensure

---

[178] Case C–311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶¶ 124, 149 (July 16, 2020).

[179] *See* Press Statement, Eur. Comm'n, *supra* note 171 (noting Commissioner Reynders' discussion of SCCs as a potential replacement with necessary modifications). In November 2020, the Commission released a draft document for new SCCs that countries such as the US could use to achieve lawful data transfers. *See Data Protection—Standard Contractual Clauses for Transferring Personal Data to Non-EU Countries (Implementing Act)*, EUR. COMM'N, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries [https://perma.cc/KQH6-W33C] (tracking the development of new SCCs produced by the EU after *Schrems II*).

[180] *See* Boardman et al., *supra* note 30 (finding SCCs to be a more practical solution because common corporate approval requirements make them less complicated, more efficient, and less uncertain than BCRs). Although not decided upon by the CJEU, BCRs should anticipate being assessed in a similar fashion to SCCs moving forward. *See* K Royal, *The Privacy Shield Is Broken*, ACC DOCKET (Dec. 10, 2020), https://www.accdocket.com/privacy-shield-broken [https://perma.cc/TCM4-AED8] (meshing the application of both mechanisms).

[181] *See* Armingaud et al., *supra* note 90 (claiming that the CJEU's decision to uphold SCCs may actually cause more problems than it resolved because their viability depends on the country's regulations, which the court simultaneously deemed inadequate).

[182] *See* Press Statement, Eur. Comm'n, *supra* note 171 (noting Commissioner Reynders' comments that changes are necessary to update some more-antiquated aspects of SCCs).

[183] *See* Royal, *supra* note 180 (advising that SCCs can only apply to US controllers and provide no support for inter-processor trading across the Atlantic). A "controller" is a business that decides: (1) to process personal data; (2) the reason to process it; and (3) in what way. *What Is a Data Controller or a Data Processor?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en [https://perma.cc/4QVL-B4ZN]. Alternatively, a "processor" is a business that helps the controller accomplish its goals. *Id.* Processors act as contractors to controllers. *Id.* Nevertheless, a single organization can play both roles. *See id.* (providing two examples to better understand the roles of controllers and processors).

Theoretically, a data transfer could occur between: (1) an EU controller and a US controller; (2) an EU processor and a US controller; (3) an EU processor and a US processor; or (4) an EU controller and a US processor. *See* Commission Implementing Decision (EU) 2021/914, *supra* note 144, at 32–33 (contemplating those four possibilities). Businesses, however, may only use older SCCs in the first two scenarios. Royal, *supra* note 180.

[184] *See* Commission Implementing Decision (EU) 2021/914, *supra* note 144, at 32 (allowing the SCCs to apply to data transfers from the EU to processors in non-EU countries); Martin Braun et al.,

that a data trade will be lawful.[185] Notably, the *Schrems II* decision left open the possibility for SCCs to be permissible, but only when deemed adequate in conjunction with the country's personal data practices and regulations.[186]

3. US Surveillance Presents a Significant Hurdle for Renegotiation

When assessing the sufficiency of the US privacy regime, however, the EU has maintained particular concern with the country's surveillance scheme.[187] Both the CJEU opinions in *Schrems v. Data Protection Commissioner* (*Schrems I*) and *Schrems II*, in 2015 and 2020, respectively, focused partly on US counter-intelligence practices to invalidate Safe Harbor and Privacy Shield.[188] Specifically, in *Schrems II*, the court focused on legislation,

---

European Commission Adopts and Publishes New Standard Contractual Clauses for International Transfers of Personal Data, WILMERHALE (June 7, 2021), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20210607-european-commission-adopts-and-publishes-new-standard-contractual-clauses-for-international-transfers-of-personal-data [https://perma.cc/5AAE-JS9M] (commenting that the adequacy of the updated SCCs is unclear because they are still early-stage). The Commission released new SCCs on June 4, 2021. Commission Implementing Decision (EU) 2021/914, *supra* note 144, at 31. The modernization effort sought to streamline SCCs into a standalone comprehensive decision. *See* Braun et al., *supra* (explaining that the directive included provisions for four different categories of data transfer in a single record). The most recent SCCs provide clauses for personal data transfers from an: (1) EU controller to a non-EU controller; (2) EU controller to a non-EU processor; (3) EU processor to a non-EU processor and sub-processor; and (4) EU processor to a non-EU controller. Commission Implementing Decision (EU) 2021/914, *supra* note 144, at 32–33. Additionally, Commission Implementing Decision (EU) 2021/914 provided some guidance to international data collectors in countries with more troublesome privacy laws, like the US—mainly that the less interaction the collector had with the government, the more likely it was to be compliant. *See id.* at 53 n.12 (stating that "different elements may be considered" to assess an entity's adequacy, including "relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests"). The new Commission did not require businesses to adopt the new SCCs immediately, rather allowing them until 2023 to convert over. *Id.* at 31.

[185] *See* Umhoefer & Serwin, *supra* note 159 (emphasizing the fact that the CJEU merely concluded that SCCs could be used to make a lawful transfer, and not that they would guarantee one). The legality of a transfer using SCCs was tied closely to the adequacy of national regulations. *See* Case C–311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶ 126 (July 16, 2020) (showing that the validity SCCs depends on the laws provided by the relevant country).

[186] *See Schrems II*, ECLI:EU:C:2020:559, ¶¶ 126, 149 (holding that SCCs, when viewed in addition to national protections, can be valid); Umhoefer & Serwin, *supra* note 159 (commenting that the court's holding was not as beneficial as it might appear).

[187] *See Schrems II*, ECLI:EU:C:2020:559, ¶¶ 60, 61, 63, 65, 166, 178–81, 184, 192 (discussing the US surveillance law, the Foreign Intelligence Surveillance Act (FISA), and its counterparts at great length); Case C–362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650, ¶ 33 (Oct. 6, 2015) (acknowledging some concern for US surveillance practices).

[188] *See Schrems II*, ECLI:EU:C:2020:559, ¶¶ 179–180 (leaning on US surveillance regulations and practical applications as a basis for its holding that Privacy Shield is unusable); *Schrems I*, ECLI:EU:C:2015:650, ¶ 30 (contemplating the lower court's assessment of US federal security agencies).

such as the Foreign Intelligence Surveillance Act (FISA), which allows for various US surveillance programs.[189]

First passed in 1978, FISA provides the US government with the ability to monitor individuals anonymously and, in fact, to do so without meeting procedural standards elsewise required.[190] At its core, the federal law purported to balance the government's need to safeguard the US with the privacy entitlements provided by the Bill of Rights.[191] But, the scope of FISA's reach has fluctuated over years, often broadening or shrinking in response to the public's perception of national security.[192] The government, however, has always used the statute to collect personal and private information throughout its history.[193]

---

[189] *See Schrems II*, ECLI:EU:C:2020:559, ¶ 165 (explaining the court's concern with section 702 of FISA); Maldoff & Tene, *supra* note 74, at 227 (discussing the concern held by the CJEU that the US federal government would actively permit and promote the actions of the NSA). *See generally* 50 U.S.C. § 1881a (providing section 702 of FISA, as amended, which specifically allows US surveillance programs to investigate foreigners, like EU citizens).

[190] *See* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1633 (2010) (commenting that FISA removes the requirement that the US government meet usual "probable cause" standards, and replaces it with an altered standard). *See generally* Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, § 106, 92 Stat. 1783, 1793–95 (codified as amended at 50 U.S.C. § 1806) (providing the US government with broad powers to surveil without disclosure that they are doing so). Congress has since updated and amended FISA with several pieces of legislation, including the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) of 2001 and the FISA Amendments Act of 2008. *See* FISA Amendments Act of 2008, Pub. L. No. 110-261, §§ 101–201, 122 Stat. 2436, 2437–70 (codified as amended at 50 U.S.C. §§ 1881–1885c) (amending FISA to include more ways for the government to obtain data); USA PATRIOT ACT of 2001, Pub. L. No. 107-56, 115 Stat. 272 (providing for the counteraction of terrorism). Outside of FISA, the government must rationally suspect that an individual took part or would take part in a violation of the law to obtain such information. *See* U.S. CONST. amend. IV (requiring "probable cause" to inspect an individual or confiscate belongings); Jonathan Kim, *Fourth Amendment*, LEGAL INFO. INST. Para. II.B, https://www.law.cornell.edu/wex/fourth_amendment [https://perma.cc/ZF8J-7A29] (June 2017) (explaining the standard in terms of a police investigation). But, under the protection of FISA, the government need only demonstrate some suspicion that an individual is an agent to another country. *See* Banks, *supra*, at 1633 (discussing the difference between probable cause standards inside and outside of the FISA umbrella).

[191] *See* Banks, *supra* note 190, at 1633 (complimenting the early institution of FISA); William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1214 (2007) (begging the US government to return FISA back to its better-balanced intentions).

[192] *See* Banks, *supra* note 191, at 1211–12 (providing a historic account of FISA limitations waxing and waning). The Supreme Court began to reduce the scope of federal surveillance in the 1960s, fearing that it might over-impose on the privacy rights of Americans. *See id.* (citing the 1960s as a time that privacy rights shifted balance toward the individual). After Watergate, however, the US adopted measures to prevent similar tapping from exposing the country to foreign powers. *See id.* (distinguishing the 1970s as a shift in balance back toward the government). Most significantly, in the immediate aftermath of 9/11, the US adopted even broader legislation to provide the government with increased power to oversee the actions of suspected terrorists. *See id.* at 1212 (suggesting that the 2000s represented the largest shift in favor of the government's powers under FISA).

[193] *See Warrantless Surveillance Under Section 702 of FISA*, ACLU, https://www.aclu.org/issues/national-security/privacy-and-surveillance/warrantless-surveillance-under-section-702-fisa [https://perma.cc/B3QP-R55G] (detailing the government's collection of personal data under the guise of

Many, including the CJEU, have criticized FISA for compromising too far in favor of the government and leaving the people's personal information vulnerable.[194] There are several known instances of the government directly subverting its requirements to invade individual privacy.[195] Furthering the sentiment in *Schrems I*, the *Schrems II* decision blanketly sourced FISA's current implementation as precluding the US from being "adequate" to use European data.[196] Consequently, US surveillance practices are necessarily an obstacle for the EU and US to renegotiate a sustainable data trading agreement.[197]

B. From Sea to Shining (Priva)Sea

Another significant complication for reforming Privacy Shield is the lack of consistent data privacy regulation within the US's borders.[198] Because of the US's two-tiered sovereignty structure, states are able to elevate their protections to a higher standard than that required by the federal government.[199] As a

---

FISA through a critical lens). Misuses of FISA and intrusions upon the privacy rights of individuals often disproportionally affect ethnic and cultural minorities. *See id.* (reporting on the inherently racist way that FISA has been used). In April 2018, Jake Laperruque, the senior counsel to the Constitution Project, an organization focused on government surveillance, testified to the House Committee on Appropriations' Subcommittee on Defense that government officials often use surveillance programs to unacceptably prey upon certain religious groups without a substantial reason to do so. Jake Laperruque, *In Support of Research and Reporting on the Disparate Use and Impact of* FISA, POGO (Apr. 8, 2019), https://www.pogo.org/testimony/2019/04/in-support-of-research-and-reporting-on-the-disparate-use-and-impact-of-fisa/ [https://perma.cc/2VG4-MZ7B]. These officials often use broad language of surveillance statutes to shield their racist intrusions under the pretext of self-protection. *Id.*

[194] *See, e.g.*, *Schrems II*, ECLI:EU:C:2020:559, ¶ 180 (bringing into question the amount of power that FISA provides to the government); Banks, *supra* note 191, at 1214 (suggesting that recent FISA practices did not properly account for fundamental civil liberties, including individual privacy).

[195] *See, e.g.*, *Foreign Intelligence Surveillance Act (FISA)*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/surveillance/fisa/#Overview [https://perma.cc/9HH2-3AQL] (citing "Crossfire Hurricane" as one instance of the FBI directly violating FISA). A more recent example of the government subverting FISA occurred in 2016 through 2017 when the FBI investigated a Donald Trump presidential campaign official, Carter Page. *See id.* (discussing the unravelling of "Crossfire Hurricane"). Although the agency could not and did not meet the requisite cause standards to monitor Page, the FBI proceeded to do so anyway. *Id.* At the conclusion of this scandal, the agency was merely accosted by a report that suggested that the FBI rework its practices to better comply in the future and guarantee that it would properly document any other investigations that it was pursuing. *See id.*

[196] *Schrems II*, ECLI:EU:C:2020:559, ¶¶ 180–181; *see Schrems I*, ECLI:EU:C:2015:650, ¶ 30 (stating that US surveillance may be a greater issue than addressed in the present case).

[197] *See* Joshua P. Meltzer, *Why* Schrems II *Requires US-EU Agreement on Surveillance and Privacy*, BROOKINGS (Dec. 8, 2020), https://www.brookings.edu/techstream/why-schrems-ii-requires-us-eu-agreement-on-surveillance-and-privacy/ [https://perma.cc/SHV3-6JBP] (commenting that a successful agreement will require the EU and US to address the court's clear issues with US surveillance practices).

[198] *See* Voss, *supra* note 29, at 410 (contending that the lack of consistency in US data privacy legislation will be a source of struggle and monetary loss).

[199] *See* U.S. CONST. art. VI, cl. 2 (providing the constitutional Supremacy Clause that gives preference to federal regulation over state laws); Daunt, *supra* note 104 (distinguishing that, so long as

result, the privacy rights of American citizens can significantly depend on their state-level residency.[200]

The only US states that have passed broad privacy legislation are California, Colorado, and Virginia.[201] Delaware and Illinois also have impressive privacy regulations.[202] Several other states have recently introduced similar legislation in their respective governments.[203] Notwithstanding their attempts, the majority have not successfully passed those laws.[204] Other states, like Wyoming and Idaho, have notably few privacy laws and have made no attempt to pass comprehensive ones.[205] California has proven to be the national leader in this area and regulates data more stringently than any other US state.[206]

---

there are no conflicts between a state and federal law, a state can provide additional rights through legislation).

[200] *See* Casey Leins, *States with the Strongest Online Privacy Protections*, U.S. NEWS (Oct. 23, 2019), https://www.usnews.com/news/best-states/articles/2019-10-23/states-with-the-strongest-online-privacy-laws [https://web.archive.org/web/20200112153331/https://www.usnews.com/news/best-states/articles/2019-10-23/states-with-the-strongest-online-privacy-laws] (depicting the significant disparity between privacy regulations in higher and lower ranked US states).

[201] *US State Privacy Legislation Tracker: Bills Introduced 2021*, IAAP, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf [https://perma.cc/MT2J-GHQN] (Sept. 1, 2021). California has passed two comprehensive privacy laws in recent years. *See infra* notes 207–214 and accompanying text (discussing California's privacy regulations in detail). In July 2021, Colorado passed Colorado Senate Bill 21-190, the "Colorado Privacy Act." S.B. 21-190, 73d Gen. Assemb., 1st Reg. Sess. (Colo. 2021); *US State Privacy Legislation Tracker: Bills Introduced 2021*, *supra*. Similarly, in March 2021, Virginia passed the comprehensive Virginia Senate Bill 1392, called the "Consumer Data Protection Act." S.B. 1392, 2021 Gen. Assemb., 1st Spec. Sess. (Va. 2021); *US State Privacy Legislation Tracker: Bills Introduced 2021*, *supra*.

[202] *See* Paul Bischoff, *Internet Privacy Laws by State: Which US States Best Protect Privacy Online?*, COMPARITECH, https://www.comparitech.com/blog/vpn-privacy/which-us-states-best-protect-online-privacy/ [https://perma.cc/4MET-CMYY] (July 27, 2021) (ranking states by privacy protection and giving Illinois one of the top scores); Leins, *supra* note 200 (highlighting Delaware as a state that has better standards than most states in 2019).

[203] *US State Privacy Legislation Tracker: Bills Introduced 2021*, *supra* note 201.

[204] *Id.* Massachusetts, New York, North Carolina, Ohio, and Pennsylvania all have pending proposed privacy legislation as of publication. *Id.* But, the legislation proposed in Alabama, Alaska, Arizona, Connecticut, Florida, Illinois, Kentucky, Maryland, Minnesota, Mississippi, North Dakota, Oklahoma, Texas, Utah, Washington, and West Virginia were all unsuccessful. *Id*. That means that, of twenty-four states, only three have succeeded in introducing large state privacy acts. *Id.* These bills may have failed because political parties tend to disagree on where best to draw the line for privacy regulation. *See* Kendra Clark, *The Current State of US State Data Privacy Laws*, THE DRUM (Apr. 26, 2021), https://www.thedrum.com/news/2021/04/26/the-current-state-us-state-data-privacy-laws [https://perma.cc/2E5M-XXEU] (commenting that recent privacy bills did not succeed because some advocates felt they went too far, while others felt they did not go far enough).

[205] *See* Bischoff, *supra* note 202 (ranking those two states among the worst privacy regulators); *US State Privacy Legislation Tracker: Bills Introduced 2021*, *supra* note 201 (not including Wyoming or Idaho as states that brought privacy bills to their legislature). The state of Wyoming provided the least amount of additional privacy protection to its citizens, lagging significantly behind the nation's frontrunners. *See* Leins, *supra* note 200 (scoring Wyoming last, and rating the state as fifteen times less protective than California). Mississippi also has worse privacy regulation than most states, but attempted to pass Mississippi Senate Bill 2612 on privacy legislation in 2021. Bischoff, *supra* note 202; *US State Privacy Legislation Tracker: Bills Introduced 2021*, *supra* note 201. *See generally* S.B.

C. Take the 405 to Better Privacy Protection: California Becomes the Strictest Personal Data Regulator in the US

The California Consumer Privacy Act (CCPA) of 2018, effective in 2020, marks the first instance of a state adopting such broad and generalized data privacy regulation.[207] The legislature sought to provide its population with fundamental privacy rights not yet afforded by federal or other states' laws.[208] Subsequently, in November 2020, California adopted the California Privacy Rights Act (CPRA) of 2020, which will broaden the privacy rights of Californians even more by 2023.[209]

Both the CCPA and CPRA read like pseudo-omnibus legislation, and both share vast similarities with the EU's GDPR.[210] For example, both the CCPA and GDPR provide individuals with the right to obtain their data, to receive that data in a usable format, and to request that businesses delete that data.[211]

2612, 2021 Leg., Reg. Sess. (Miss. 2021) (providing the failed Mississippi Consumer Data Privacy Act).

[206] *See* Leins, *supra* note 200 (crowning California as the best regulated state in the US). Although Maine was not the highest ranked state, it was the only state to ban its police from using mobile data to monitor individuals' locations. *See id.* (recognizing Maine as best regulated in this specific sector).

[207] *See* Brian Hengesbaugh & Amy de la Lama, *US State Omnibus Privacy Laws—A Primer*, GLOB. COMPLIANCE NEWS (July 26, 2019), https://globalcompliancenews.com/us-state-omnibus-privacy-laws-primer-20190703/ (suggesting that the CCPA was the initial step towards state omnibus laws in the US); Liens, *supra* note 200 (claiming that California has the highest caliber of privacy legislation in the US). *See generally* CAL. CIV. CODE §§ 1798.100–.199.95 (Supp. 2021) (providing the CCPA, which gives Californians many additional means and assurances to better protect their data).

[208] *See California Consumer Privacy Act (CCPA)*, STATE OF CAL. DEP'T OF JUST., OFF. OF THE ATT'Y GEN., https://oag.ca.gov/privacy/ccpa [https://perma.cc/37KM-XQYM] (listing the addition of the "right to know," "right to delete," "right to opt-out," and "right to non-discrimination" to Californians' bundle of privacy rights).

[209] *See* Brian H. Lam, *California Privacy Rights Act Passes—Dramatically Altering the CCPA*, NAT'L L. REV. (Nov. 6, 2020), https://www.natlawreview.com/article/california-privacy-rights-act-passes-dramatically-altering-ccpa [https://perma.cc/FHP5-Z7AZ] (discussing the success of Proposition 24 in California in November 2020, which will bring forth additional privacy rights by January 1, 2023). The California Privacy Rights Act (CPRA) of 2020 includes provisions covering: (1) a new regulatory agency that will administrate the law; (2) an expansion of the scope of businesses required to comply; (3) a heightened standard to provide sufficient notice about collection; (4) carved out standards for more delicate and personal data; and (5) generally required stricter standards for those who collect, use, or process data. *See id.* (listing the ways that the CPRA will add to the CCPA).

[210] *See* Hengesbaugh & de la Lama, *supra* note 207 (equating the CCPA to "omnibus" legislation). *See generally* Mark Smith, *ANALYSIS: California Privacy Reboot Puts Rights in Spotlight*, BLOOMBERG L. (Jan. 15, 2021), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-california-privacy-reboot-puts-rights-in-spotlight [https://perma.cc/YZ4Y-3K9R] (demonstrating the rights that the CPRA will add to the CCPA to make it even more reaching and similar to EU law).

[211] *See* LAURA JEHL & ALAN FRIEL, CCPA AND GDPR COMPARISON CHART 4–5 (2018), https://iapp.org/media/pdf/resource_center/CCPA_GDPR_Chart_PracticalLaw_2019.pdf [https://perma.cc/Z276-UVVS] (comparing the provisions of the CCPA with the GDPR and drawing similarities between the rights to "access," "portability," and "deletion"). For example, both the CCPA and GDPR

Likewise, both pieces of legislation have the potential to affect entities outside of their natural jurisdictions.[212] In instances where the two laws differ, most often the GDPR is the stricter provision.[213] There are, nevertheless, some provisions wherein the CCPA regulates data collection more than the EU does.[214] Because of these qualities, it is likely that California's privacy regime is better suited than the US's to meet the adequacy requirements set by the EU in *Schrems II*.[215]

III. WINNING THE BATTLE BY USING STATE-BASED ADEQUACY TO OVERCOME *SCHREMS III*

Following the CJEU invalidating Privacy Shield in *Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II)*, in July 2020, the future of the transatlantic data trade and American adequacy is indeterminate.[216] Schrems will undoubtedly continue to push back against any agreements made

---

provide essentially the same provisions requiring entities to store data in a manner that makes it compatible and understandable if the user ever wishes to access it. *Compare* CIV. §§ 1798.100(d), 1798.130(a)(2) (requiring businesses to reply to data requests with immediately utilizable responses), *with* Regulation (EU) 2016/679, *supra* note 10, art. 20, at 45 (demanding that businesses send the data in a familiar and discernable form).

[212] *See* CIV. § 1798.140(g) (providing the CCPA's extraterritorial provision); Regulation (EU) 2016/679, *supra* note 10, art. 4(1), at 33 (supplying the related provision from the GDPR).

[213] *Compare* CIV. § 1798.105(d) (providing Californian businesses with discretion to deny an individual's request to erase their data), *with* Regulation (EU) 2016/679, *supra* note 10, art. 17, at 43–44 (allowing little flexibility to entities with the right to erasure). One of the more significant differences where the GDPR is the more restrictive law is its "legal basis" requirement. Umhoefer, *supra* note 107. The CCPA does not demand that businesses prove their legal ground for processing consumer data. *Id.*

[214] *See, e.g.*, CIV. §§ 1798.120, 1798.135(a)–(b) (depicting an individual's absolute "right to opt-out" of having their data sold in California). Although the GDPR allows its citizens to opt-out of certain marketing and processing uses, it does not provide Europeans with an absolute right to not participate. *See* JEHL & FRIEL, *supra* note 211, at 4 (commenting on the dissimilarity between the opt-out provisions in the GDPR and the CCPA). *See generally* Regulation (EU) 2016/679, *supra* note 10 (missing an all-inclusive opt out provision). On the other hand, the CCPA allows Californians to opt out of any sale of data. *See* CIV. §§ 1798.120, 1798.135(a)–(b) (requiring businesses to include an obvious way for users to forbid the business from selling their data with the phrase "Do Not Sell My Personal Information"). In addition, because the US has federal privacy legislation at both the state and federal levels, provisions that do not appear in state privacy laws could already receive protection from relevant federal legislation. *See* Maldoff & Tene, *supra* note 74, at 221 (describing the tiered levels of privacy law in the US).

[215] *See* Maldoff & Tene, *supra* note 74, at 238–40 (suggesting that a sustainable adequacy determination must include: (1) understandable and available standards; (2) data minimization; (3) neutral supervision; and (4) an effective means to remedy violations). The court reasoned that the "essentially equivalent" requirement placed an obligation on states wishing to trade data with the EU to develop the proper data agencies required to safeguard information. *Id.* at 231.

[216] Chiavetta, *supra* note 154; *see* Case C–311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶ 201 (July 16, 2020).

with the US, effectively making a *Schrems III* case inevitable.[217] The EU and US should adopt a state-specific adequacy agreement because individual states are likely better suited to meet European standards than the federal government is.[218] Section A of this Part predicts the unavoidable reality of *Schrems III*, which necessitates the durability of a renegotiated transatlantic data trade mechanism.[219] Section B proposes and analyzes state-specific adequacy determinations as a possible solution to not only defeat *Schrems III*, but also to cultivate national adequacy over time.[220]

*A. With "*Schrems v. the Next Transatlantic Privacy Mechanism (Schrems III)*" on the Horizon, the US Must Forge the Path to Victory*

The US must initiate a suitable compromise with the EU because it cannot afford to lose *Schrems III*.[221] Although both parties have expressed that they are willing to develop a new transatlantic data transfer mechanism, the US has the greater incentive and capability to do so.[222] The US likely suffers more

---

[217] *See* MILDEBRATH, *supra* note 12 (noting Schrems' suggestion that the US completely change its surveillance regime to obtain adequacy from the EU); *Our Detailed Concept*, *supra* note 15 (suggesting that Schrems, and his organization, will instigate litigation that would provoke the EU to assess its privacy standards and relationships with other countries based on their regulations). At one point, Schrems went so far as to recommend that the best way to protect European data was to keep it within its jurisdiction. *See* Chander, *supra* note 110, at 771 (presenting Schrems' proposal for a closed border approach to privacy regulation). Given the sheer amount of money tied to the transatlantic data trade, this is unlikely to ever occur. *See* Press Release, U.S. Dep't of Com., *supra* note 167 (stating that the international market produced trillions of dollars). Schrems, nevertheless, has pledged himself and his organization to seek legal recourse. *See Our Detailed Concept*, *supra* note 15 (pledging to bring challenges like those in *Schrems I* and *Schrems* II). Importantly, both Safe Harbor and Privacy Shield were defeated by complaints that did not directly challenge them. *See generally Schrems II*, ECLI:EU:C:2020:559, ¶¶ 52–54 (stemming from a complaint about SCCs); Case C–362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650, ¶¶ 26–30, 35 (Oct. 6, 2015) (developing from a complaint about a commissioner's refusal to stop a Facebook subsidiary from making transfers to the US).

[218] *See infra* notes 232–260 and accompanying text.

[219] *See infra* notes 221–231 and accompanying text.

[220] *See infra* notes 232–260 and accompanying text.

[221] *See* Nigel Cory et al., *'*Schrems II*': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation*, INFO. TECH. & INNOVATION FOUND. (Dec. 3, 2020), https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic [https://perma.cc/3DM3-A4TA] (claiming that *Schrems II* will devastate thousands of American businesses). Ambiguity prevents businesses from trading data successfully. *Id.* The *Schrems II* decision put businesses at a significant risk to face harsh legal ramifications for misinterpreting the applicability of other transfer mechanisms, like SCCs. *See* Hidalgo et al., *supra* note 163 (acknowledging that Privacy Shield was no longer a valid mechanism at the exact moment the CJEU released its decision on July 16, 2020); Swagerman, *supra* note 85 (pointing out the dramatic economic hit that a business may take if the GDPR fines it).

[222] *Compare* Press Release, U.S. Dep't of Com., *supra* note 167 (expressing the US's desire to find a compromise with the EU on transatlantic privacy transfers quickly and demonstrating that the US should be incentivized to make a replacement work during a time of economic uncertainty), *with* Press Statement, Eur. Comm'n, *supra* note 171 (stating Commissioner Reynders' recognition that the

from *Schrems II* than the EU because the determination exclusively limits American businesses from profiting off of Europeans' data.[223] Meanwhile, European corporations can continue to process Americans' data without restriction.[224] The inability to fully use and profit from data ultimately burdens the US's economy, businesses, and citizens.[225] As the volume and profitability of personal data continue to grow over time, this harm will metastasize.[226]

The US is better suited than the EU to resolve that conflict for several reasons.[227] First, a national privacy structure ideally balances economic incentives with security risks.[228] Second, the US faces both economic loss and insuf-

---

EU wished to continue its close relationship with the US in the data trade even after the *Schrems II* decision, but that it would not compromise its fundamental privacy values).

[223] *See* Tony DeBos et al., *What to Do Now That the EU-US Privacy Shield Framework Is Invalid*, EY (Sept. 28, 2020), https://www.ey.com/en_us/consulting/what-to-do-now-that-the-eu-us-privacy-shield-framework-is-invalid [https://perma.cc/5P28-KV3N] (commenting on the disproportionate effect of the *Schrems II* decision between the EU and US); *FAQs—EU-U.S. Privacy Shield Program Update*, PRIV. SHIELD FRAMEWORK, https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update [https://perma.cc/SKE6-WT7J] (Mar. 31, 2021) (noting that *Schrems II* only limited the flow of data from the EU to the US). Although the decision put transatlantic data trade into question, the ability for an EU entity to collect, sell, or assess the data of a US citizen has never been brought into question. *See FAQs—EU-U.S. Privacy Shield Program Update*, *supra* (reflecting on the directional limitation imposed by the CJEU's decisions). Thus, although the stifling of transfers affected both sides, the EU could hold a favorable bargaining position in any future negotiation because *Schrems II* only limited data flow from the EU to the US. *See id.* (recognizing that *Schrems II* only stops US access to EU data).

[224] *See* RACHEL F. FEFER & KRISTIN ARCHICK, CONG. RSCH. SERV., IF 10896, EU DATA PROTECTION RULES AND IMPLICATIONS (9th version 2020), https://fas.org/sgp/crs/row/IF10896.pdf [https://perma.cc/7ZE6-G6MZ] (stating that the US does not limit the flow of its citizens' data to other countries). In 2018, the Bureau of Economic Analysis estimated that the EU traded $127 billion worth of data to the US. *Id.* The US nearly doubled that figure, trading $218 billion of data to the EU. *Id.*

[225] *See* NORTH, *supra* note 25, at 14 (suggesting that, in part, the benefit that an individual gains from data collection requires the collector to amass the information to make macroscopic decisions); Press Release, U.S. Dep't of Com., *supra* note 167 (worrying about the harsh economic impact that *Schrems II* would have on the economy); Cory et al., *supra* note 221 (claiming that Privacy Shield was especially harmful to smaller companies because they do not have the funds to use other mechanisms, like SCCs); *see also* MILDEBRATH, *supra* note 12 (presenting the argument that SCCs might only be plausible alternatives outside of the realities of US privacy and surveillance legislation); Boardman et al., *supra* note 30 (concluding that substitutes to SCCs are even less sufficient of a solution).

[226] *See* HURLEY, *supra* note 2, at 20 (proposing that data engulfs the world around us); Press Release, U.S. Dep't of Com., *supra* note 167 (estimating a $7.1 trillion, and growing, appraisal on the exchange of personal data between the EU and US).

[227] *See infra notes* 228–231 and accompanying text.

[228] *See* Hirsch, *supra* note 35, at 375 (demonstrating that privacy legislation has an inherent counterbalance between the individual privacy and broader economic concerns). The US does not necessarily strike the balance well. *See* Natasha Singer, *The Government Protects Our Food and Cars. Why Not Our Data?*, N.Y. TIMES (Nov. 2, 2019), https://www.nytimes.com/2019/11/02/sunday-review/data-protection-privacy.html [https://perma.cc/MNE3-P7CR] (questioning why the US government chooses to better protect people from less-personal tangible harm, like discontinuing an unsafe tablet device, but not preventing fundamental intangible harm, like a privacy violation).

ficient data security in the wake of *Schrems II*, whereas the EU has properly compromised profit for the sake of protection.[229] Moreover, the EU has made abundantly clear that it will not disregard its citizens' personal security to make an agreement with the US work.[230] Accordingly, the US must find the way for a transatlantic data agreement to survive an inevitable challenge in the CJEU.[231]

B. Brick by Brick, State by State: State-Based Adequacy as a Short-Term Fix to Propagate a Long-Term Solution

State-based adequacy is the best solution for the transatlantic data trade to continue and flourish.[232] Although it may only be a short-term answer, the US needs a workable strategy to defeat *Schrems III* now.[233] Federal law does not have a privacy standard that is sufficient to produce an impenetrable adequacy determination from the EU.[234] Individual states that meet the EU's standards should be allowed to negotiate state-based adequacy with the EU so that they can profit from transatlantic data.[235] Over time, state-specific adequacy will economically incentivize the collective US to meet EU adequacy standards,

---

[229] *See* ACQUISTI, *supra* note 48, at 3 (stating that there should be some inherent compromise between the value of trade and the value of privacy in data regulation). *See generally* Case C–311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559 (July 16, 2020) (limiting the amount of data that the US could collect, and therefore profit from, while also criticizing the US for having insufficient data privacy regulations).

[230] *See* Press Statement, Eur. Comm'n, *supra* note 171 (noting Vice-President Jourová's assurance that the EU policy will continue to favor protecting EU citizens' data over finding a sufficient agreement with the US). As EU courts and the Commission have made clear, they will continue to put the personal security of their citizens above any argument for the economy. *See Schrems II*, ECLI:EU:C:2020:559, ¶ 201 (eliminating a major mechanism for lucrative trade in the name of privacy protection); Press Statement, Eur. Comm'n, *supra* note 171 (indicating Vice-President Jourová's concession that the court made the correct decision in *Schrems II*).

[231] *See* Cory et al., *supra* note 221 (lamenting that businesses suffer when the US does not have clear-cut ways for its businesses to trade data abroad); Umhoefer & Serwin, *supra* note 159 (suggesting that the *Schrems II* decision left businesses in an improperly difficult situation).

[232] *See* Press Release, U.S. Dep't of Com., *supra* note 167 (commenting on the harm caused when the CJEU invalidated Privacy Shield). An unsuccessful outcome in *Schrems III* would likely have similar ramifications to those of *Schrems II*. *See id.* (dwelling on the economic complications that *Schrems II* caused).

[233] *See id.* (labeling the transatlantic data trade as a $7.1 trillion market).

[234] *See* Peter M. Lefkowitz, Opinion, *Why America Needs a Thoughtful Federal Privacy Law*, N.Y. TIMES (June 25, 2019), https://www.nytimes.com/2019/06/25/opinion/congress-privacy-law.html [https://perma.cc/N73W-S2DL] (commenting that the US does not have strong federal data privacy laws and arguing in support of the US adopting such legislation).

[235] *See* Andrea Little Limbago, *DIY Data Protection: As Congress Stalls, States Take Charge*, GCN (Mar. 23, 2020), https://gcn.com/articles/2020/03/23/states-lead-data-privacy-protections.aspx [https://perma.cc/VV2M-AKZM] (claiming that states are leading the way toward strong data privacy legislation in the US, while the federal government stands by the wayside). Although California is the current frontrunner in US data privacy legislation, many states follow closely behind it. *See id.* (claiming that a majority of states made headway to improve their privacy regulations in 2019).

because states will improve their regulations to compete in the transatlantic data trade.[236]

Some of the more highly regulated US states may be individually capable of satisfying European standards.[237] The best example being California, which substantially heightened its state protections with the recent CCPA and oncoming CPRA.[238] Although the Californian regulations do not create a carbon copy of the European model, they provide many similar protections.[239] In fact, the state's data privacy standard structure is now more akin to the EU's regime than the US's and is better suited to the EU than any other state.[240] As noted by the CJEU, territories do not need to have an exact match to EU privacy regulations for lawful data transfers to occur.[241] Rather, they only need to have a system that is fundamentally comparable to the European caliber for protection.[242]

Even if state-based adequacy does not fully replace the need for a nationwide mechanism, it could facilitate a more comprehensive agreement in the future.[243] Several states already seem to follow California's lead closely.[244] By allowing individual states to pursue adequacy determinations from the Com-

---

[236] *See* Lefkowitz, *supra* note 234 (claiming that 7% of the entire US economy is based in technology and that portion is increasing quickly); Limbago, *supra* note 235 (showing that states take influence from other states' privacy regulations to develop their own); N. Gregory Mankiw, *Competition Is Healthy for Governments, Too*, N.Y. TIMES (Apr. 14, 2012), https://www.nytimes.com/2012/04/15/business/competition-is-good-for-governments-too-economic-view.html [https://perma.cc/NDL5-ZAKJ] (proposing that governments improve when they compete with each other).

[237] *See* Leins, *supra* note 200 (reflecting on the wide range of additional privacy regulation among the states).

[238] *See California Consumer Privacy Act (CCPA)*, *supra* note 208 (addressing the recent umbrella privacy law in California that encompasses a wide majority of personal data and its use); *see also* Lam, *supra* note 209 (including the relevant additions that the CPRA will affect).

[239] *See generally* JEHL & FRIEL, *supra* note 211 (noting some similarities and differences between the CCPA and GDPR). Both the CCPA and GDPR safeguard relatively similar types of persons and information. *Id.* But the right to "opt-out" diverges significantly between the two documents. *Id.*

[240] *See* Lam, *supra* note 209 (adding even more "omnibus-esque" provisions to Californians' bundle of privacy rights); Umhoefer, *supra* note 107 (textualizing the common equation of the CCPA to the GDPR to show that, although very similar to the GDPR, the CCPA does not quite match its level of regulation); *EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce*, *supra* note 5 (differentiating the US from EU legislation because of its sectoral approach); *see also California Consumer Privacy Act (CCPA)*, *supra* note 208 (stating the additional rights provided in the CCPA). *See generally* JEHL & FRIEL, *supra* note 211 (comparing the CCPA with the GDPR to determine the similarities and less frequent differences).

[241] *See* Case C–362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650, ¶ 73 (Oct. 6, 2015) (requiring "essentially equivalent" protection for a country to be adequate to lawfully transfer data with the EU).

[242] *Id.*

[243] Jennifer Bryant, *2021 'Best Chance' for US Privacy Legislation*, IAPP (Dec. 7, 2021), https://iapp.org/news/a/2021-best-chance-for-federal-privacy-legislation/ [https://perma.cc/3Q3W-Z5SR] (predicting that US privacy standards will change in 2021 because the new executive leadership may try to follow the states' thrust towards stricter regulations).

[244] *See US State Privacy Legislation Tracker: Bills Introduced 2021*, *supra* note 201 (noting the later passed legislation in Colorado and California and a list of similar pending privacy bills).

mission, the US would create an economic incentive for all states to improve their local privacy regulations.[245] Over time, additional states would likely adopt pseudo-omnibus legislation similar to California's to allow their businesses to participate in the transatlantic trade more confidently.[246] As more states augment their own standards, it would then become easier for the US to raise the federal floor to a suitable level.[247]

Some argue, however, that the US should adopt national umbrella legislation to pacify the tension between the EU and US privacy frameworks.[248] As US data breaches become more dangerous and prevalent than ever, the desire to protect personal information broadly has intensified.[249] Federal omnibus

---

[245] *See* Kennedy, *supra* note 51 (noting the tremendous profit that a business can gain by competing in the data market).

[246] *See* Limbago, *supra* note 235 (suggesting that most states are following the guidance of privacy leaders, like California, to adopt their own pseudo-omnibus legislation in a trend toward heightened protection); *see also* Christopher DeMuth, *Competition and the Constitution*, NAT'L AFFS. (2011), https://www.nationalaffairs.com/publications/detail/competition-and-the-constitution [https://perma.cc/BWB2-UQRC] (concluding that competition is an important policy consideration, as well as is a fundamental component of human nature). Competition is everywhere. *See* DeMuth, *supra* (proposing that people experience genetic competition in their DNA, social competition in their relationships with others, and material competition in their resources); *see also* Malcolm H. Dunn, *Do Nations Compete Economically? A Critical Comment on Prof. Krugman's Essay "Competitiveness: A Dangerous Obsession,"* 29 INTERECONOMICS 303, 304–06 (1994), https://www.econstor.eu/bitstream/10419/140477/1/v29-i06-a07-BF02928169.pdf [https://perma.cc/SY5Q-YYAA] (explaining that there is a benefit to inter-jurisdictional economic competition). Regardless of whether competition among the states is beneficial, it is likely to occur, meaning that they will likely compete for better privacy standards if incentivized. *See* Dunn, *supra*, at 304–06 (proposing an alternative line of thinking to another professor's proposal that national competition is bad). And, if pseudo-omnibus legislation was incentivized, other states would undoubtedly pursue it. *See generally* DeMuth, *supra* (suggesting that rivalry could drive legislative choices).

[247] *See* MILDEBRATH, *supra* note 12 (reasoning that revamping federal law is currently impractical given the overall privacy regime of the US and its states). States only possess the power to provide their constituents with privacy regulations that are stricter and agreeable with those afforded by the federal government. *See* U.S. CONST. art. VI, cl. 2 (giving precedent to any federal law over conflicting state law); Stephen A. Gardbaum, *The Nature of Preemption*, 79 CORNELL L. REV. 767, 770 (1994) (explaining that states can still regulate in the same area as a federal law so long as its provisions do not conflict with those of the supreme document). Thus, states that do not choose to regulate beyond the federal floor can clamp down on their ability to easily change. *See* MILDEBRATH, *supra* note 12 (demonstrating that it would be far-fetched for the federal government to reconstruct the US privacy standard). If states, however, each elevated their protection above the baseline, the federal government could raise its standard to match stricter state laws with more ease, rather than having to hoist up all fifty states itself. *Id.*

[248] *See* Tanith L. Balaban, *Comprehensive Data Privacy Legislation: Why Now Is the Time*, 1 CASE W. RSRV. J.L. TECH. & INTERNET 1, 30 (2009) (claiming that the US can and should enact omnibus legislation because it would comport with American principles); Candice L. Kline, Comment, *Security Theater and Database-Driven Information Markets: A Case for an Omnibus U.S. Data Privacy Statute*, 39 U. TOL. L. REV. 443, 494–95 (2008) (arguing in favor of the US adopting omnibus legislation to rectify data privacy fallacies made in response to 9/11).

[249] *See* Carol Li, Note, *A Repeated Call for Omnibus Federal Cybersecurity Law*, 94 NOTRE DAME L. REV. 2211, 2233 (2019) (noting that the level of data insecurity in the US is so pervasive that individuals often must become complacent and accepting of businesses that violate their privacy).

legislation, therefore, often appears to be the obvious way to meet EU standards and change the reality of cybersecurity in the US.[250] But, this approach is not currently realistic because the US's regulatory framework is too fragmented.[251] The US has neither the resources nor the willingness to execute the degree of modernization necessary to completely restructure the national framework in the near future.[252] In fact, *Schrems III* will certainly occur before the US could practically adopt an omnibus law.[253]

A 'state-based adequacy now, national adequacy over time' approach could also alleviate the EU's concern for US surveillance practices.[254] The EU will undoubtedly continue to scrutinize US security programs and regulations.[255] But, the recent trend by states to tighten data privacy regulations has sparked Congress to develop a national data privacy authority that could eventually limit federal surveillance programs.[256] Besides, state advances could

---

[250] *See id.* at 2234–39 (arguing that an omnibus privacy law in the US could protect the safety of citizens, the goodwill of businesses, the ability for smaller entities to remain profitable, and holistically raise the bar for the protection of information nationwide). Some have even presented drafts of potential omnibus legislation that the US could use if it decided to enact an omnibus law. *See generally* Scot Ganow & Sam S. Han, *Model Omnibus Privacy Statute*, 35 U. DAYTON L. REV. 345 (2010) (drafting an example of one way that the US could structure an umbrella law based on a survey of the current sectoral federal statutes and their protections).

[251] *See* MILDEBRATH, *supra* note 12 (reciting the US's response that it could not actually adopt the recommendations made by the EU and Schrems); Voss, *supra* note 29, at 410 (commenting on the structural conflict between EU and US data privacy frameworks).

[252] *See* MILDEBRATH, *supra* note 12 (citing the official opinion from the US that restructuring its privacy framework is unlikely to occur at this time because it would be too difficult). The US has a massive debt that inflates with time. *See* Marcus Lu, *Charting America's Debt: $27 Trillion and Counting*, VISUAL CAPITALIST (Oct. 30, 2020), https://www.visualcapitalist.com/americas-debt-27-trillion-and-counting/ (claiming that the government continues to make greater expenditures than earnings) [https://perma.cc/9X42-Y6VA]. This debt became increasingly problematic in 2020 because COVID-19 strained the country's resources even more. *Id.*

[253] *See* MILDEBRATH, *supra* note 12 (contrasting Schrems' opinion that the US needs to adopt omnibus legislation with the government's response that it could not do so).

[254] *See* Limbago, *supra* note 235 (assessing the individual paths by various states to better regulate data privacy concerns); Peter Margulies & Ira Rubinstein, *EU Privacy Law and U.S. Surveillance: Solving the Problem of Transatlantic Data Transfers*, LAWFARE (Mar. 10, 2021), https://www.lawfareblog.com/eu-privacy-law-and-us-surveillance-solving-problem-transatlantic-data-transfers [https://perma.cc/E3WL-VVMV] (commenting that the US must implement "checks" to reduce EU concern for its national security programs); Brian Roberts, *State Governments Check Federal Power*, TENTH AMENDMENT CTR. (Jan. 29, 2012), https://tenthamendmentcenter.com/2012/01/29/state-governments-check-federal-power/ [https://perma.cc/8JQW-2D5K] (discussing the ability for state governments to monitor federal actions and dissuade or prevent abuse).

[255] *See* MILDEBRATH, *supra* note 12 (suggesting that the US's privacy structure will, as a whole, remain stagnant in the oncoming years); *see, e.g.*, Case C–311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶ 65 (July 16, 2020) (lambasting FISA).

[256] *See* Gardbaum, *supra* note 247, at 770 (stating the long-understood concept that, in the instance that a state law disagrees with a federal law, the federal law will always prevail); Bryant, *supra* note 243 (suggesting that the federal government may take cues from state-level privacy laws). The tiered structure of the US government allows the states with some self-sovereignty to differentiate themselves from federal legislation, so long as they do not attempt to disband any of the privacy regu-

quell this apprehension, even without the ability to displace federal legislation.[257] Individual states are removed from the federal government's complete control, and could therefore develop truly autonomous ombudspersons to address privacy complaints brought by Europeans.[258] Each state could reconcile any remaining surveillance concerns while negotiating adequacy with the Commission to guarantee its approval.[259] And with each state that moved the US towards a national omnibus standard, the EU's uneasiness would necessarily shrink.[260]

CONCLUSION

The transatlantic trade of personal information is critical to the EU and US economies. Although recent technological advances make the access to and usability of personal information incredibly profitable, the dissemination of highly individualized information raises substantial concern for the privacy rights of individuals. Because the EU and the US have weighed these considerations differently in their privacy regimes, they have struggled to trade data with each other.

---

lations enacted by the federal government. *See* Gardbaum, *supra* note 247, at 771 (explaining how the separation of powers between the federal and states' legislatures allows each to regulate differently).

[257] *See* Zack Whittaker, *A New Senate Bill Would Create a US Data Protection Agency*, TECHCRUNCH (Feb. 13, 2020), https://techcrunch.com/2020/02/13/gilliband-law-data-agency/ [https://perma.cc/E2HG-DW48] (commenting on the potential for the US to adopt a "data protection agency" in the near future). Senator Kirsten Gillibrand's proposed legislation, the Data Protection Act, purports to design a new federal agency that would govern data privacy regulations across the US. *Id.*

[258] *See* MILDEBRATH, *supra* note 12 (questioning the effectiveness and autonomy of the federal-level ombudsperson mechanism installed between Safe Harbor and Privacy Shield); CONG. RSCH. SERV., *supra* note 104, at 1 (explaining the separation between federal and state powers); Dave Roos, *When the Founding Fathers Settled States' vs. Federal Rights—and Saved the Nation*, HIST., https://www.history.com/news/federalism-constitution-founding-fathers-states-rights [https://perma.cc/2HYG-VQW6] (Apr. 30, 2020) (recognizing that states are constitutionally separated, at least in part, from the control of the federal government, a concept known as "federalism"). The CJEU ruled, upon close examination, that the ombudsperson was not actually structurally or personally separate from the agencies that it was meant to protect European from. MILDEBRATH, *supra* note 12. It concluded that this arrangement not only failed to ease its qualms about US surveillance but actually heightened the concerns over the US's ability to provide meaningful accountability for its government's practices. *See id.*

[259] *See* Andrei Gribakov, *Road to Adequacy: Can California Apply Under the GDPR?*, LAWFARE (Apr. 22, 2019), https://www.lawfareblog.com/road-adequacy-can-california-apply-under-gdpr [https://perma.cc/5587-AS7Y] (stating that California will have to arrange to help alleviate some of the discrepancies between the GDPR and CCPA to achieve "adequacy" from the EU). The two pieces of legislation differ most in the types of businesses that are included in the laws' definitions, the opportunity to fix any incorrect information, the necessity of legal justification to process data, and the existence of an enforcement agency. *See id.* (addressing where the privacy laws fail to line up). The CPRA, nevertheless, may work to eliminate at least some of these concerns. *See* Lam, *supra* note 209 (announcing that the CPRA will add a privacy enforcement agency in California that was not present in the CCPA).

[260] *See* Limbago, *supra* note 235 (predicting a national trend toward pseudo-omnibus state legislation in the US); *see, e.g.*, *Schrems II*, ECLI:EU:C:2020:559 (representing the worry that the EU and CJEU continue to hold for US privacy adequacy).

To remedy these differences, the EU and the US have tried to negotiate mechanisms that allow the US to obtain the requisite "adequacy" determination to make lawful data transfers with European entities in Safe Harbor and Privacy Shield. The CJEU struck both down, respectively, with *Schrems v. Data Protection Commissioner* (*Schrems I*), in 2015, and *Data Protection Commissioner v. Facebook Ireland Ltd.* (*Schrems II*), in 2020. The court cited the US's insufficient privacy protections to disallow these data transfers.

The US, however, is unlikely to nationally meet the strict and high standards set by the EU before there is a *Schrems III* challenge. Instead, certain individual states, like California, should negotiate state-specific adequacy. Over time, more states will likely raise their own privacy regulations to seek adequacy as well. Eventually, this shift will help the federal government to elevate its standard and earn a nationwide adequacy determination from the EU to guarantee the transatlantic data privacy trade.

EMILY A. IVERS